

М. Нильсен, И. Чанг

**КВАНТОВЫЕ ВЫЧИСЛЕНИЯ
И КВАНТОВАЯ ИНФОРМАЦИЯ**

Перевод с английского
под редакцией М. Н. Вялого и П. М. Островского
с предисловием К. А. Валиева



Москва «Мир» 2006

УДК 530 145 (21)

ББК 22 12 22 134

Н66

Переводчики. Басова М А (гл. 12), Бравый С Б (гл 7, 11),
Завьялов В В (гл 9, 10), Кондратьев В.В (гл 2, 6, Приложения),
Львовский С М. (гл. 3 – 5), Мельниковский Л А. (гл. 8),
Москалев Т.Ю (Предисловие, гл 1)

Нильсен М., Чанг И.

Н66 Квантовые вычисления и квантовая информация. Пер. с англ — М : Мир, 2006 г. — 824 с., ил

ISBN 5-03-003524-9

Книга известных американских специалистов дает подробное и всестороннее введение в новую область исследований изучение роли физических законов (и, особенно, законов квантовой механики) при решении задач информатики. Охвачены такие темы, как квантовые алгоритмы (факторизация, дискретный логарифм), квантовая телепортация, сверхплотное кодирование, устойчивые к ошибкам вычисления, квантовая криптография.

Книга доступна читателям, начинаяющим знакомиться с предметом приведены необходимые сведения из физики, математики и информатики. Множество рисунков и упражнений способствует более глубокому усвоению материала. Каждая глава заканчивается историческими замечаниями и списком литературы для дальнейшего изучения.

Для студентов, аспирантов, преподавателей и исследователей в области физики, информатики, математики и электротехники, интересующихся квантовыми вычислениями и квантовой информацией

УДК 530 145 (21)

ББК 22 12 22.134



Издание осуществлено при поддержке
Российского фонда фундаментальных исследований по проекту
№ 02-01-14056

Редакция литературы по информатике и новой технике

© Cambridge University Press
2000, 2001

© перевод на русский язык,
издательство "Мир", 2006

ISBN 5-03-003524-9 (русс.)

ISBN 0-521-63503-9 (англ.)

ПРЕДИСЛОВИЕ К РУССКОМУ ИЗДАНИЮ

Авторы рекомендуемой русскому читателю книги «Квантовые вычисления и квантовая информация», Майкл Нильсен и Исаак Чанг, в авторских предисловии и введении подробно излагают структуру, содержание и цели написанной ими книги. Поэтому нет необходимости заниматься этим в нашем предисловии. Тем не менее, мы хотим в нескольких словах представить книгу русскому читателю.

Темы книги М Нильсена и И Чанга — квантовые компьютеры и квантовые вычисления, квантовая связь, квантовая криптография, телепортация и др — вызывают большой интерес широких масс русскоязычной публики. Не только научные и научно-популярные издания, но и газеты и телевидение стремятся публиковать новости из этой области, удовлетворяя интерес читателей и слушателей. Тем не менее, мало кто из читателей по-настоящему понимает такие научно-популярные тексты. Дело в том, что идеи квантовой информатики вообще и квантовых вычислений, в частности, являются продуктом новейшего времени и совершенно не успели войти в практику вузовского (и, тем более, школьного) образования, в учебники и учебные руководства. Даже классические учебники по квантовой механике не содержат важнейших понятий квантовой физики, лежащих в основе квантовой информатики (понятия запутанных состояний, например). Поэтому, при наличии острого интереса к этой интригующей тематике, у читателей почти нет «бэкграунда» к восприятию достижений в области квантовой информатики.

В этой ситуации выбор книги М Нильсена и И Чанга для издания на русском языке представляется весьма удачным решением издательства «Мир». Среди десятка англоязычных книг по этой тематике рекомендуемая книга стоит особняком. По полноте и научной строгости изложения она является настоящей энциклопедией. Не случайно, что с момента ее издания в 2000 году, почти в каждой научной статье по данной тематике можно найти ссылку на эту книгу. Научная строгость изложения, полнота математического (теоретического) описания предмета делают книгу настоящей находкой для тех, кто хотел бы присоединиться к новой области исследований. Вместе с тем, насыщенность изложения математикой делает чтение книги настоящей работой, которая, несомненно, будет вознаграждена в дальнейшей деятельности читателя. Для тех читателей, которые хотели бы получить первичные знания в этой новой области науки, текст книги содержит разделы вводного характера, которые могут быть прочтены в первую очередь. Мы не сомневаемся, что каждый специалист в области информатики найдет для себя полезным чтение этой замечательной книги.

Переводчики книги столкнулись с отсутствием установившейся русскоязычной терминологии для области квантовой информатики. В этой ситуации авторы перевода пользовались терминами, которые сочли предпочтительными. Можно надеяться, что терминологические проблемы не слишком затруднят чтение книги. Добавим также, что в список литературы включены ряд книг и обзоров на русском языке, а также в конце книги приведен русскоязычный предметный указатель.

Москва

Декабрь 2005 г.

K. A. Валиев

ПРЕДИСЛОВИЕ

Нашим родителям и нашим учителям.

Эта книга представляет собой введение в основные понятия и методы, относящиеся к области квантовых вычислений и квантовой информации. Быстрые темпы прогресса в этой области и ее междисциплинарный характер привели к тому, что начинающим знакомиться с этим предметом трудно получить общее представление о наиболее важных методах и результатах.

Книга имеет двойное назначение. Во-первых, мы приводим основные сведения из информатики, математики и физики, необходимые для понимания квантовых вычислений и квантовой информации. Это делается на уровне, доступном для читателей с базовой подготовкой хотя бы в одной из трех указанных дисциплин; наиболее важные требования — определенная степень математической зрелости и желание изучать квантовые вычисления и квантовую информацию. Второе назначение этой книги — подробно раскрыть главные результаты в области квантовых вычислений и квантовой информации. При тщательном изучении у читателя должно выработать понимание основных инструментов и достижений в этой увлекательной области, которое станет для него либо частью общего образования, либо основой для самостоятельных исследований в сфере квантовых вычислений и квантовой информации.

Структура книги

Базовая структура книги показана на рис. 1. Книга разделена на три части. Общая стратегия состоит в том, чтобы по возможности идти от конкретного к более абстрактному. Так, мы рассматриваем квантовые вычисления прежде квантовой информации, конкретные коды, исправляющие квантовые ошибки, перед более общими результатами квантовой теории информации, и на протяжении всей книги пытаемся приводить примеры до того, как будет развита общая теория.

В части I дается обзор главных идей и результатов в области квантовых вычислений и квантовой информации, а также приводятся базовые сведения из информатики, математики и физики, необходимые для глубокого понимания предмета. Глава 1 является вводной, в ней обрисовываются история развития и фундаментальные понятия рассматриваемой области и по ходу изложения отмечаются некоторые важные нерешенные проблемы. Материал представлен так, чтобы быть доступным даже при отсутствии подготовки в области информатики и физики. Сведения, необходимые для более глубокого понимания, приводятся в главах 2 и 3. В них подробно рассматриваются основные понятия

квантовой механики и информатики соответственно. В зависимости от своей подготовки вы можете уделять различным главам части I больше или меньше внимания, возвращаясь к ним позже при необходимости восполнить какие-либо пробелы в своих знаниях основ квантовой механики и информатики.



Рис. 0.1. Структура книги.

В части II подробно описываются квантовые вычисления. В гл. 4 вводятся основные элементы, необходимые для выполнения квантовых вычислений, и многие элементарные операции, которые можно использовать для разработки более сложных применений квантовых вычислений. В главах 5 и 6 описываются квантовое преобразование Фурье и квантовый алгоритм поиска — два основных известных к настоящему времени квантовых алгоритма. В гл. 5 также объясняется, как можно использовать квантовое преобразование Фурье для решения задач факторизации и вычисления дискретного логарифма, и почему эти результаты важны в криптографии. В гл. 7 описываются общие принципы проектирования и свойства хороших физических реализаций квантовых компьютеров. При этом в качестве примеров используется несколько реализаций, успешно продемонстрированных в лабораториях.

В части III речь идет о квантовой информации: что это такое, как представлять и передавать информацию при помощи квантовых состояний, а также как описывать и устранять искажения квантовой и классической информации. В гл. 8 описываются свойства квантового шума, что необходимо для

понимания того, как обрабатывается квантовая информация в реальном мире, и *формализм квантовых преобразований* — мощный математический инструмент, способствующий пониманию квантового шума. В гл. 9 рассматриваются *меры различия* квантовой информации, которые позволяют придавать количественную точность утверждениям о том, что два элемента квантовой информации похожи. В гл. 10 описываются коды, исправляющие квантовые ошибки, которые можно использовать для защиты квантовых вычислений от влияния шума. В этой главе важным результатом является *пороговая теорема*, показывающая, что для реалистичных моделей шум в *принципе* не является серьезным препятствием для квантовых вычислений. В гл. 11 вводится фундаментальное теоретико-информационное понятие *энтропии* и объясняются многие свойства энтропии как в классической, так и в квантовой теории информации. Наконец, в гл. 12 обсуждаются свойства квантовых состояний, относящиеся к передаче информации, а также квантовые каналы связи с подробным рассмотрением многих непривычных и интересных свойств этих систем в плане передачи классической и квантовой информации и в отношении передачи секретной информации.

На протяжении всей книги встречается большое число упражнений и задач. Упражнения нацелены на то, чтобы закрепить понимание базового материала, и находятся внутри основного текста. За редкими исключениями они должны легко выполняться в течение нескольких минут. Задачи приводятся в конце каждой главы и предназначены для того, чтобы познакомить с новым и интересным материалом, для которого не нашлось достаточно места в основном тексте. Многие задачи состоят из нескольких частей, развивающих определенную нить рассуждений. К моменту выхода книги некоторые из задач еще не были решены. В соответствующих случаях это отмечается в формулировке задачи. Каждая глава завершается кратким изложением материала, а также разделом «История и дополнительная литература», в котором прослеживается развитие основных идей главы и приводятся рекомендации по дальнейшему чтению.

В начале книги помещен список терминов и обозначений, который поможет вам в процессе чтения. В конце книги приведены шесть приложений, список литературы, предметный указатель и оглавление.

Приложение 1 содержит некоторые основные определения, обозначения и утверждения из элементарной теории вероятностей. Этот материал (подразумевается, что он знаком читателям) включен для облегчения ссылок. В приложении 2 дается обзор некоторых элементарных понятий теории групп, оно также включено главным образом для удобства. Приложение 3 содержит доказательство теоремы Соловея–Китаева — важного для квантовых вычислений результата, который показывает, что с помощью конечного набора квантовых элементов можно быстро аппроксимировать произвольный квантовый элемент. В приложении 4 приводятся элементарные сведения из теории чисел, необходимые для понимания квантовых алгоритмов факторизации и вычисления дискретного логарифма, а также криптосистемы RSA, рассматриваемой в приложении 5. Приложение 6 содержит доказательство теоремы Либа — одного из

наиболее важных результатов в области квантовых вычислений и квантовой информации, из которого следуют такие важные энтропийные неравенства, как неравенство сильной субаддитивности. Доказательства теоремы Соловея–Китаева и теоремы Либа довольно длинные, поэтому мы считаем оправданным их рассмотрение отдельно от основного текста.

В списке литературы перечислены все работы, на которые давались ссылки в тексте книги. Приносим извинения тем исследователям, чья работа была ненамеренно пропущена.

Область квантовых вычислений и квантовой информации в последние годы развивается столь быстро, что мы не смогли охватить все темы настолько глубоко, насколько нам этого хотелось бы. Три темы заслуживают отдельного упоминания. Одной из них является тема *мер запутанности*. Как объясняется в книге, запутанность (*entanglement*) — это ключевое звено в таких вопросах, как квантовая телепортация, быстрые квантовые алгоритмы и исправление квантовых ошибок. Короче говоря, это очень полезный ресурс в квантовых вычислениях и квантовой информации. К настоящему времени сложилось быстро растущее исследовательское сообщество, занимающееся изучением явления запутывания как нового типа физического ресурса и ведущее поиск принципов, определяющих способы его практического применения. Мы полагаем, что эти исследования, будучи исключительно многообещающими, еще не достаточно завершены, чтобы их можно было широко обсуждать, как другие темы данной книги, и поэтому ограничились лишь их кратким описанием в гл. 12. Аналогично, тема распределенных квантовых вычислений (которые иногда называют квантовой коммуникационной сложностью) является исключительно многообещающей и разрабатывается столь активно, что мы не стали ее освещать, опасаясь устаревания материала еще до публикации книги. Реализация устройств обработки квантовой информации также развилаась в увлекательную и обширную область, и мы ограничились лишь одной главой по этой теме. Очевидно, что о физических реализациях можно рассказать гораздо больше, но при этом пришлось бы затрагивать многие другие области физики, химии и техники, для чего мы не имеем здесь места.

Как использовать эту книгу

Эта книга допускает большое разнообразие способов использования. Она может быть взята в качестве основы для различных учебных курсов, от коротких лекций по определенной теме из области квантовых вычислений и квантовой информации до годичных курсов, охватывающих всю область. Ее могут использовать для самостоятельного изучения как те, кто хотел бы лишь в общих чертах узнать о квантовых вычислениях и квантовой информации, так и те, кто хотел бы оказаться на переднем крае исследований. Предполагается также, что она послужит справочником для тех, кто сейчас ведет исследования в рассматриваемой области.

Замечание для изучающих предмет самостоятельно

Книга написана так, чтобы быть доступной для самостоятельного изучения. Текст снабжен большим числом упражнений, которые могут использоваться для самопроверки понимания основного материала. Оглавление книги и краткое изложение в конце глав позволяют быстро определять, какие главы вы хотите изучать наиболее глубоко. Диаграмма на рис. 1 поможет определить, в каком порядке можно изучать материал книги.

Замечание для преподавателя

В этой книге охватывается широкий диапазон тем и, следовательно, она может использоваться в качестве основы для самых разнообразных курсов.

Односеместровый курс по квантовым вычислениям может основываться на материале из глав 1–3, выбранном в зависимости от подготовки группы, за которым последуют гл. 4 (по квантовым схемам), главы 5 и 6 (по квантовым алгоритмам), выбранные части гл. 7 (по физическим реализациям), а также главы 8–10 по вопросам исправления квантовых ошибок с особым упором на гл. 10.

Односеместровый курс по квантовой информации может базироваться на материале из глав 1–3, выбранном в зависимости от подготовки группы. Затем последуют главы 8–10 (по исправлению квантовых ошибок), а за ними — главы 11 и 12 (по квантовой энтропии и квантовой теории информации соответственно).

Годичный курс может охватывать всю книгу, включая дополнительный материал, выбранный из разделов «История и дополнительная литература» нескольких глав. Кроме того, квантовые вычисления и квантовая информация идеально подходят для самостоятельных исследовательских проектов студентов.

Мы надеемся, что помимо курсов по квантовым вычислениям и квантовой информации книга будет использована и другим способом, а именно как учебник для вводного курса по квантовой механике для студентов-физиков. Традиционные введения в квантовую механику в значительной степени опираются на математический аппарат дифференциальных уравнений в частных производных. Как мы полагаем, это часто скрывает основные идеи. Квантовые вычисления и квантовая информация предоставляют великолепную концептуальную лабораторию для понимания основных понятий и отдельных аспектов квантовой механики без применения громоздкого математического аппарата. В основу такого курса могут быть положены введение в квантовую механику из гл. 2, базовый материал по квантовым схемам из гл. 4, выбранный материал по квантовым алгоритмам из глав 5 и 6, гл. 7 о физических реализациях квантовых вычислений, а затем по вкусу почти любая выборка материала из части III.

Замечание для студента

Мы написали эту книгу так, чтобы она по возможности была самодостаточной. Главное исключение в том, что время от времени мы опускали доказательства, которые на самом деле нужно проводить самостоятельно, обычно они предлагаются как упражнения. Мы советуем вам хотя бы пытаться делать все упражнения по мере чтения книги. За редкими исключениями упражнения могут быть выполнены в несколько минут. Если вы испытываете значительные трудности со многими упражнениями, это может свидетельствовать о том, что вам нужно вернуться назад и повторить один или несколько ключевых вопросов.

Дополнительная литература

Как уже отмечалось, каждая глава завершается разделом «История и дополнительная литература». Кроме того, существует несколько источников с широким охватом материала, которые могут представлять интерес для читателей.¹ В превосходных конспектах лекций Прескилла [329] квантовые вычисления и квантовая информация преподносятся с несколько иной точки зрения, нежели в этой книге. К хорошим обзорным статьям по конкретным тематикам относятся (в порядке их упоминания в этой книге) обзор Аароновой по квантовым вычислениям [9], обзор Китаева по алгоритмам и методам исправления ошибок [213], диссертация Москса по квантовым алгоритмам [294], диссертация Фукса [157] по различимости и мерам различия в квантовой информации, диссертация Готтесмана [166] по исправлению квантовых ошибок, обзор Прескилла по методам исправления квантовых ошибок [327], диссертация Нильсена по квантовой теории информации [303] и обзоры этой теории, составленные Беннетом и Шором [72], а также Беннетом и Дивинченцо [37]. Другие полезные работы — книга Груски [172] и сборник обзорных статей под редакцией Ло, Шпиллера и Попеску [270].

Ошибки

В любой книге есть ошибки и упущения, и эта, конечно, не является исключением. По мере обнаружения опечаток мы будем добавлять их к списку, ведущемуся на web-сайте книги <http://www.squint.org/qci/>

¹На русском языке имеются также книги Китаев А., Шень А., Вялый М. Классические и квантовые вычисления, М. МЦНМО — Чэ Ро, 1999 Холево А С Введение в квантовую теорию информации, К. МЦНМО, 2000 — Прим. ред

БЛАГОДАРНОСТИ

Некоторые люди оказали решающее влияние на наши представления о квантовых вычислениях и квантовой информации. За многочисленные приятные дискуссии, которые помогли сформировать и уточнить наши взгляды, Майкл Нильсен благодарит Карла Кейвза, Криса Фукса, Джерарда Милбурна, Джона Прескилла и Бена Шумахера, а Исаак Чанг — Тома Кавера, Умеша Вазирани, Йоши Ямамото и Берни Юрка.

В создании этой книги нам прямо и косвенно помогало огромное количество людей. Вот лишь частичный список. Дорит Ааронова, Андريس Амбайнис, Набил Амер, Говард Барнум, Дейв Бекман, Гарри Берман, группа изучения квантовой оптики Калтека, Эндрю Чайлдс, Фред Чонг, Ричард Клив, Джон Конвей, Джон Кортез, Майкл Дешазо, Рональд де Вулф, Дэвид Дивинченцо, Стивен ван Энк, Генри Эверит, Рон Фагин, Майк Фридман, Майкл Гаген, Нейл Гершенфельд, Даниэль Готтесман, Джим Харрис, Александр Холево, Эндрю Хайберс, Джулия Кемпе, А. Китаев, Манни Нилл, Шинг Конг, Раймонд Лафламм, Эндрю Лэндаль, Рон Легер, Дебби Люнг, Даниэль Лидар, Эллиот Либ, Тереза Линн, Гидео Мабучи, Ю. И. Манин, Майк Моска, Алекс Пайнс, Шридхар Раджагопалан, Билл Риск, Бет Рускай, Сара Шнейдер, Роберт Шредер, Питер Шор, Шери Столл, Волкер Штрассен, Армин Ульман, Ливен Вандерспен, Анна Верхальст, Дебби Уоллач, Майк Вестморленд, Дейв Уайнленд, Говард Уайзман, Джон Ярд, Зинлан Жоу и Войтек Зурек.

Спасибо сотрудникам Cambridge University Press за помощь в воплощении замысла этой книги в реальность. Отдельной благодарности заслуживают наш заботливый и энергичный редактор Симон Капелин, который вел этот проект более трех лет, а также Маргарет Паттерсон — за своевременную и тщательную корректуру рукописи.

Во время работы над книгой Майкл Нильсен был толмансским стипендиатом в Калифорнийском технологическом институте, членом группы теоретической астрофизики Т-6 в Лос-Аламосской национальной лаборатории и сотрудником центра перспективных исследований университета Нью-Мексико, а Исаак Чанг — сотрудником Альмаденского исследовательского центра IBM, консультирующим доцентом электротехники в Стэнфордском университете, приглашенным исследователем в отделении информатики Калифорнийского университета Беркли, членом группы теоретической астрофизики Т-6 в Лос-Аламосской национальной лаборатории и приглашенным исследователем в институте теоретической физики при Калифорнийском университете в Санта-Барбаре. Мы также высоко ценим теплоту и гостеприимство Аспенского физического центра, где была выполнена окончательная вычитка страниц книги.

Авторы глубоко признательны за поддержку, оказанную DARPA в рамках исследовательского проекта NMRQC и институтом QUIC при Управлении военных исследований. Мы также благодарим за щедрую поддержку Национальный научный фонд, Национальное агентство безопасности, Управление военно-морских исследований и компанию IBM.

ТЕРМИНОЛОГИЯ И ОБОЗНАЧЕНИЯ

Некоторые термины и обозначения, используемые в области квантовых вычислений и квантовой информации, имеют два или более общеупотребительных значения. Для предотвращения возможной путаницы многие из таких часто используемых терминов и обозначений собраны в этом разделе вместе с соглашениями, которых авторы будут придерживаться на протяжении книги.

Линейная алгебра и квантовая механика

Все векторные пространства считаются конечномерными, если не указано другое. Во многих случаях такое ограничение является излишним или может быть снято за счет некоторой дополнительной технической работы, но его повсеместное использование делает изложение более доходчивым и не слишком умаляет значимость многих предполагаемых применений полученных результатов.

Неотрицательно определенным оператором A называется такой оператор, для которого $\langle \psi | A | \psi \rangle \geq 0$ для всех $|\psi\rangle$. *Положительно определенным оператором* A называется такой оператор, для которого $\langle \psi | A | \psi \rangle > 0$ для всех $|\psi\rangle \neq 0$. *Носитель* оператора определяется как ортогональное дополнение к его ядру. Для эрмитова оператора это означает, что носитель порожден собственными векторами оператора с ненулевыми собственными значениями.

Обозначение U (и часто, но не всегда, V) будет, как правило, использоваться для унитарного оператора или матрицы. *H* обычно используется для обозначения квантового логического элемента, элемента Адамара, а иногда — для обозначения гамильтонiana квантовой системы, что будет ясно из контекста.

Векторы иногда будут записываться в виде столбца, например

$$\begin{bmatrix} 1 \\ 2 \end{bmatrix}, \quad (1)$$

а иногда в виде $(1, 2)$. Последнее нужно рассматривать как сокращенную запись для вектора-столбца. Для двухуровневых квантовых систем, используемых в качестве кубитов, мы обычно будем отождествлять состояние $|0\rangle$ с вектором $(1, 0)$, а $|1\rangle$ — с вектором $(0, 1)$. Мы также определяем матрицы Паули традиционным способом — см. ниже раздел «Часто используемые обозначения квантовых элементов и схем». Здесь наиболее существенно то, что соглашение для z -матрицы Паули выглядит как $\sigma_z|0\rangle = |0\rangle$ и $\sigma_z|1\rangle = -|1\rangle$, т. е. обратно тому, что интуитивно ожидают увидеть некоторые физики (но, как правило, не математики). Это несоответствие вызвано тем, что собственное значение σ_z , равное +1, физики часто отождествляют с так называемым «возбужденным состоянием», и для многих кажется естественным отождествить его с $|1\rangle$, а не с $|0\rangle$, как сделано в настоящей книге. Наш выбор продиктован стремлением

сохранить согласованность с традиционным индексированием матричных элементов в линейной алгебре. В этом случае естественно отождествлять первый столбец σ_z с действием σ_z на $|0\rangle$, а второй столбец — с действием на $|1\rangle$. Такой подход используется всеми, кто занимается вопросами квантовых вычислений и квантовой информации. В дополнение к традиционным обозначениям матриц Паули, σ_x , σ_y и σ_z , нам будет удобно использовать для этих трех матриц обозначения σ_1 , σ_2 , σ_3 и определить σ_0 как единичную матрицу 2×2 . Однако чаще всего мы используем для σ_0 , σ_1 , σ_2 и σ_3 обозначения I , X , Y и Z соответственно.

Теория информации и вероятность

Как принято в теории информации, логарифмы всегда берутся по основанию два, если не указано другое. Мы используем $\log(x)$ для обозначения логарифмов по основанию 2, а $\ln(x)$ — в тех редких случаях, когда нужно взять натуральный логарифм. Под термином *распределение вероятностей* понимается конечное множество таких действительных чисел p_x , что $p_x \geq 0$ и $\sum_x p_x = 1$. *Относительная энтропия* неотрицательно определенного оператора A по отношению к неотрицательно определенному оператору B определяется как $S(A||B) \equiv \text{tr}(A \log A) - \text{tr}(A \log B)$.

Прочее

\oplus обозначает сложение по модулю два.

Часто используемые обозначения квантовых элементов и схем

Для унитарных операторов часто используются определенные условные обозначения, полезные при проектировании квантовых схем. Для удобства читателей многие из них приведены ниже. Строки и столбцы унитарных преобразований нумеруются слева направо и сверху вниз как $00\dots 0, 00\dots 1, \dots, 11\dots 1$; самый нижний провод соответствует самому младшему биту. Обратите внимание, что $e^{i\pi/4}$ есть корень квадратный из i , поэтому элемент $\pi/8$ представляет собой корень квадратный из фазового элемента, который, в свою очередь, является корнем квадратным из элемента Паули Z .

Элемент Адамара	\boxed{H}	$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Элемент Паули X	\boxed{X}	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Элемент Паули Y	\boxed{Y}	$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$

Элемент Паули Z



$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Фазовый элемент



$$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

Элемент $\pi/8$



$$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/8} \end{bmatrix}$$

Управляемый
NOT (CNOT)



$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Обмен



$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Управляемый- Z



$$=$$


$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

Управляемый
фазовый
элемент



$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{bmatrix}$$

Элемент
Тоффоли



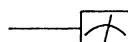
$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Элемент
Фредкина
(управляемый
обмен)

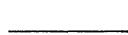
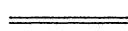
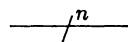


$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Измерение

Проекция на $|0\rangle$ и $|1\rangle$

Кубит

Провод, несущий один кубит
(время течет слева направо)Классический
битПровод, несущий один
классический бит n кубитовПровод, несущий n кубитов

Часть I

Фундаментальные принципы

Глава 1

ВВЕДЕНИЕ И ОБЩИЙ ОБЗОР

Наука несет в себе самую смелую метафизику эпохи. Она является чисто человеческим построением, движимым верой в то, что если мы порассуждаем, приложим усилия для открытия, объясним его и снова порассуждаем, тем самым раз за разом прорываясь на новую территорию, мир станет в чем-то понятнее и мы поймем истинную странность вселенной. И эта странность все обединит и будет иметь смысл.

Эдвард О. Вильсон

Информация материальна.

Рольф Ландауэр

Каковы фундаментальные принципы квантовых вычислений и квантовой информации? Как они развивались? Где их можно применить? Как они будут представлены в книге? Эта вводная глава предназначена для того, чтобы дать ответы на перечисленные вопросы, обрисовав в самых общих чертах область квантовых вычислений и квантовой информации. Наша задача состоит в том, чтобы познакомить читателя с основными понятиями данной области, показать, как они развивались, и помочь решить, как подходить к остальной части книги.

Мы начнем в разд. 1.1 с истории развития области квантовых вычислений и квантовой информации. В каждом из остальных разделов этой главы дается краткое изложение одного или нескольких фундаментальных вопросов рассматриваемой области: разд. 1.2 — квантовые биты; разд. 1.3 — квантовые

компьютеры, квантовые элементы и квантовые схемы, разд. 1.4 — квантовые алгоритмы, разд. 1.5 — экспериментальная обработка квантовой информации; разд. 1.6 — квантовая информация и связь.

В этой главе также описываются иллюстративные и легко доступные для понимания примеры, такие как квантовая телепортация и некоторые простые квантовые алгоритмы. При этом используется элементарная математика. Изложение является самодостаточным и задумано так, чтобы быть доступным даже при отсутствии подготовки в области информатики или физики. По мере изложения материала мы указываем на более развернутые обсуждения в последующих главах, где, в свою очередь, можно найти и рекомендации по дальнейшему чтению.

Если в процессе чтения вы начнете испытывать затруднения, пропускайте такие места, пока не почувствуете себя более комфортно. В некоторых местах мы не могли обойтись без использования профессионального языка, который будет полностью объяснен несколько позже. Пока просто примите это к сведению, а когда глубже поймете всю терминологию, вернитесь обратно. В этой главе акцент делается на общую картину, детализация которой будет проведена позже.

1.1 Глобальные перспективы

В области квантовых вычислений и квантовой информации изучаются задачи по обработке информации, которые могут быть выполнены с использованием квантовомеханических систем. Просто и очевидно, не так ли? Подобно тому, как было со многими простыми, но глубокими идеями, прошло довольно много времени, прежде чем кто-либо стал думать об обработке информации при помощи квантовомеханических систем. Чтобы понять, почему это произошло, мы должны вернуться в прошлое и последовательно рассмотреть каждую из областей, внесших фундаментальный вклад в квантовые вычисления и квантовую информацию: квантовую механику, информатику, теорию информации и криптографию. Чтобы получить некоторое представление о существенно различных направлениях, слившихся воедино в квантовых вычислениях и квантовой информации, вы должны на протяжении нашего короткого исторического обзора перечисленных областей последовательно представлять себя физиком, специалистом по информатике, по теории информации, и, наконец, криптографом.

1.1.1 История квантовых вычислений и квантовой информации

На рубеже девятнадцатого и двадцатого веков в науке назревала революция. В физике разразилась серия кризисов. Проблема состояла в том, что физические теории того времени (называемые сейчас *классической физикой*) предсказывали абсурдные результаты, например, существование «ультрафиолетовой катастрофы» с бесконечными энергиями, или неизбежность постепенного паде-

ния электронов на атомные ядра. Сначала такие проблемы разрешались путем введения в классическую физику специальных гипотез, но по мере того, как улучшалось понимание свойств атомов и излучения, выдвигаемые объяснения все более и более усложнялись. В начале 20-х гг. XX в. после четвертьвекового смятения кризис достиг своего пика и вылился в создание современной теории квантовой механики. С этого времени квантовая механика стала неотъемлемой частью науки и с невероятным успехом применялась ко всему, что находится под солнцем и внутри него, включая структуру атома, термоядерные реакции в звездах, сверхпроводники, структуру ДНК и элементарные частицы.

Что представляет собой квантовая механика? Квантовая механика — это математическая платформа, или совокупность правил, предназначенная для построения физических теорий. Например, существует физическая теория, известная как квантовая электродинамика, с фантастической точностью описывающая взаимодействие атомов со светом. Квантовая электродинамика построена на основе квантовой механики, но содержит специфические правила, не определяемые квантовой механикой. Связь квантовой механики с конкретными физическими теориями, например, с квантовой электродинамикой, в чем-то похожа на связь операционной системы компьютера с конкретной прикладной программой — операционная система задает некоторые базовые параметры и режимы работы, но не определяет, каким образом прикладные программы будут выполнять свои специфические задачи.

Принципы квантовой механики просты, но даже специалисты находят их противоречащими интуиции, истоки квантовых вычислений и квантовой информации можно усмотреть в постоянном желании физиков лучше понять квантовую механику. Самый известный критик квантовой механики Альберт Эйнштейн до конца жизни так и не примирился с теорией, которую сам же помог создать. Поколения физиков боролись с трудностями квантовой механики, пытаясь приспособить ее предсказания к человеческой интуиции. Одной из задач области квантовых вычислений и квантовой информации является разработка инструментов, которые развивали бы наше интуитивное понимание квантовой механики и делали ее предсказания более доступными для человеческого разума.

Например, в начале 80-х гг. ученых стало интересовать, можно ли использовать квантовые эффекты для передачи сигнала со скоростью, превышающей скорость света, что безоговорочно запрещено эйнштейновской теорией относительности. Решение этой проблемы свелось к выяснению того, можно ли копировать неизвестное квантовое состояние. Если бы копирование оказалось возможным, то при помощи квантовых эффектов можно было бы передавать сигнал со скоростью, превышающей скорость света. Однако копирование, столь легко выполнимое для классической информации, в общем случае оказывается невозможным в квантовой механике. Эта *теорема о невозможности копирования* (*no-cloning theorem*), сформулированная в начале 80-х гг., является одним из самых первых результатов в области квантовых вычислений и квантовой информации. С тех пор к ней было сделано много уточнений, и теперь у нас есть концептуальные инструменты, позволяющие понимать, насколько

хорошо может работать устройство (всегда несовершенное) квантового копирования. Эти инструменты, в свою очередь, были применены для понимания других аспектов квантовой механики.

Другое историческое направление, внесшее вклад в развитие квантовых вычислений и квантовой информации, зародилось в 70-х гг. в связи с интересом к *получению полного контроля над одиночными квантовыми системами*. В применениях квантовой механики до 70-х гг. обычно осуществлялся общий контроль над объемным образцом, содержащим невообразимое количество квантовомеханических систем, ни одна из которых не была доступна напрямую. Например, квантовая механика замечательно объясняет сверхпроводимость. Но поскольку сверхпроводник представляет собой огромный (по сравнению с атомными масштабами) образец проводящего металла, мы можем исследовать лишь немногие аспекты его квантовомеханической природы. При этом отдельные квантовые системы, составляющие сверхпроводник, остаются недоступными. Такие устройства, как ускорители частиц, позволяют получать ограниченный доступ к отдельным квантовым системам, но по-прежнему не дают полного контроля над элементарными системами.

Начиная с 70-х гг. было разработано много методов управления одиночными квантовыми системами. В качестве примера можно привести методы удержания одиночного атома в «атомной ловушке», обеспечивающие его изоляцию от всего остального мира и позволяющие с невероятной точностью исследовать различные аспекты его поведения. При помощи сканирующего туннельного микроскопа удается перемещать отдельные атомы, составляя из них заданные массивы. Были продемонстрированы электронные устройства, работа которых основана на переносе единичных электронов.

К чему все эти усилия, направленные на достижение полного контроля над одиночными квантовыми системами? Если оставить в стороне многочисленные технологические причины и сосредоточиться только на чистой науке, то главный ответ будет таков: исследователи действовали из интуитивных соображений. В науке самые глубокие озарения часто приходят тогда, когда разрабатывается метод для исследования новой области Природы. Например, появление радиоастрономии в 30–40-х гг. повлекло за собой ряд захватывающих открытий, в том числе ядра галактики Млечный Путь, пульсаров и квазаров. В физике низких температур достигнуты поразительные успехи в результате поиска способов понижения температур различных систем. Точно также, работая над проблемой получения полного контроля над одиночными квантовыми системами, мы исследуем нетронутую область Природы в надежде открыть новые, неожиданные явления. Сейчас мы делаем лишь первые шаги в этих направлениях и уже получили несколько интересных сюрпризов. Чего же можно ожидать, если мы добьемся более полного контроля над одиночными квантовыми системами и распространим его на более сложные системы?

Квантовые вычисления и квантовая информация естественным образом вписываются в эту программу. Они ставят ряд практических задач разных уровней сложности для людей, ищущих способы лучшего манипулирования одиночными квантовыми системами, стимулируют развитие новых экспери-

ментальных методик и показывают наиболее интересные направления, в которых нужно ставить эксперименты. И наоборот возможность управления одиночными квантовыми системами играет существенную роль, если мы хотим воспользоваться мощью квантовой механики применительно к квантовым вычислениям и квантовой информации.

Несмотря на большой интерес к рассматриваемой области, усилия по построению систем обработки квантовой информации дали на сегодняшний день скромные результаты. Современная техника для квантовых вычислений представлена маленькими квантовыми компьютерами, способными выполнять десятки операций над несколькими квантовыми битами (*кубитами*). Были продемонстрированы экспериментальные прототипы устройств для реализации *квантовой криптографии* — способа секретной связи на больших расстояниях — и даже на таком уровне, когда они могут быть полезны в некоторых реальных приложениях. Однако разработка технологий для реализации крупномасштабной обработки квантовой информации остается серьезной задачей для физиков и инженеров будущего.

Давайте перейдем от квантовой механики к еще одному великому интеллектуальному триумфу двадцатого столетия — информатике (computer science). Истоки информатики теряются в глубине веков. Например, клинописные таблички свидетельствуют, что во времена правления Хаммурапи (около 1750 г. до н. э.) вавилоняне разработали некоторые довольно сложные алгоритмы, и весьма вероятно, что многие идеи относятся к еще более ранним временам.

Начало современной информатики было положено великим математиком Алланом Тьюрингом в его выдающейся работе 1936 г. Тьюринг подробно описал абстрактное понятие, которое мы назвали бы сейчас программируемым компьютером, а именно, модель вычислений, впоследствии названную в его честь *машиной Тьюринга*. Он показал, что существует *универсальная машина Тьюринга*, которая может использоваться для моделирования любой другой машины Тьюринга. Более того, он утверждал, что его универсальная машина *полностью* отвечает на вопрос, что значит решать задачу алгоритмическими средствами. Иначе говоря, если алгоритм может быть выполнен на *любом физическом устройстве*, например, на современном персональном компьютере, то существует эквивалентный алгоритм для универсальной машины Тьюринга, который решает ту же самую задачу, что и алгоритм, выполняемый на персональном компьютере. Это утверждение, называемое *тезисом Чёрча-Тьюринга* (в честь Тьюринга и другого пионера информатики Алондо Черча), устанавливает эквивалентность между физическим понятием класса алгоритмов, выполнение которых возможно на *некотором физическом устройстве*, и строгим математическим понятием универсальной машины Тьюринга. Широкое признание этого тезиса положило начало развитию обширной теории информатики.

Вскоре после появления работы Тьюринга были построены первые компьютеры на электронных компонентах. Джон фон Нейман разработал простую теоретическую модель, объясняющую, как на практике собрать компьютер, обладающий всеми свойствами универсальной машины Тьюринга. Тем не ме-

нее, настоящая разработка аппаратного обеспечения началась только в 1947 г., когда Джон Бардин, Уолтер Браттейн и Уилл Шокли создали транзистор. С этого момента мощь компьютерного «железа» стала расти поразительными темпами. В 1965 г. Гордон Мур даже сформулировал закон этого роста, известный как *закон Мура*, согласно которому производительность компьютеров, обеспечиваемая при одной и той же цене, будет удваиваться примерно каждые два года.

Как это ни удивительно, закон Мура оставался приблизительно справедливым на протяжении десятилетий. Тем не менее, большинство наблюдателей ожидают, что этот сказочный рост прекратится где-то в районе первых двух десятилетий двадцать первого века. Традиционные подходы к разработке компьютерной технологии начинают упираться в фундаментальные трудности, связанные с размерами. По мере того, как электронные устройства становятся все меньше и меньше, в их функционирование постепенно вмешиваются квантовые эффекты.

Одним из возможных решений проблемы, связанной с прекращением действия закона Мура, является переход к другой вычислительной парадигме. Одна из таких парадигм предоставляется квантовой теорией вычислений, основанной на идее использования для выполнения вычислений квантовой механики, а не классической физики. Оказывается, что несмотря на возможность применения классического компьютера для моделирования квантового компьютера, *эффективное* осуществление такого моделирования невозможно. Таким образом, квантовые компьютеры существенно превосходят по скорости классические компьютеры. Это преимущество в скорости настолько значительно, что по мнению многих исследователей никакой мыслимый прогресс в классических вычислениях не поможет преодолеть разрыв в производительности между классическим и квантовым компьютерами.

Что имеется в виду под «эффективным» или «неэффективным» моделированием квантового компьютера? Многие ключевые понятия, необходимые для ответа на этот вопрос, фактически появились еще до того, как возникла идея квантового компьютера. В частности, понятия *эффективного* и *неэффективного* алгоритма обрели математическую точность в *теории сложности вычислений*. Грубо говоря, эффективным является алгоритм, время выполнения которого полиномиально зависит от объема решаемой задачи. Для выполнение неэффективного алгоритма, напротив, требуется сверхполиномиальное (обычно экспоненциальное) время. В конце 60-х и начале 70-х гг. было замечено, что машина Тьюринга обладает как минимум такой же эффективностью, как и любая другая модель вычислений, в том смысле, что задача, которая может быть эффективно решена в рамках некоторой модели вычислений, может быть эффективно решена и на машине Тьюринга путем использования машины Тьюринга для моделирования другой модели вычислений. Это наблюдение было сформулировано в виде усиленной версии тезиса Чёрча–Тьюринга:

Любой алгоритмический процесс может быть эффективно смоделирован на машине Тьюринга.

Усиление этой версии тезиса Чёрча–Тьюринга заключено в слове «эффективно». Если сильный тезис Чёрча–Тьюринга верен, то из него следует, что независимо от типа машины, используемой для выполнения алгоритмов, эта машина может быть эффективно смоделирована при помощи стандартной машины Тьюринга. Это важное усиление, поскольку оно подразумевает, что для анализа возможности эффективного выполнения данной вычислительной задачи мы можем ограничиться анализом машины Тьюринга.

Некоторые аргументы против сильного тезиса Чёрча–Тьюринга нашлись в области аналоговых вычислений. Уже после Тьюринга различные группы исследователей обнаружили, что некоторые типы аналоговых компьютеров могут эффективно решать задачи, не имеющие, по всей видимости, эффективного решения на машине Тьюринга. На первый взгляд такие аналоговые компьютеры нарушают сильную форму тезиса Чёрча–Тьюринга. К сожалению, если сделать реалистичные предположения о наличии шума в аналоговых компьютерах, то они окажутся неэффективными во всех известных реализациях и не смогут решать задачи, не имеющие эффективного решения на машине Тьюринга. Этот урок, состоящий в том, что при оценке эффективности модели вычислений необходимо учитывать влияние реального шума, стал одним из первых крупных вызовов, брошенных квантовым вычислениям и квантовой информации. Ответом на него стала разработка теории *кодов, исправляющих квантовые ошибки, и устойчивых к ошибкам квантовых вычислений*. Таким образом, в отличие от аналоговых вычислений квантовые вычисления в принципе допускают наличие конечного уровня шума, сохраняя свои вычислительные достоинства.

Первое серьезное возражение против сильного тезиса Чёрча–Тьюринга появилось в середине 70-х гг., когда Роберт Соловей и Волкер Штрассен показали, что проверить, является ли целое число простым или составным, можно с помощью *вероятностного алгоритма*. В тесте Соловея–Штрассена случайность использовалась как *существенная* часть алгоритма. Алгоритм не давал достоверного ответа на вопрос, является ли данное целое число простым или составным, определяя это лишь с некоторой *вероятностью*. Повторяя тест Соловея–Штрассена несколько раз, можно определить это почти наверняка. Нужно особо отметить, что во время появления теста Соловея–Штрассена не было известно какого-либо эффективного детерминированного алгоритма для проверки целых чисел на простоту.¹ Получалось, что компьютеры, имеющие доступ к генератору случайных чисел, могли эффективно выполнять вычислительные задачи, для которых не было эффективного решения на традиционной детерминированной машине Тьюринга. Это открытие послужило толчком к поиску других вероятностных алгоритмов, который полностью оправдал себя, приведя к созданию успешно развивающейся области исследований.

Вероятностные алгоритмы поставили под сомнение тезис Чёрча–Тьюринга, показав, что существуют эффективно решаемые задачи, которые, тем не менее, не могут быть эффективно решены на детерминированной машине Тьюринга.

¹ Такой алгоритм появился в июле 2002 г. — Прим. ред.

Впрочем, возникшее затруднение легко устраняется простой модификацией тезиса:

Любой алгоритмический процесс может быть эффективно смоделирован на вероятностной машине Тьюринга.

Эта модификация сильного тезиса Чёрча–Тьюринга должна оставлять чувство неудовлетворенности. Не может ли оказаться так, что через некоторое время еще какая-нибудь модель вычислений позволит эффективно решать задачи, не имеющие эффективного решения в рамках модели вычислений Тьюринга? Можно ли найти модель вычислений, которая бы эффективно моделировала любую другую модель вычислений?

Заинтересовавшись этим вопросом, Дэвид Дойч в 1985 г. решил выяснить, можно ли использовать законы физики для вывода еще более сильной версии тезиса Чёрча–Тьюринга. Вместо принятия специальных гипотез Дойч стал искать физическую теорию для обоснования тезиса Чёрча–Тьюринга, которое было бы столь же надежным, как и статус самой этой теории. В частности, Дойч попытался описать вычислительное устройство, которое было бы способно эффективно моделировать произвольную физическую систему. Поскольку законы физики в конечном счете являются квантовомеханическими, Дойч естественным образом пришел к рассмотрению вычислительных устройств, основанных на принципах квантовой механики. От этих устройств — квантовых аналогов машин, описанных Тьюрингом полвека назад — ведет свое начало концепция современного квантового компьютера, используемая в этой книге.

На момент написания книги еще не было ясно, достаточно ли универсального квантового компьютера Дойча для эффективного моделирования произвольной физической системы. Доказательство или опровержение этой гипотезы представляет собой одну из больших проблем в области квантовых вычислений и квантовой информации. Возможно, например, что некоторый эффект из квантовой теории поля или даже более эзотерический эффект, основанный на теории струн, квантовой гравитации или на какой-либо другой физической теории, может вывести нас за рамки универсального квантового компьютера Дойча, предоставив еще более мощную модель вычислений. На данном этапе мы этого просто не знаем.

Модель квантового компьютера Дойча позволила оспорить сильную форму тезиса Чёрча–Тьюринга. Дойч задался вопросом, может ли квантовый компьютер эффективно решать вычислительные задачи, не имеющие эффективного решения на классическом компьютере, даже если это вероятностная машина Тьюринга. Он построил простой пример, показывающий, что квантовые компьютеры действительно могут превосходить по вычислительной эффективности классические компьютеры.

Этот выдающийся первый шаг, сделанный Дойчем, в последующие десять лет был развит многими людьми. Кульминация этого развития пришла на 1994 г., когда Питер Шор продемонстрировал, что две исключительно важные задачи — поиск простых сомножителей целого числа и так называемая задача вычисления дискретного логарифма — могут быть эффективно решены на

квантовом компьютере. Это вызвало большой интерес, поскольку две указанные задачи считались (и по-прежнему считаются) эффективно неразрешимыми на классическом компьютере. Результаты Шора убедительно показывали, что квантовые компьютеры превосходят по производительности машины Тьюринга, включая их вероятностный вариант. Следующее доказательство эффективности квантовых компьютеров появилось в 1995 г., когда Лов Гровер показал, что выполнение другой важной задачи — проведения поиска в некотором неструктурированном поисковом пространстве — также может быть ускорено на квантовом компьютере. Правда, алгоритм Гровера не давал такого эффективного ускорения, как алгоритмы Шора, но ввиду широкого применения методологий, основанных на поиске, он вызвал значительный интерес.

Примерно в то же время, когда были открыты алгоритмы Шора и Гровера, многие разрабатывали идею Ричарда Фейнмана, высказанную им в 1982 г. Фейнман указал, что моделирование квантовомеханических систем на классических компьютерах сопряжено с существенными трудностями, и предположил, что построение компьютеров на основе принципов квантовой механики позволило бы этих трудностей избежать. В 90-х гг. несколько групп исследователей начали развивать эту идею, показав несомненную возможность использования квантовых компьютеров для эффективного моделирования систем, не имеющих какой-либо известной эффективной модели на классическом компьютере. Вероятно, в будущем одним из главных применений квантовых компьютеров станет моделирование квантовомеханических систем, слишком сложных для моделирования на классическом компьютере. Решение этой задачи требует глубоких научных и технологических разработок.

Какие еще задачи квантовые компьютеры могут решать быстрее, чем классические? Краткий ответ таков: мы не знаем. Разработать хороший квантовый алгоритм *трудно*. Пессимист может усмотреть причину в том, что квантовые компьютеры подходят только для уже известных применений. Мы придерживаемся другой точки зрения. Разработка алгоритмов для квантовых компьютеров трудна потому, что здесь приходится сталкиваться с двумя непростыми проблемами, которых нет при разработке алгоритмов для классических компьютеров. Во-первых, наша интуиция имеет корни в классическом мире. Если мы прибегнем к помощи этой интуиции при разработке алгоритмов, то алгоритмические идеи, к которым придет, будут классическими. Для создания хороших квантовых алгоритмов необходимо «отключить» классическую интуицию хотя бы на каком-то этапе процесса разработки, используя для достижения желаемого результата чисто квантовые эффекты. Во-вторых, недостаточно разработать алгоритм, который просто является квантовомеханическим. Этот алгоритм должен быть *лучше*, чем любой из существующих классических алгоритмов! Ведь может случиться так, что кто-то найдет алгоритм, использующий чисто квантовые аспекты квантовой механики, но этот алгоритм не будет представлять большого интереса из-за существования классических алгоритмов со сравнимой производительностью. Сочетание двух описанных проблем делает разработку новых квантовых алгоритмов многообещающей задачей для будущего.

Поставим вопрос еще шире: можно ли сделать какие-либо обобщения относительно производительности квантовых компьютеров по сравнению с классическими? Что именно делает квантовые компьютеры эффективнее классических, если, конечно, это на самом деле так? Задачи какого класса можно эффективно решать на квантовом компьютере и как этот класс соотносится с классом задач, эффективно решаемых на классическом компьютере? Одной из самых интригующих особенностей квантовых вычислений и квантовой информации является то, насколько мало известно об ответах на эти вопросы! Необходимость их лучшего понимания представляет собой великий вызов будущему.

Подойдя к переднему краю квантовых вычислений, давайте обратимся к истории другого направления мысли, внесшего вклад в квантовые вычисления и квантовую информацию: теории информации. В 40-х гг. одновременно со взрывным развитием информатики происходила революция в понимании связи (*communication*). В 1948 г. Клод Шенон опубликовал пару выдающихся работ, заложивших основы современной теории информации и связи.

Возможно, самый важный шаг, сделанный Шенном, состоял в *математическом определении понятия информации*. Во многих математических науках существует значительная гибкость в выборе фундаментальных определений. Попробуйте несколько минут подумать, исходя из самых обычных соображений, над следующим вопросом: как бы вы подошли к математическому определению понятия «источник информации»? Широкое распространение получили сразу *несколько* решений этой проблемы; однако определение Шенона оказалось гораздо более плодотворным в плане улучшения понимания. Его использование привело к получению целого ряда серьезных результатов и созданию обширной теории, которая, по всей видимости, адекватно отражает многие (хотя и не все) реальные проблемы связи.

Шенна интересовали два ключевых вопроса, относящихся к обмену информацией по каналу связи. Во-первых, какие ресурсы требуются для передачи информации по каналу связи? Например, телефонным компаниям нужно знать, сколько информации они могут надежно передать по данному телефонному кабелю. Во-вторых, может ли информация передаваться таким образом, чтобы она была защищена от шумов в канале связи?

Шенон ответил на два этих вопроса, доказав две фундаментальные теоремы теории информации. Первая из них — *теорема о кодировании для канала без шума* — определяет, какое количество физических ресурсов требуется для хранения выходных данных источника информации. Вторая фундаментальная теорема Шенона — *теорема о кодировании для канала с шумом* — определяет, какое количество информации можно надежно передать по каналу связи в присутствии шума. Шенон показал, что для достижения надежной передачи в присутствии шума можно использовать коды, исправляющие ошибки. Теорема Шенона о кодировании для канала с шумом устанавливает верхний предел защиты информации, обеспечиваемой кодами, исправляющими ошибки. К сожалению, теорема не дает явного вида кодов, при помощи которых можно было бы достичь этого предела на практике. С момента опубликования

работ Шеннона и до настоящего времени исследователи разрабатывают все новые и лучшие классы кодов, исправляющих ошибки, пытаясь приблизиться к пределу, установленному теоремой Шеннона. Существует сложная теория кодов, исправляющих ошибки, которая предлагает пользователю, желающему разработать хороший код, множество вариантов выбора. Такие коды широко применяются; они используются, например, в проигрывателях компакт-дисков, компьютерных модемах и спутниковых системах связи.

Квантовая теория информации развивалась похожим образом. В 1995 г. Бен Шумахер доказал аналог теоремы Шеннона о кодировании в отсутствие шума, по ходу дела определив «квантовый бит», или «кубит», как реальный физический ресурс. Однако до сих пор неизвестно никакого аналога теоремы Шеннона о кодировании для канала с шумом применительно к квантовой информации. Несмотря на это, по аналогии с классическими эквивалентами была разработана теория исправления квантовых ошибок, которая, как уже упоминалось, позволяет квантовым компьютерам эффективно проводить вычисления в присутствии шума, а также осуществлять надежную связь по *квантовым* каналам с шумом.

Классические идеи исправления ошибок оказались очень важными для разработки и понимания кодов, исправляющих квантовые ошибки. В 1996 г. независимо работавшие Роберт Калдербанк с Питером Шором и Эндрю Стин открыли важный класс квантовых кодов, называемых сейчас CSS-кодами, по первым буквам их фамилий. Впоследствии эти коды были отнесены к категории симплектических (стабилизирующих) кодов, независимо разработанных Робертом Калдербанком, Эриком Рейнсом, Питером Шором и Нейлом Слонуном, а также Даниэлем Готтесманом. Эти открытия, опирающиеся на основные идеи классической теории линейного кодирования, в значительной степени способствовали быстрому пониманию кодов, исправляющих квантовые ошибки, и их применению в области квантовых вычислений и квантовой информации.

Теория кодов, исправляющих квантовые ошибки, была разработана с целью защиты квантовых состояний от шума. А как насчет передачи обычной классической информации по квантовому каналу? Насколько эффективно это можно делать? В этой области было обнаружено несколько сюрпризов. В 1992 г. Чарльз Беннет и Стивен Уиснер объяснили, как передавать *два* классических бита информации путем передачи от отправителя к получателю только *одного* квантового бита. Это было названо *сверхплотным кодированием*.

Еще больший интерес представляют результаты в области *распределенных квантовых вычислений*. Представьте, что у вас есть два соединенных в сеть компьютера, на которых решается некоторая задача. Сколько передач по сети требуется для решения этой задачи? Недавно было показано, что квантовые компьютеры могут потребовать экспоненциально меньшего количества передач для решения определенных задач по сравнению с классическими сетевыми компьютерами! К сожалению, эти задачи пока не представляют особого интереса в реальных условиях, и имеют некоторые нежелательные технические ограничения. Важным вопросом, которым нужно заняться в области кванто-

вых вычислений и квантовой информации в будущем, является поиск практических важных задач, для которых распределенные квантовые вычисления имеют значительное преимущество над распределенными классическими вычислениями.

Но вернемся к теории информации. Эта теория начинается с изучения свойств одиночного канала связи. В приложениях мы часто имеем дело не с одним каналом связи, а с сетью из многих каналов. Свойства таких сетей, относящиеся к передаче информации, изучаются в *сетевой теории информации*, которая развила в обширную и сложную науку.

Сетевая квантовая теория информации, напротив, во многом еще только зарождается. Мы очень мало знаем даже о возможностях передачи информации по сетям квантовых каналов. В последние несколько лет был получен ряд довольно ошеломляющих предварительных результатов; однако единой сетевой теории информации для квантовых каналов пока не существует. Одного примера из этой области должно хватить, чтобы убедить вас в значимости такой общей теории. Предположим, что мы пытаемся передавать информацию от Алисы к Бобу по квантовому каналу с шумом. Если этот канал имеет нулевую пропускную способность для квантовой информации, то по нему нельзя надежно передавать никакую информацию. Теперь допустим, что мы рассматриваем две копии канала, работающие синхронно. С интуитивной точки зрения очевидно (и это можно строго доказать), что для квантовой информации такой канал также имеет нулевую пропускную способность. Но если мы изменим направление одного из каналов на обратное, как показано на рис. 1.1, то оказывается, что иногда можно получить ненулевую пропускную способность для передачи информации от Алисы к Бобу! Противоречащие интуиции свойства наподобие только что описанного иллюстрируют странную природу квантовой информации. Лучшее понимание возможностей передачи информации по сетям квантовых каналов представляет собой большую проблему в области квантовых вычислений и квантовой информации.

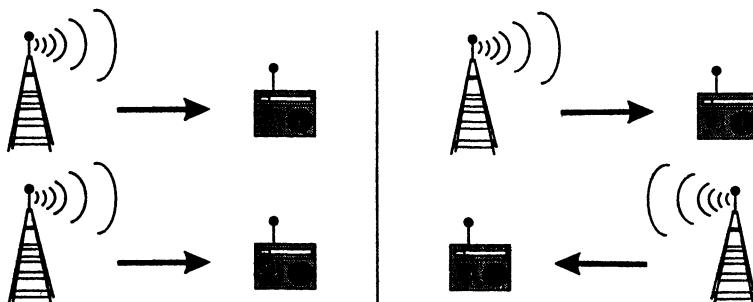


Рис. 1.1. Если в классическом случае мы имеем два канала с сильным шумом и нулевой пропускной способностью, работающих параллельно, то объединенный канал также имеет нулевую пропускную способность. Неудивительно, что если изменить направление одного из каналов на обратное, то мы по-прежнему будем иметь нулевую пропускную способность. В квантовомеханическом случае обращение одного из каналов с нулевой пропускной способностью может позволить нам передавать информацию!

Давайте сменим тему, обратившись к старому как мир искусству *криптографии*. Говоря в самых общих чертах, криптография решает проблему осуществления *связи* или *вычислений* с участием двух и более сторон, которые *не могут доверять друг другу*. Самая известная криптографическая проблема — это передача секретных сообщений. Предположим, что две стороны желают засекретить связь. Например, вы хотите передать продавцу номер своей кредитной карты в обмен на товары, причем так, чтобы этот номер не могла перехватить третья сторона. Это делается при помощи *криптографического протокола*. Далее в книге мы подробно опишем работу криптографических протоколов, а пока достаточно провести несколько простых разграничений. Наиболее важно понимать различие между *криптосистемами с секретным ключом (private key)* и *криптосистемами с открытым ключом (public key)*.

Работа криптосистемы с секретным ключом основана на том, что две стороны, Алиса и Боб, используют для связи *секретный ключ*, известный только им. Точный формат ключа сейчас не имеет значения; представьте себе строку нулей и единиц. Главное в том, что этот ключ используется Алисой для *шифрования* информации, которую она хочет послать Бобу. Зашифрованную информацию Алиса посыпает Бобу, который теперь должен восстановить исходную информацию. Как именно Алиса зашифрует сообщение — *зависит от секретного ключа*, поэтому для восстановления исходного сообщения Боб должен знать этот ключ, чтобы обратить примененное Алисой преобразование.

К сожалению, криптосистемы с секретным ключом имеют недостатки во многих отношениях. Наиболее фундаментальный вопрос — как распределять ключи? Проблема распределения ключей по своей сложности во многом аналогична исходной проблеме секретной связи — третья сторона может перехватить ключ, а затем использовать его для расшифровки передаваемых сообщений.

Одним из самых первых открытий в области квантовых вычислений и квантовой информации стал тот факт, что квантовая механика позволяет исключить нарушение конфиденциальности при распределении ключей. Соответствующая процедура известна как *квантовая криптография* или *квантовое распределение ключей*. Основная идея заключается в том, чтобы использовать квантовомеханический принцип, согласно которому наблюдение в общем случае возмущает наблюдаемую систему. Если злоумышленник попытается вести подслушивание во время передачи ключа между Алисой и Бобом, то его присутствие будет проявляться в виде возмущения канала связи, используемого Алисой и Бобом для согласования ключа. В таком случае Алиса и Боб могут отбросить биты ключа, принятые во время подслушивания, и начать все заново. Принципы квантовой криптографии были впервые предложены Стивеном Уиснером в конце 60-х гг., но, к сожалению, его работу не приняли к печати! В 1984 г. Чарльз Беннет и Джилльз Брассар, опираясь на более раннюю работу Уиснера, предложили квантовомеханический протокол распределения ключей, исключающий любую возможность их компрометации. С тех пор было предложено множество квантовых криптографических протоколов и разработано не меньшее количество их экспериментальных прототипов. На момент написания

книги эти прототипы почти достигли такого состояния, когда они могут быть полезны в реальных приложениях ограниченного масштаба.

Вторым важным типом криптосистем являются *криптосистемы с открытым ключом*. Эти криптосистемы не опираются на предварительную передачу секретного ключа между Алисой и Бобом. Вместо этого Боб просто публикует свой «открытый ключ», делая его доступным всем желающим. Алиса может воспользоваться этим открытым ключом для шифрования сообщения, посылаемого Бобу. Интересно, что при этом третья сторона *не может* использовать открытый ключ Боба для расшифровки сообщения! Точнее говоря, шифрующее преобразование выбирается настолько хитроумным и нетривиальным способом, что его *исключительно трудно* (хотя в принципе возможно) обратить, зная только открытый ключ. Чтобы обращение было простым для Боба, у него есть *секретный ключ*, соответствующий открытому ключу. Вместе эти ключи позволяют с легкостью выполнять расшифровку. Секретный ключ известен только Бобу, и это дает ему определенную степень уверенности, что никто другой не сможет прочитать сообщение Алисы. Действительно, вряд ли у кого-то окажется достаточно вычислительных ресурсов, чтобы обратить шифр только по открытому ключу. Таким образом, криптосистемы с открытым ключом решают проблему распределения ключей, делая ненужной передачу секретного ключа перед установлением связи.

Удивительно, что криптография с открытым ключом, которая произвела революцию в области криптографии, не получала широкого распространения до середины 70-х гг., когда она была независимо предложена Уитфилдом Диффи и Мартином Хеллманом, а также Ральфом Меркле. Немного позже Рональд Райвест, Ади Шамир и Леонард Эдельман разработали *криптосистему RSA*, которая на момент написания книги является наиболее распространенной криптосистемой рассматриваемого типа, превосходно сочетающей в себе безопасность и практичность. В 1997 г. выяснилось, что все это — криптография с открытым ключом, криптосистемы Диффи-Хеллмана и RSA — на самом деле было изобретено в конце 60-х и начале 70-х гг. исследователями из Британского разведывательного управления GCHQ.

Безопасность криптосистем с открытым ключом основана на том факте, что обращение стадии шифрования только при наличии открытого ключа в общем случае должно быть затруднительным. Например, оказывается, что задача обращения стадии шифрования RSA тесно связана с задачей факторизации. Предположение о безопасности RSA во многом обусловлено верой в то, что задачу факторизации трудно решить на классическом компьютере. Однако быстрый алгоритм факторизации на квантовом компьютере, разработанный Шором, мог бы использоваться для взлома RSA! Другие криптосистемы с открытым ключом также могли бы быть взломаны, если бы был известен быстрый классический алгоритм решения задачи о вычислении дискретного логарифма, подобный шоровскому квантовому алгоритму вычисления дискретного логарифма. Именно это практическое применение квантовых компьютеров — взлом криптографических кодов — в значительной степени стимулировало интерес к квантовым вычислениям и квантовой информации.

Выше мы рассматривали исторические корни квантовых вычислений и квантовой информации. Конечно, с ростом и развитием этой области из нее выделились самостоятельные подобласти исследований.

Возможно, наиболее поразительным из них является изучение *квантовой запутанности*. Запутанность — это уникальный квантовомеханический ресурс, который играет ключевую роль во многих наиболее интересных применениях квантовых вычислений и квантовой информации; это своего рода железо в бронзовом веке классического мира. Запутанность считается фундаментальным ресурсом Природы, сравнимым по важности с энергией, информацией, энтропией или любым другим фундаментальным ресурсом. В последние годы предпринимаются огромные усилия, направленные на лучшее понимание ее свойств. Хотя законченной теории запутанности пока нет, к настоящему времени удалось достичь некоторого прогресса в понимании этого странного понятия квантовой механики. Многие исследователи надеются, что дальнейшее изучение свойств запутанности даст сведения, которые будут способствовать разработке ее новых применений в области квантовых вычислений и квантовой информации.

1.1.2 Направления будущих исследований

Мы немного познакомились с историей и современным состоянием квантовых вычислений и квантовой информации. Что ждет нас в будущем? Что могут предложить квантовые вычисления и квантовая информация науке, технике и всему человечеству? Что нового дает эта область по сравнению с ее родительскими дисциплинами — информатикой, теорией информации и физикой? Каковы основные нерешенные проблемы? Перед тем, как переходить к более подробному описанию вычислений и квантовой информации, мы сделаем несколько очень коротких замечаний по этим глобальным вопросам.

Квантовые вычисления и квантовая информация научили нас думать о *вычислениях физически*, и мы обнаружили, что этот подход открывает много новых возможностей в области связи и обработки информации. Специалисты по информатике и теории информации получили новую плодотворную парадигму для исследований. Более того, фактически мы поняли, что *любая физическая теория*, а не только квантовая механика, может служить базисом для теории обработки информации и теории связи. В результате этих исследований однажды могут быть созданы устройства обработки информации, намного превосходящие по своим возможностям современные вычислительные и коммуникационные системы, что будет иметь свои положительные и отрицательные последствия для всего общества.

Конечно, квантовые вычисления и квантовая информация ставят перед физиками массу задач, но при этом не совсем понятно, что эта область предлагает физике в долгосрочной перспективе. Мы полагаем, что точно так же, как мы научились думать о *вычислениях физически*, мы можем научиться думать о физике в терминах вычислений. Физика традиционно является дисциплиной, где основное внимание сосредоточено на понимании «элементарных» объектов

и простых систем, однако многие интересные аспекты Природы проявляются лишь с ростом размеров и сложности. Такие явления отчасти исследуются в химии и инженерных науках, но всякий раз довольно специфическим образом. Квантовые вычисления и квантовая информация предоставляют новые инструменты, позволяющие перебрасывать мост от простого к относительно сложному: в сфере вычислений и алгоритмов есть систематические средства для построения и изучения таких систем. Применение идей из этих областей уже начинает приводить к выработке новых взглядов на физику. Мы надеемся, что в последующие годы этот подход будет успешно применяться во всех ее разделах.

Выше были кратко рассмотрены некоторые ключевые мотивации и идеи, лежащие в основе квантовых вычислений и квантовой информации. В остальной части этой главы будет дано более техническое, но по-прежнему доступное введение в эти мотивации и идеи в надежде сформировать у вас общее представление о рассматриваемой области в ее современном состоянии.

1.2 Квантовые биты

Бит – это фундаментальное понятие в области классических вычислений и классической информации. Квантовые вычисления и квантовая информация построены вокруг аналогичного понятия *квантового бита* (*quantum bit*), или для краткости *кубита* (*qubit*). В этом разделе мы описываем свойства одиночных кубитов и систем, состоящих из нескольких кубитов, сопоставляя их со свойствами классических битов.

Что такое кубит? Мы намерены описывать кубиты как *математические объекты* с некоторыми заданными свойствами. «Но постойте, — скажете вы, — ведь кубиты являются физическими объектами!» Действительно, кубиты, подобно битам, реализуются как физические системы, и в разд. 1.5 (а также в гл. 7) мы подробно расскажем, как осуществляется переход от абстрактного математического представления к реальным системам. Однако по большей части мы будем рассматривать кубиты как абстрактные математические объекты. Такой подход удобен тем, что предоставляет нам свободу при построении общей теории квантовых вычислений и квантовой информации, не зависящей от конкретной системы, используемой для ее реализации.

Так что же такое кубит? Аналогично классическому биту, который может находиться в *состоянии* 0 или 1, кубит также имеет *состояние*. Двумя возможными состояниями кубита являются $|0\rangle$ и $|1\rangle$, соответствующие, как можно догадаться, состояниям 0 и 1 классического бита. Символ $\langle|\rangle$ называется *директо́рским обозначением*, и мы будем часто с ним встречаться, поскольку это стандартное обозначение состояний в квантовой механике. Различие между битами и кубитами в том, что кубит может находиться в состоянии, отличном от $|0\rangle$ или $|1\rangle$. Можно составить *линейную комбинацию* состояний, часто называемую *суперпозицией*:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle. \quad (1.1)$$

Числа α и β являются комплексными, хотя для многих целей их можно без особого ущерба считать действительными. Иначе говоря, состояние кубита представляет собой вектор в двумерном комплексном векторном пространстве. Специальные состояния $|0\rangle$ и $|1\rangle$ называются *состояниями вычислительного базиса* и образуют ортонормированный базис этого векторного пространства.

Мы можем измерить бит, чтобы определить, находится ли он в состоянии 0 или 1. Например, компьютеры делают это каждый раз, когда считывают содержимое своей памяти. Но мы не можем измерить кубит, чтобы определить его квантовое состояние, т. е. значения α и β . Из квантовой механики следует, что можно получить лишь гораздо более ограниченную информацию о квантовом состоянии. При измерении кубита мы получаем либо результат 0 с вероятностью $|\alpha|^2$, либо результат 1 с вероятностью $|\beta|^2$. Разумеется, $|\alpha|^2 + |\beta|^2 = 1$, поскольку сумма вероятностей должна быть равна единице. Геометрически мы можем интерпретировать это как условие, что состояние кубита должно иметь единичную длину. Таким образом, в общем случае состояние кубита представляет собой единичный вектор в двумерном комплексном векторном пространстве.

Этот разрыв между ненаблюдаемым состоянием кубита и доступными нам наблюдениями лежит в основе квантовых вычислений и квантовой информации. В большинстве наших абстрактных моделей мира существует прямое соответствие между элементами абстракции и реальностью, точно так же, как планы архитектора по постройке здания соответствуют конечному результату строительства. Отсутствие такого прямого соответствия в квантовой механике затрудняет интуитивное понимание поведения квантовых систем. Однако существует непрямое соответствие: состояния кубита можно менять тем или иным способом, в результате чего данные измерений будут существенно зависеть от различных свойств состояния. Таким образом, наличие квантовых состояний приводит к реальным, экспериментально подтверждаемым следствиям, которые, как мы увидим, и определяют эффективность квантовых вычислений и квантовой информации.

Способность кубита находиться в состоянии суперпозиции противоречит нашим обыденным представлениям об окружающем физическом мире. Классический бит подобен монете: либо орел, либо решка. Для несовершенных монет возможны промежуточные состояния, например, балансирование на ребре, но в идеальном случае их можно отбросить. Кубит, напротив, до момента наблюдения может находиться в целом *континууме состояний* между $|0\rangle$ и $|1\rangle$. Подчеркнем еще раз, что измерение кубита всегда дает только 0 или 1 с некоторой вероятностью. Например, кубит может находиться в состоянии

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \quad (1.2)$$

измерение которого в половине случаев ($|1/\sqrt{2}|^2$) дает результат 0, а в другой половине случаев — результат 1. Мы будем часто возвращаться к этому состоянию, которое иногда обозначается как $|+\rangle$.

Несмотря на эту странность, реальность кубитов не вызывает сомнений.

Их существование и свойства были подтверждены многочисленными экспериментами (обсуждаемыми в разд. 1.5 и гл. 7). Для реализации кубитов можно использовать много различных физических систем. Чтобы получить конкретное представление о том, как это может быть сделано, полезно перечислить некоторые из возможных способов такой реализации: две разных поляризации фотона; направление ядерного спина в однородном магнитном поле; два состояния электрона в одиночном атоме, как показано на рис. 1.2. В модели атома электрон может существовать либо в так называемом основном, либо в возбужденном состоянии, которые мы будем обозначать как $|0\rangle$ и $|1\rangle$ соответственно. Облучая атом светом с подходящей энергией в течение некоторого времени, можно перевести электрон из состояния $|0\rangle$ в состояние $|1\rangle$ и наоборот. Но более интересно то, что сокращая время облучения можно оставить электрон, первоначально находившийся в состоянии $|0\rangle$, на полпути между $|0\rangle$ и $|1\rangle$ в состоянии $|+\rangle$.

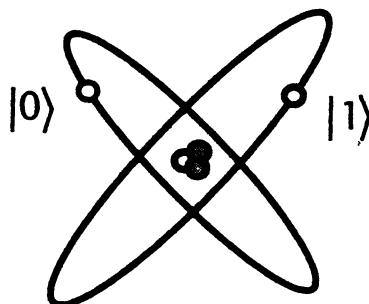


Рис. 1.2. Кубит, представленный двумя электронными уровнями в атоме.

Само собой разумеется, что интерпретации суперпозиции состояний, как и вероятностной природы наблюдений над квантовыми системами, уделялось много внимания. Однако в этой книге мы не будем касаться подобных дискуссий. Наша цель будет состоять в построении математических и концептуальных схем предикативного характера. Одной из схем, полезных при рассмотрении кубитов, является следующее геометрическое представление. Поскольку $|\alpha|^2 + |\beta|^2 = 1$, можно переписать формулу (1.1) в виде

$$|\psi\rangle = e^{i\gamma} \left(\cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle \right). \quad (1.3)$$

где θ , φ и γ — действительные числа. В гл. 2 будет показано, что множитель $e^{i\gamma}$ можно игнорировать, поскольку он не приводит к наблюдаемым эффектам, и по этой причине формула (1.3) фактически сводится к

$$|\psi\rangle = \left(\cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle \right). \quad (1.4)$$

Числа θ и φ задают точку на единичной трехмерной сфере, как показано на рис. 1.3. Эта сфера часто называется *сферой Блоха*; она позволяет наглядно представлять состояние одиночного кубита и часто служит в качестве превосходного «испытательного стенда» для идей из области квантовых вычислений и квантовой информации. Многие операции над одиночными кубитами, рассматриваемые далее в этой главе, изящно описываются с использованием сферы Блоха. Однако, нужно иметь в виду, что возможности этого представления ограничены, так как не известно простого обобщения сферы Блоха на случай нескольких кубитов.

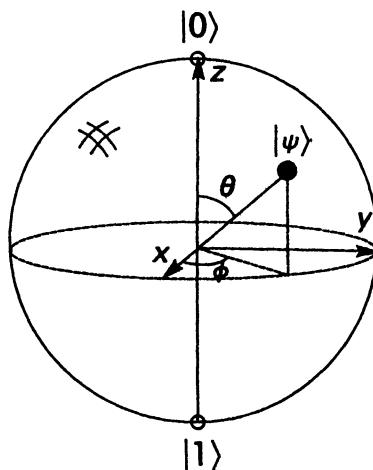


Рис. 1.3. Представление кубита при помощи сферы Блоха.

Сколько информации представляет кубит? Как ни парадоксально, на единичной сфере бесконечное количество точек, поэтому в принципе можно хранить все тексты Шекспира в бесконечном двоичном разложении θ . Однако этот вывод оказывается обманчивым из-за поведения кубита при наблюдении. Вспомните, что измерение кубита дает только 0 или 1. Более того, измерение *меняет* состояние кубита — он колапсирует из суперпозиции $|0\rangle$ и $|1\rangle$ в определенное состояние, соответствующее результату измерения. Например, если измерение $|+\rangle$ дает 0, то после измерения кубит останется в состоянии $|0\rangle$. Почему происходит этот коллапс — никто не знает. Как обсуждается в гл. 2, такое поведение является просто одним из *фундаментальных постулатов* квантовой механики. Для наших целей важно то, что одно измерение дает только один бит информации о состоянии кубита, разрешая тем самым кажущийся парадокс. Определить же коэффициенты α и β для состояния кубита, заданного формулой (1.1), можно только путем измерения бесконечного множества одинаково подготовленных кубитов.

Еще более интересным может быть следующий вопрос: сколько информации представляет кубит, *если мы не измеряем его?* Ответить на него не так

просто, поскольку нельзя определить количество информации, не выполняя соответствующего измерения. Тем не менее, здесь есть принципиально важный момент. Когда Природа реализует эволюцию замкнутой квантовой системы, не выполняя никаких «измерений», она, по-видимому, следит за всеми непрерывными переменными, описывающими состояние (такими, как α и β). Можно сказать, что в состоянии кубита Природа прячет массу скрытой информации. Еще более интересно то, что потенциальный объем этой дополнительной информации, как мы скоро увидим, экспоненциально растет с увеличением числа кубитов. Понимание этой скрытой *квантовой информации* является той задачей, которую мы пытаемся решать на протяжении значительной части книги; это ключевой момент в вопросе о том, что же именно делает квантовую механику столь эффективным инструментом обработки информации.

1.2.1 Несколько кубитов

В гильбертовом пространстве много места.

Карлтон Кэйвз

Предположим, что у нас есть два кубита. Будь это классические биты, для них существовало бы четыре возможных состояния: 00, 01, 10 и 11. Подобно этому, система двух кубитов имеет четыре *состояния вычислительного базиса*, обозначаемых как $|00\rangle$, $|01\rangle$, $|10\rangle$ и $|11\rangle$. Пара кубитов также может находиться в суперпозициях этих четырех состояний, поэтому для описания квантового состояния такой системы требуется сопоставить каждому состоянию вычислительного базиса комплексный коэффициент, иногда называемый *амплитудой*. В итоге вектор состояния, описывающий два кубита, имеет вид

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle. \quad (1.5)$$

Подобно случаю одиночного кубита, результат измерения x ($= 00, 01, 10$ или 11) встречается с вероятностью $|\alpha_x|^2$ и после измерения кубиты остаются в состоянии $|x\rangle$. Требование, чтобы сумма вероятностей равнялась единице, выражается условием *нормировки* $\sum_{x \in [0,1]^2} |\alpha_x|^2 = 1$, где $«[0,1]^2»$ обозначает множество строк из двух символов, где каждый символ является либо нулем, либо единицей. Для системы двух кубитов мы могли бы измерять только подмножество кубитов, скажем, первый кубит. Возможно, вы догадались, как это работает: при измерении только первого кубита получается 0 с вероятностью $|\alpha_{00}|^2 + |\alpha_{01}|^2$, а система переходит в состояние

$$|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}. \quad (1.6)$$

Обратите внимание, что состояние после измерения *перенормировано* на коэффициент $\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}$, поэтому оно по-прежнему удовлетворяет условию нормировки, как и следует ожидать для допустимого квантового состояния.

Важным частным случаем состояния двух кубитов является состояние Белла, или ЭПР-пара,

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}. \quad (1.7)$$

Это безобидное на первый взгляд состояние ответственно за многие сюрпризы в области квантовых вычислений и квантовой информации. Оно играет ключевую роль в квантовой телепортации и сверхплотном кодировании, которые обсуждаются в подразд. 1.3.7 и разд. 2.3 соответственно, и является прототипом многих других интересных квантовых состояний. Для состояния Белла характерно то, что при измерении первого кубита возможны два результата: 0 с вероятностью $1/2$ и конечным состоянием $|\varphi'\rangle = |00\rangle$, и 1 с вероятностью $1/2$ и конечным состоянием $|\varphi'\rangle = |11\rangle$. Как следствие, измерение второго кубита всегда дает тот же результат, что и измерение первого кубита, т. е. данные измерений оказываются *коррелированными*. Над состоянием Белла можно выполнять измерения и других типов, применяя сначала некоторые операции к первому или второму кубиту, и эта любопытная корреляция между результатами измерения первого и второго кубитов по-прежнему будет существовать. Эти корреляции вызывают большой интерес с момента появления известной работы Эйнштейна, Подольского и Розена (ЭПР), в которой было впервые указано на странные свойства состояний наподобие белловского. Идеи ЭПР были подхвачены и значительно развиты Джоном Беллом, доказавшим потрясающий факт: корреляция измерений в состоянии Белла *сильнее любой корреляции, которая может существовать между какими-либо классическими системами*. Эти результаты, подробно описанные в разд. 2.6, были первым указанием на то, что квантовая механика позволяет обрабатывать информацию принципиально иначе, чем в классическом мире.

В более общем случае мы можем рассмотреть систему из n кубитов. Состояния вычислительного базиса этой системы имеют вид $|x_1x_2\dots x_n\rangle$, а ее квантовое состояние характеризуется 2^n амплитудами. Для $n = 500$ это больше, чем оцениваемое количество атомов во вселенной! Ни на каком мыслимом классическом компьютере невозможно сохранить все эти комплексные числа. В гильбертовом пространстве поистине много места. Однако Природа в принципе манипулирует такими невообразимыми объемами данных даже для систем, содержащих лишь несколько сотен атомов. Она как бы держит у себя 2^{500} скрытых черновиков, на которых выполняет вычисления по мере эволюции системы. Было бы очень хорошо воспользоваться этой потенциально огромной вычислительной мощью. Но как состыковать квантовую механику и вычисления?

1.3 Квантовые вычисления

Изменения, происходящие с квантовым состоянием, можно описать на языке *квантовых вычислений*. Аналогично тому, как классический компьютер строится из электрических схем, содержащих провода и логические элементы, квантовый компьютер строится из *квантовых схем*, которые состоят из проводов и

элементарных квантовых элементов, позволяющих передавать квантовую информацию и манипулировать ею. В этом разделе мы опишем некоторые простейшие квантовые элементы и приведем несколько примеров схем, иллюстрирующих их применение, включая схему для телепортации кубитов!

1.3.1 Однокубитовые элементы

Схемы классических компьютеров состоят из *проводов (wires)* и *логических элементов (gates)*. Провода используются для передачи информации, тогда как логические элементы выполняют манипуляции с этой информацией, преобразуя ее из одного вида в другой. Рассмотрим, например, классические однобитовые логические элементы. Единственным нетривиальным членом этого класса является элемент NOT. Его функционирование определяется *таблицей значений (truth table)*, в которой $0 \rightarrow 1$ и $1 \rightarrow 0$, т. е. состояния 0 и 1 обмениваются.

Можно ли определить для кубитов аналогичный квантовый элемент NOT? Допустим, что у нас есть некоторый процесс, который переводит состояние $|0\rangle$ в состояние $|1\rangle$ и наоборот. Очевидно, что такой процесс был бы хорошим кандидатом на роль квантового аналога элемента NOT. Однако указание действия элемента на состояния $|0\rangle$ и $|1\rangle$ ничего не говорит о том, что происходит с суперпозициями этих состояний. Нужны дополнительные сведения о свойствах квантовых элементов. На самом деле квантовый элемент NOT действует линейно, т. е. переводит состояние

$$\alpha|0\rangle + \beta|1\rangle \quad (1.8)$$

в соответствующее состояние, где $|0\rangle$ и $|1\rangle$ поменялись ролями:

$$\alpha|1\rangle + \beta|0\rangle. \quad (1.9)$$

Почему квантовый элемент NOT действует линейно, а не каким-либо нелинейным образом — очень интересный вопрос, и ответ на него совершенно не очевиден. Оказывается, что это линейное поведение является одним из общих положений квантовой механики и имеет очень хорошее эмпирическое обоснование; нелинейное поведение, напротив, может приводить к явным парадоксам — путешествию во времени, передаче информации со скоростью, большей скорости света и нарушениям второго начала термодинамики. В следующих главах мы разберем этот вопрос подробнее, а пока просто примем сказанное как данность.

Существует удобный способ представления квантового элемента NOT в матричном виде, следующий непосредственно из линейности квантовых элементов. Определим матрицу X для представления квантового элемента NOT следующим образом:

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \quad (1.10)$$

(Обозначение X для квантового элемента NOT используется по историческим причинам.) Если квантовое состояние $\alpha|0\rangle + \beta|1\rangle$ записано в векторном виде

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix}, \quad (1.11)$$

где верхний элемент соответствует амплитуде для $|0\rangle$, а нижний — амплитуде для $|1\rangle$, то на выходе квантового элемента NOT будет

$$X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}. \quad (1.12)$$

Обратите внимание, что действие элемента NOT состоит в замене состояния $|0\rangle$ на состояние, соответствующее первому столбцу матрицы X . Аналогично этому, состояние $|1\rangle$ заменяется на состояние, соответствующее второму столбцу матрицы.

Итак, квантовые элементы на одном кубите могут быть описаны матрицами размера 2×2 . Существуют ли какие-нибудь ограничения на матрицы, которые могут использоваться для описания квантовых элементов? Оказывается, да. Вспомните, что условие нормировки требует выполнения равенства $|\alpha|^2 + |\beta|^2 = 1$ для квантового состояния $\alpha|0\rangle + \beta|1\rangle$. То же самое должно быть справедливо и для квантового состояния $|\psi'\rangle = \alpha'|0\rangle + \beta'|1\rangle$ после действия квантового элемента. Как оказывается, нужное условие на матрицу U , описывающую однокубитовый элемент, состоит в том, что матрица должна быть *унитарной*, т. е. $U^\dagger U = I$, где U^\dagger — сопряженная матрица (получаемая транспонированием и последующим комплексным сопряжением U), а I — единичная матрица 2×2 . Например, для элемента NOT легко убедиться, что $U^\dagger U = I$.

Удивительно, но это ограничение *унитарности* является *единственным* ограничением на квантовые элементы. Любая унитарная матрица описывает физически возможный квантовый элемент! Интересным следствием является то, что в отличие от классического случая, где существует только один нетривиальный однобитовый элемент NOT, нетривиальных однокубитовых элементов может быть много. Два важных квантовых элемента, которые мы будем использовать далее — это элемент Z

$$Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \quad (1.13)$$

оставляющий $|0\rangle$ без изменений и переводящий $|1\rangle$ в $-|1\rangle$, и элемент Адамара

$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \quad (1.14)$$

Элемент Адамара иногда характеризуют как своего рода «корень квадратный из NOT», поскольку он переводит состояние $|0\rangle$ в $(|0\rangle + |1\rangle)/\sqrt{2}$ (первый столбец H), оставляя на «полпути» между $|0\rangle$ и $|1\rangle$, а состояние $|1\rangle$ в $(|0\rangle - |1\rangle)/\sqrt{2}$

(второй столбец H), что также находится на «полпути» между $|0\rangle$ и $|1\rangle$). Заметим, однако, что H^2 не является элементом NOT, поскольку из простых алгебраических соображений следует, что $H^2 = I$, и следовательно, двукратное применение H к любому состоянию никак его не меняет.

Элемент Адамара является одним из самых полезных квантовых элементов, поэтому стоит попытаться наглядно представить его работу, обратившись к сфере Блоха. Оказывается, что здесь действия однокубитовых элементов соответствуют вращениям сферы. Операция Адамара — это вращение сферы вокруг оси y на 90° с последующим вращением относительно оси $x - y$ на угол 180° , как показано на рис. 1.4. На рис. 1.5 показаны некоторые важные однокубитовые элементы в сравнении с классическим случаем.

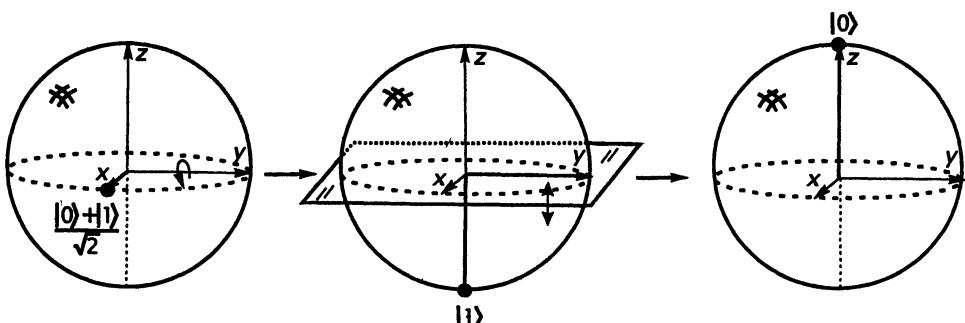


Рис. 1.4. Наглядное представление элемента Адамара, действующего на входное состояние $(|0\rangle + |1\rangle)/\sqrt{2}$, при помощи сферы Блоха

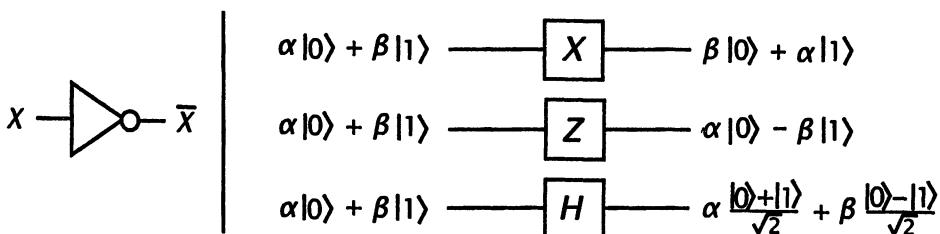


Рис. 1.5. Однобитовый (слева) и однокубитовые (справа) логические элементы

Существует бесконечно много унитарных матриц размера 2×2 , а, следовательно, бесконечно много однокубитовых элементов. Но оказывается, что для понимания свойств всего этого множества достаточно знать свойства намного меньшего множества. Например (см. вставку 1.1), произвольный однокубитовый унитарный элемент можно разложить на произведение вращений, описываемых матрицами вида

$$\begin{bmatrix} \cos \frac{\gamma}{2} & -\sin \frac{\gamma}{2} \\ \sin \frac{\gamma}{2} & \cos \frac{\gamma}{2} \end{bmatrix}, \quad (1.15)$$

и элемента, описываемого матрицей

$$\begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix}, \quad (1.16)$$

который, как мы поймем позже, представляет собой вращение вокруг оси z , в сочетании с (общим) фазовым сдвигом — постоянным множителем вида $e^{i\alpha}$. Эти элементы можно разлагать дальше — нет необходимости строить элементы с произвольными α , β и γ , достаточно построить сколь угодно точное приближение к таким элементам, используя лишь несколько элементов со специальными фиксированными значениями α , β и γ . В этом случае можно построить произвольный однокубитовый элемент, используя конечный набор квантовых элементов. Справедливо и более общее утверждение: произвольное квантовое вычисление над любым количеством кубитов можно осуществить при помощи конечного универсального набора элементов. Для получения такого набора элементов мы должны в первую очередь ввести некоторые квантовые элементы, оперирующие с несколькими кубитами.

Вставка 1.1. Разложения однокубитовых операций

В разд. 4.2 доказывается, что произвольная унитарная матрица 2×2 может быть представлена в виде разложения

$$U = e^{i\alpha} \begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix} \begin{bmatrix} \cos \frac{\gamma}{2} & -\sin \frac{\gamma}{2} \\ \sin \frac{\gamma}{2} & \cos \frac{\gamma}{2} \end{bmatrix} \begin{bmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{bmatrix}, \quad (1.17)$$

где α , β , γ и δ — действительные числа. Заметьте, что вторая матрица представляет обычное вращение. Первая и последняя матрицы также описывают вращения, но в другой плоскости. Это разложение можно использовать для точного описания произвольного однокубитового квантового логического элемента.

1.3.2 Многокубитовые элементы

Теперь проведем обобщение на случай нескольких кубитов. На рис. 1.6 показаны пять классических логических элементов, заслуживающих внимания: AND (И), OR (ИЛИ), XOR (исключающее ИЛИ), NAND (НЕ-И) и NOR (НЕ-ИЛИ). Существует важный теоретический результат, который заключается в том, что любая функция от битов может быть вычислена путем комбинирования одних лишь элементов NAND.² По этой причине данный элемент называется *универсальным*. В отличие от него элемент XOR (даже в комбинации с NOT) не универсален.

Простейшим элементом на нескольких кубитах является элемент CNOT (controlled-NOT). Он имеет два входных кубита — *управляющий (control)* и *управляемый (target)*, соответственно. Условное обозначение CNOT показано

² Предполагается возможность копирования бита. — Прим. ред.

на рис. 1.6 справа вверху. Верхняя линия представляет управляющий, а нижняя — управляемый кубит. Функционирование этого элемента можно описать следующим образом. Если управляющий кубит установлен в 0, то управляемый кубит не меняется. Если управляющий кубит установлен в 1, то значение управляемого кубита меняется. Формальная запись:

$$|00\rangle \rightarrow |00\rangle, |01\rangle \rightarrow |01\rangle, |10\rangle \rightarrow |11\rangle, |11\rangle \rightarrow |00\rangle, \quad (1.18)$$

CNOT можно описать другим способом, а именно как обобщение классического элемента XOR, поскольку его действие можно представить как $|A, B\rangle \rightarrow |A, B \oplus A\rangle$, где \oplus обозначает сложение по модулю два — это то, что делает элемент XOR. Иначе говоря, управляющий и управляемый кубиты складываются по модулю два и результат сохраняется в управляемом кубите.

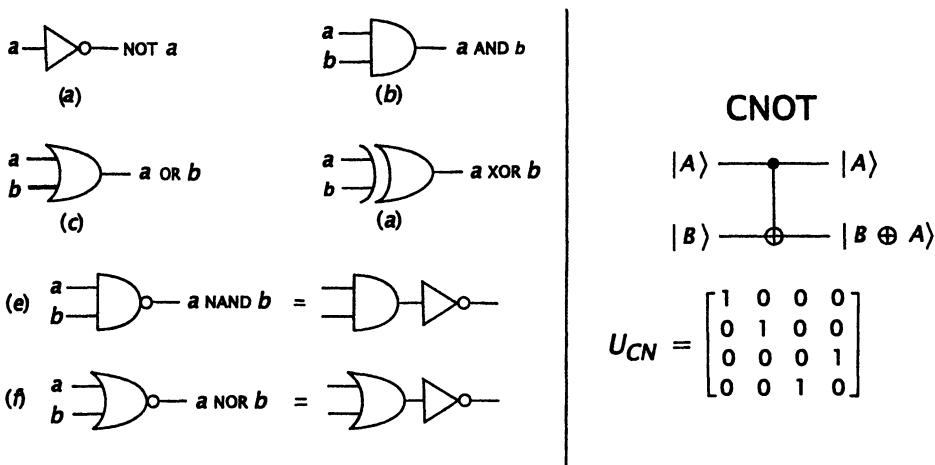


Рис. 1.6. Слева показаны некоторые стандартные одно- и многобитовые логические элементы, а справа — простейший элемент на нескольких кубитах, CNOT. Его матричное представление U_{CN} записано для амплитуд $|00\rangle, |01\rangle, |10\rangle$ и $|11\rangle$, расположенных именно в таком порядке.

Еще один способ описать действие CNOT — это дать его матричное представление, как показано на рис. 1.6 справа внизу. Вы можете легко убедиться, что первый столбец U_{CN} описывает преобразование, происходящее с $|00\rangle$, и выполнить такие же проверки для других состояний вычислительного базиса, $|01\rangle, |10\rangle$ и $|11\rangle$. Как и в случае одного кубита, требование сохранения вероятности выражено тем фактом, что U_{CN} является *унитарной матрицей*, т. е. $U_{CN}^\dagger U_{CN} = I$.

Мы отметили, что CNOT можно рассматривать как разновидность обобщенного элемента XOR. Допускают ли другие классические логические элементы, такие как NAND и обычный XOR, унитарную трактовку подобно тому, как квантовый элемент NOT представляет классический элемент NOT? Оказывается, нет. Причина в том, что элементы XOR и NAND принципиально *не обратимы*. Например, по выходному значению $A \oplus B$ элемента XOR невозможно

определить, каковы были входные значения A и B ; происходит безвозвратная потеря информации, обусловленная необратимым действием элемента XOR. Унитарные квантовые элементы всегда обратимы (по той причине, что обращение унитарной матрицы снова дает унитарную матрицу), и, следовательно, результат действия квантового элемента всегда может быть инвертирован другим квантовым элементом. Понимание того, как выполнять классические вычисления при условии обратимости станет решающим шагом в понимании того, как использовать возможности квантовой механики для вычислений. Мы объясним основную идею обратимых вычислений в подразд. 1.4.1.

Конечно, кроме элемента CNOT существует много других интересных квантовых элементов. Однако CNOT и однокубитовые элементы являются в некотором смысле прототипами всех остальных элементов в силу замечательной теоремы полноты: любой многокубитовый логический элемент может быть составлен из CNOT и однокубитовых элементов. Доказательство этого результата, являющегося квантовым аналогом утверждения об универсальности элемента NAND, приведено в разд. 4.5.

1.3.3 Измерения в базисах, отличных от вычислительного

Мы описали квантовое измерение одного кубита в состоянии $\alpha|0\rangle + \beta|1\rangle$ как получение результата 0 или 1 с переходом кубита в состояние $|0\rangle$ (с вероятностью $|\alpha|^2$) или $|1\rangle$ (с вероятностью $|\beta|^2$) соответственно. На самом деле класс возможных измерений в квантовой механике несколько шире, хотя, конечно, речь совсем не идет о том, чтобы восстанавливать α и β по одному измерению.

Заметим, что состояния $|0\rangle$ и $|1\rangle$ представляют собой лишь один из многих возможных наборов базисных состояний кубита. Другим возможным вариантом является набор $|+\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}$ и $|-\rangle \equiv (|0\rangle - |1\rangle)/\sqrt{2}$. Произвольное состояние $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ можно выразить через состояния $|+\rangle$ и $|-\rangle$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha \frac{|+\rangle + |-\rangle}{\sqrt{2}} + \beta \frac{|+\rangle - |-\rangle}{\sqrt{2}} = \frac{\alpha + \beta}{\sqrt{2}}|+\rangle + \frac{\alpha - \beta}{\sqrt{2}}|-\rangle. \quad (1.19)$$

Оказывается, что состояния $|+\rangle$ и $|-\rangle$ можно рассматривать так, как если бы они были состояниями вычислительного базиса, и выполнять измерения относительно этого нового базиса. Естественно, что измерение относительно базиса $|+\rangle, |-\rangle$ дает результат «+» с вероятностью $|\alpha + \beta|^2/2$ и результат «-» с вероятностью $|\alpha - \beta|^2/2$. Состояниями после измерения будут $|+\rangle$ и $|-\rangle$ соответственно.

В более общем случае произвольное состояние кубита можно выразить в виде линейной комбинации $\alpha|a\rangle + \beta|b\rangle$ любых базисных состояний $|a\rangle$ и $|b\rangle$. Более того, если состояния ортонормированы, то можно выполнять измерения относительно базиса $|a\rangle, |b\rangle$, получая результат a с вероятностью $|\alpha|^2$ и результат b с вероятностью $|\beta|^2$. Ограничение ортонормированности необходимо для того, чтобы $|\alpha|^2 + |\beta|^2 = 1$, как это и ожидается для вероятностей. В принципе, аналогичным образом можно проводить измерения над квантовой системой из нескольких кубитов относительно произвольного ортонормированного базиса.

Однако наличие принципиальной возможности не означает, что такое измерение можно легко осуществлять, и позже мы вернемся к вопросу о том, как эффективно проводить измерения в произвольном базисе.

Есть много причин для использования этого расширенного формализма квантовых измерений, но в конечном счете главной из них является следующая: этот формализм позволяет нам описывать наблюдаемые экспериментальные результаты, как мы увидим при обсуждении эксперимента Штерна-Герлаха в подразд. 1.5.1. Еще более сложный и удобный (но по существу эквивалентный) формализм для описания квантовых измерений рассматривается в следующей главе, в подразд. 2.2.3.

1.3.4 Квантовые схемы

Мы уже встречались с несколькими простыми квантовыми схемами. Рассмотрим элементы квантовых схем немного подробнее. На рис. 1.7 показана простая квантовая схема, содержащая три квантовых элемента. Схему следует читать слева направо. Каждая линия на схеме представляет провод квантовой схемы. Этот провод не обязательно соответствует физическому проводу; он может соответствовать течению времени или физической частице (например, фотону — частице света), перемещающейся в пространстве из одного места в другое. Традиционно предполагается, что входным состоянием схемы является одно из состояний вычислительного базиса, обычно состоящее из всех $|0\rangle$. В литературе по квантовым вычислениям и квантовой информации это правило часто нарушается, однако считается хорошим тоном информировать об этом читателя.

Схема на рис. 1.7 выполняет простую, но полезную задачу — обменивает состояния двух кубитов. Чтобы понять, как она это делает, обратите внимание, что данная последовательность элементов меняет состояние вычислительного базиса $|a, b\rangle$ следующим образом:

$$\begin{aligned} |a, b\rangle &\rightarrow |a, a \oplus b\rangle \\ &\rightarrow |a \oplus (a \oplus b), a \oplus b\rangle = |b, a \oplus b\rangle \\ &\rightarrow |b, (a \oplus b) \oplus b\rangle = |b, a\rangle, \end{aligned} \tag{1.20}$$

где все суммирования выполняются по модулю 2. Таким образом, результатом действия схемы является обмен состояний двух кубитов.

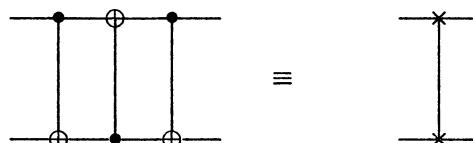


Рис. 1.7. Схема, обменивающая состояния двух кубитов, и ее условное обозначение

Существует ряд схемных решений, которые допустимы в классических схемах, но обычно отсутствуют в квантовых. Во-первых, не допускаются «циклы», т. е. обратная связь от одной части квантовой схемы к другой; говорят, что схема является *ациклической*. Во-вторых, в классических схемах разрешается «соединять» провода (операция FANIN) в один провод, который содержит побитовое OR входов. Очевидно, что эта операция необратима, а значит, неунитарна, поэтому мы не можем допускать ее в квантовых схемах. В-третьих, в квантовых схемах недопустима и обратная операция FANOUT, результатом которой являются несколько копий бита. Оказывается, что квантовая механика запрещает копирование кубита, делая операцию FANOUT вообще невозможной! Пример этого мы увидим в следующем разделе, когда попытаемся построить схему копирования кубита.

Далее по мере необходимости мы будем вводить новые квантовые элементы. А сейчас удобно ввести еще одно соглашение о квантовых схемах, которое иллюстрируется на рис. 1.8. Пусть U — произвольная унитарная матрица, действующая на некоторое количество кубитов n , так что ее можно рассматривать как квантовый элемент, оперирующий с этими кубитами. Тогда мы можем определить элемент управляемый- U , являющийся естественным расширением элемента CNOT. Такой элемент имеет один *управляющий кубит*, обозначаемый линией с черной точкой, и n *управляемых кубитов*, обозначаемых прямоугольником с буквой U . Если управляющий кубит установлен в 0, то с управляемыми кубитами ничего не происходит. Если же управляющий кубит установлен в 1, то к управляемым кубитам применяется элемент U . Примером элемента управляемый- U служит элемент CNOT, который представляет собой управляемый- U , где $U = X$ (рис. 1.9).

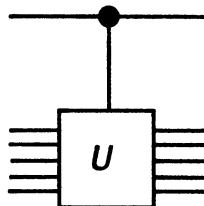


Рис. 1.8. Элемент управляемый- U .

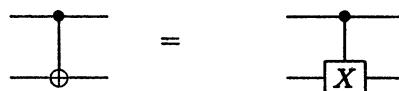


Рис. 1.9. Два различных представления элемента CNOT.

Другая важная операция — это измерение, которую мы представляем символом измерительного прибора (рис. 1.10). Как объяснялось выше, эта операция преобразует состояние одного кубита $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ в вероятностный

классический бит M (изображаемый двойной линией, чтобы отличать его от кубита), который имеет значение 0 с вероятностью $|\alpha|^2$ или 1 с вероятностью $|\beta|^2$.

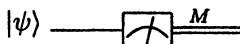


Рис. 1.10. Обозначение измерителя на квантовой схеме.

Как мы увидим, квантовые схемы оказываются полезными в качестве моделей всех квантовых процессов, в том числе (но не только) вычислений, связи и даже квантового шума. Это иллюстрируется несколькими простыми примерами, приведенными ниже.

1.3.5 Схема копирования кубита?

Элемент CNOT удобен для демонстрации одного фундаментального свойства квантовой информации. Рассмотрим задачу копирования классического бита. Это можно сделать при помощи классического элемента CNOT, который принимает на вход копируемый бит (в некотором неизвестном состоянии x) и бит-«заготовку», инициализированную нулем, как иллюстрируется на рис. 1.11. На выходе будут два бита, имеющие одинаковые состояния x .

Допустим, что мы пытаемся скопировать кубит в неизвестном состоянии $|\psi\rangle = a|0\rangle + b|1\rangle$ точно таким же образом, используя квантовый элемент CNOT. Состояние двух кубитов на входе можно записать как

$$[a|0\rangle + b|1\rangle]|0\rangle = a|00\rangle + b|10\rangle. \quad (1.21)$$

Функция CNOT инвертирует второй кубит, когда первый кубит равен 1, поэтому на выходе будет просто $a|00\rangle + b|11\rangle$. Удалось ли нам успешно скопировать $|\psi\rangle$? Иначе говоря, создали ли мы состояние $|\psi\rangle|\psi\rangle$? В случае, когда $|\psi\rangle = |0\rangle$ или $|\psi\rangle = |1\rangle$, это удается; квантовые схемы можно использовать для копирования классической информации, закодированной как $|0\rangle$ или $|1\rangle$. Однако, если взять состояние $|\psi\rangle$ в общем виде, то мы найдем, что

$$|\psi\rangle|\psi\rangle = a^2|00\rangle + ab|01\rangle + ab|10\rangle + b^2|11\rangle. \quad (1.22)$$

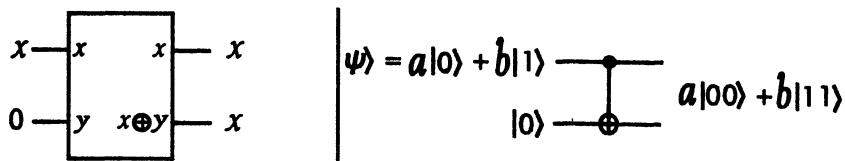


Рис. 1.11. Классическая и квантовая схемы «копирования» неизвестного бита или кубита.

Сравнивая это с $a|00\rangle + b|11\rangle$, мы видим, что кроме случая $ab = 0$ приведенная на рис.1.11 «схема копирования» не копирует входное квантовое состояние. Оказывается, что сделать копию неизвестного квантового состояния вообще *невозможно*. Это свойство (что кубиты нельзя копировать) известно как теорема о невозможности копирования; оно представляет собой одно из главных различий между квантовой и классической информацией. Более развернутое обсуждение теоремы о невозможности копирования приведено во вставке 12.1; доказательство очень простое, и мы советуем вам прочитать его прямо сейчас. Неудачу со схемой копирования, приведенной на рис. 1.11, можно объяснить и по-другому, исходя из интуитивного представления о том, что кубит содержит «скрытую» информацию, которую нельзя измерить непосредственно. Рассмотрим, что происходит при измерении одного из кубитов в состоянии $a|00\rangle + b|11\rangle$. Как говорилось выше, мы получаем 0 или 1 с вероятностью $|a|^2$ или $|b|^2$. Однако после измерения одного кубита состояние другого полностью определено и никакой дополнительной информации об a и b извлечь нельзя. Та дополнительная скрытая информация, которая присутствовала в исходном кубите $|\psi\rangle$, теряется при первом измерении и не может быть восстановлена. Но при копировании кубита состояние другого кубита должно по-прежнему содержать какую-то часть этой скрытой информации. Следовательно, копию кубита создать невозможно.

1.3.6 Пример: состояния Белла

Рассмотрим более сложную схему, показанную на рис. 1.12. Она содержит элемент Адамара с последующим CNOT и преобразует четыре состояния вычислительного базиса согласно приведенной таблице. Например, элемент Адамара переводит входное состояние $|00\rangle$ в $(|0\rangle + |1\rangle)|0\rangle/\sqrt{2}$, после чего CNOT формирует выходное состояние $(|00\rangle + |11\rangle)/\sqrt{2}$. Обратите внимание на то, как это работает: сначала преобразование Адамара переводит верхний кубит в состояние суперпозиции; затем эта суперпозиция поступает на управляющий вход CNOT, и управляемый кубит инвертируется только в том случае, когда значение управляющего кубита равно 1. Выходные состояния

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \quad (1.23)$$

$$|\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \quad (1.24)$$

$$|\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \quad (1.25)$$

$$|\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \quad (1.26)$$

называются *состояниями Белла*, а иногда — *ЭПР-состояниями*, или *ЭПР-парами*, в честь тех людей, которые первыми указали на странные свойства подоб-

ных состояний — Белла и Эйнштейна, Подольского, Розена. Мнемоническую запись $|\beta_{00}\rangle$, $|\beta_{01}\rangle$, $|\beta_{10}\rangle$ и $|\beta_{11}\rangle$ можно понять при помощи формулы

$$|\beta_{xy}\rangle = \frac{|0, y\rangle + (-1)^x|1, \bar{y}\rangle}{\sqrt{2}}, \quad (1.27)$$

где \bar{y} есть отрицание y .

Вход	Выход
$ 00\rangle$	$(00\rangle + 11\rangle)/\sqrt{2} \equiv \beta_{00}\rangle$
$ 01\rangle$	$(01\rangle + 10\rangle)/\sqrt{2} \equiv \beta_{01}\rangle$
$ 10\rangle$	$(00\rangle - 11\rangle)/\sqrt{2} \equiv \beta_{10}\rangle$
$ 11\rangle$	$(01\rangle - 10\rangle)/\sqrt{2} \equiv \beta_{11}\rangle$

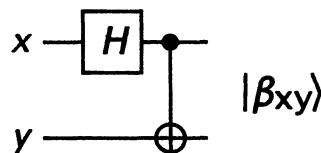


Рис. 1.12. Квантовая схема, создающая состояния Белла, и квантовая «таблица значений» для ее входных и выходных состояний.

1.3.7 Пример: квантовая телепортация

Сейчас мы применим понятия, описанные на нескольких предыдущих страницах, чтобы понять нечто нетривиальное, удивительное и весьма забавное — квантовую телепортацию! Квантовая телепортация — это технология передачи квантовых состояний из одного места в другое даже при отсутствии квантового канала связи между отправителем и получателем.

Квантовая телепортация работает следующим образом. Когда-то давно Алиса и Боб встречались, но теперь живут далеко друг от друга. Будучи вместе, они сгенерировали ЭПР-пару, и при расставании каждый взял по одному кубиту из этой пары. Много лет спустя Бобу приходится скрываться, и задача Алисы (если она согласится ее выполнять) в том, чтобы доставить Бобу кубит $|\psi\rangle$. Она не знает состояния кубита и более того может посыпать Бобу только *классическую* информацию. Стоит ли Алисе браться за эту задачу?

С интуитивной точки зрения для Алисы все выглядит довольно плохо. Она не знает состояния $|\psi\rangle$ кубита, который должна послать Бобу, и согласно законам квантовой механики не может определить это состояние, имея в своем распоряжении только одну копию $|\psi\rangle$. Еще хуже то, что даже если бы Алиса знала состояние $|\psi\rangle$, его точное описание потребовало бы бесконечного количества классической информации, поскольку $|\psi\rangle$ принимает значения в *непрерывном* пространстве. В результате ей пришлось бы описывать Бобу это состояние целую вечность. К счастью для Алисы, квантовая телепортация дает возможность использовать запутанную ЭПР-пару для посылки $|\psi\rangle$ Бобу, используя небольшое количество классической информации.

Схематически решение выглядит следующим образом: Алиса приводит кубит $|\psi\rangle$ во взаимодействие со своей половиной ЭПР-пары и затем измеряет два

имеющихся у нее кубита в базисе Белла, получая один из четырех возможных классических результатов — 00, 01, 10 и 11. Она посыпает эту информацию Бобу. В зависимости от классического сообщения Алисы Боб выполняет одну из четырех операций над своей половиной ЭПР-пары. Как ни удивительно, это позволяет ему восстановить исходное состояние $|\psi\rangle$!

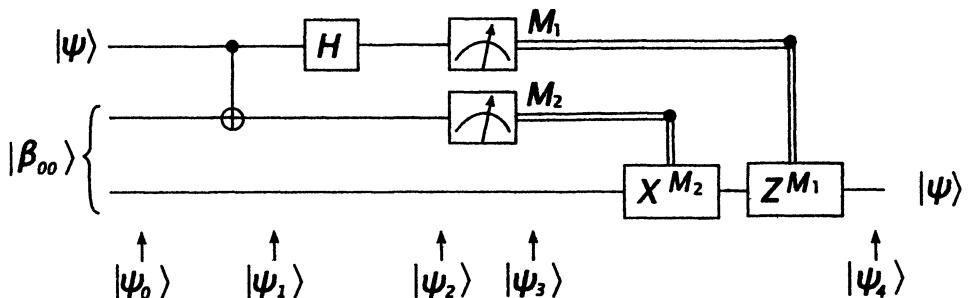


Рис. 1.13. Квантовая схема для телепортации кубита. Две верхние линии представляют систему Алисы, а нижняя линия — систему Боба. Выходящие из измерителей двойные линии несут классические биты (вспомните, что одинарные линии обозначают кубиты).

Квантовая схема, показанная на рис. 1.13, дает более точное представление о квантовой телепортации. Телепортируемым состоянием является $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, где α и β — неизвестные амплитуды. Состояние на входе схемы

$$|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle \quad (1.28)$$

$$= \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)], \quad (1.29)$$

где первые два кубита (слева) принадлежат Алисе, а третий кубит — Бобу. Как мы объясняли выше, второй кубит Алисы и кубит Боба первоначально находятся в ЭПР-состоянии. Алиса пропускает свои кубиты через элемент CNOT, получая

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)]. \quad (1.30)$$

Затем она, пропустив первый кубит через элемент Адамара, получит

$$|\psi_2\rangle = \frac{1}{2}[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)], \quad (1.31)$$

что, перегруппировав члены, можно переписать следующим образом:

$$|\psi_2\rangle = \frac{1}{2}[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)]. \quad (1.32)$$

Это выражение естественным образом распадается на четыре слагаемых. Первое слагаемое содержит кубиты Алисы в состоянии $|00\rangle$ и кубит Боба — в состоянии $\alpha|0\rangle + |1\rangle$, которое является исходным состоянием $|\psi\rangle$. Если Алиса выполняет измерение и получает результат $|00\rangle$, то система Боба будет в состоянии

$|\psi\rangle$). Таким образом, из приведенного выше выражения мы можем определить состояние кубита Боба после измерения, выполненного Алисой:

$$00 \rightarrow |\psi_3(00)\rangle \equiv [\alpha|0\rangle + \beta|1\rangle] \quad (1.33)$$

$$01 \rightarrow |\psi_3(01)\rangle \equiv [\alpha|1\rangle + \beta|0\rangle] \quad (1.34)$$

$$10 \rightarrow |\psi_3(10)\rangle \equiv [\alpha|0\rangle - \beta|1\rangle] \quad (1.35)$$

$$11 \rightarrow |\psi_3(11)\rangle \equiv [\alpha|1\rangle - \beta|0\rangle]. \quad (1.36)$$

В зависимости от исхода измерения Алисы кубит Боба окажется в одном из этих четырех возможных состояний. Конечно, чтобы знать, в каком состоянии находится кубит, Боб должен получить результат измерения Алисы. Далее мы покажем, что именно это обстоятельство не позволяет использовать телепортацию для передачи информации со скоростью, превышающей скорость света. Как только Боб узнает исход измерения, он может «подправить» состояние своего кубита и восстановить $|\psi\rangle$, применив подходящий квантовый элемент. Например, когда измерение дает 00, Бобу не нужно ничего делать. Если измерение дает 01, то Боб может скорректировать свое состояние, применив элемент X . Если измерение дает 10, то Боб может скорректировать свое состояние, применив элемент Z . Если измерение дает 11, то Боб может скорректировать свое состояние, применив сначала элемент X , а затем элемент Z . В общем случае Бобу нужно применить к этому кубиту преобразование $Z^{M_1} X^{M_2}$ (обратите внимание, что на схемах время идет слева направо, тогда как в матричных произведениях сомножители перемножаются справа налево); при этом он восстановит состояние $|\psi\rangle$.

Телепортация имеет много интересных свойств; позже мы вернемся к некоторым из них, а сейчас ограничимся двумя комментариями. Во-первых, не позволяет ли телепортация передавать квантовые состояния со скоростью, быстрее скорости света? Это было бы весьма странно, поскольку из теории относительности следует, что передача информации быстрее света могла бы использоваться для отправки информации в прошлое. К счастью, квантовая телепортация не дает возможности устанавливать сверхсветовую связь, поскольку для завершения телепортации Алисе необходимо передать результат своего измерения Бобу по классическому каналу связи. В подразд. 2.4.3 мы покажем, что без этой классической связи телепортация не переносит вообще никакой информации. Классический канал ограничен скоростью света, и, следовательно, квантовая телепортация не может осуществляться быстрее скорости света, что и разрешает кажущийся парадокс.

Второй парадокс телепортации состоит в том, что она, казалось бы, создает копию телепортируемого квантового состояния, тем самым нарушая теорему о невозможности копирования, обсуждавшуюся в подразд. 1.3.5. Но это нарушение кажущееся, так как по завершении процесса телепортации только управляемый кубит остается в состоянии $|\psi\rangle$, а исходный кубит данных оказывается в одном из состояний вычислительного базиса, $|0\rangle$ или $|1\rangle$, в зависимости от результата измерения первого кубита.

Чему нас может научить квантовая телепортация? Довольно многому! Она представляет собой гораздо больше, чем просто ловкий трюк, который можно проделывать с квантовыми состояниями. Квантовая телепортация подчеркивает взаимозаменяемость различных ресурсов в квантовой механике, показывая, что одна разделяемая ЭПР-пара вместе с двумя классическими битами связи является ресурсом, как минимум эквивалентным одному кубиту связи. Квантовые вычисления и квантовая информация выявили массу методов обмена ресурсами, многие из которых построены на квантовой телепортации. В частности, в гл. 10 мы объясним, как можно использовать телепортацию для построения квантовых элементов, устойчивых к воздействию шума, а в гл. 12 покажем, что телепортация тесно связана со свойствами кодов, исправляющих квантовые ошибки. Справедливости ради следует сказать, что несмотря на эти связи с другими дисциплинами, мы только начинаем понимать, *почему* в квантовой механике возможна квантовая телепортация; в последующих главах мы попытаемся разъяснить некоторые соображения, делающие возможным такое понимание.

1.4 Квантовые алгоритмы

Вычисления какого класса можно выполнять при помощи квантовых схем? Как этот класс соотносится с вычислениями, которые можно выполнять с использованием классических логических схем? Можно ли найти задачу, которую квантовый компьютер способен решать лучше, чем классический? В этом разделе мы исследуем перечисленные вопросы, объясняя, как выполняются классические вычисления на квантовых компьютерах, приводя некоторые примеры задач, для которых квантовые компьютеры имеют преимущества перед классическими, и характеризуя известные квантовые алгоритмы.

1.4.1 Классические вычисления на квантовом компьютере

Можно ли смоделировать классическую логическую схему при помощи квантовой схемы? Неудивительно, что ответ на этот вопрос оказывается положительным. Очень неожиданно было бы, окажись это не так, поскольку физики уверены, что все аспекты окружающего мира, включая классические логические схемы, могут быть в конечном счете объяснены квантовой механикой. Как отмечалось ранее, причина, по которой квантовые схемы не могут использоваться для непосредственного моделирования классических схем, состоит в том, что унитарные квантовые логические элементы по своей природе *обратимы*, тогда как многие классические логические элементы, такие как NAND, принципиально необратимы.

Любую классическую схему можно заменить эквивалентной схемой, содержащей только *обратимые* элементы, используя обратимый элемент, известный как элемент *Тоффоли*. Элемент Тоффоли имеет три входных и три выходных бита, как иллюстрируется на рис. 1.14. Два бита являются *управляющими*, и действие элемента их не меняет. Третий бит является *управляемым*; он ин-

вертируется, когда оба управляющих бита установлены в 1, и не меняется в противном случае. Заметьте, что двукратное применение элемента Тоффоли к набору битов дает $(a, b, c) \rightarrow (a, b, c \oplus ab) \rightarrow (a, b, c)$, и, следовательно, элемент Тоффоли обратим, поскольку имеет обратный элемент — самого себя.

Входы			Выходы		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

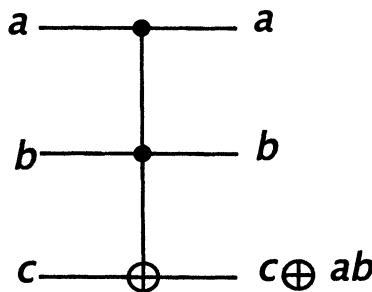


Рис. 1.14. Таблица значений для элемента Тоффоли и его условное обозначение

Элемент Тоффоли может применяться для моделирования элементов NAND (рис. 1.15), а также для выполнения операции FANOUT (рис. 1.16). Используя эти две операции, можно моделировать все остальные элементы классической схемы, и, следовательно, произвольная классическая схема может быть смоделирована эквивалентной обратимой схемой.

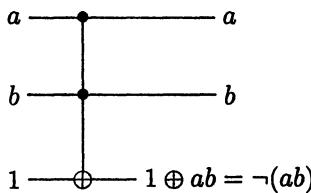


Рис. 1.15. Классическая схема, реализующая элемент NAND при помощи элемента Тоффоли. Два верхних бита представляют входы элемента NAND, а третий бит устанавливается в состоянии 1, иногда называемое вспомогательным состоянием (ancilla state). Выходом элемента NAND является третий бит.

Элемент Тоффоли был описан как классический элемент, но его можно реализовать и как квантовый элемент. По определению, квантовая реализация элемента Тоффоли просто меняет состояния вычислительного базиса таким же образом, как и классический элемент Тоффоли. Например, квантовый элемент Тоффоли, действующий на состояние $|110\rangle$, инвертирует третий кубит, поскольку первые два установлены в 1, что дает в результате $|111\rangle$. Это преобразование нетрудно (хотя и утомительно) записать в виде матрицы U размера

8×8 и явно проверить, что она унитарна, а, следовательно, элемент Тоффоли является допустимым квантовым элементом. Квантовый элемент Тоффоли, как и его классический вариант, можно использовать для моделирования необратимых классических логических элементов. Это означает, что квантовые компьютеры способны выполнять любые вычисления, которые возможны на классическом (детерминированном) компьютере.

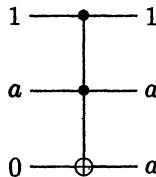


Рис. 1.16. Реализация FANOUT при помощи элемента Тoffоли. Второй бит — вход элемента FANOUT, два других бита вспомогательные. Выход элемента FANOUT — второй и третий биты.

А если классический компьютер — вероятностный, т. е. способен генерировать случайные биты для использования в вычислениях? Неудивительно, что квантовый компьютер может с легкостью моделировать и этот случай. Оказывается, что для такого моделирования достаточно производить случайные подбрасывания монеты, что может быть сделано путем приготовления кубита в состоянии $|0\rangle$, применения к нему элемента Адамара для получения $(|0\rangle + |1\rangle)/\sqrt{2}$ и последующего измерения состояния. Результатом будет $|0\rangle$ или $|1\rangle$ с вероятностью 50/50. Благодаря этому квантовый компьютер может эффективно моделировать вероятностный классический компьютер.

Конечно, если бы возможность моделирования классического компьютера была единственной отличительной чертой квантовых компьютеров, то не имело бы большого смысла решать все те проблемы, которые связаны с практическим использованием квантовых эффектов. Достоинство квантовых вычислений в том, что при использовании кубитов и квантовых элементов можно вычислять гораздо более сложные функции. В следующих нескольких разделах мы объясним, как это делается. Кульминационной точкой станет рассмотрение алгоритма Дойча-Йожа — нашего первого примера квантового алгоритма, способного решать задачу быстрее любого классического алгоритма.

1.4.2 Квантовый параллелизм

Квантовый параллелизм — это фундаментальное свойство многих квантовых алгоритмов. Если объяснить эвристически, рискуя слишком упростить ситуацию, то квантовый параллелизм позволяет квантовым компьютерам вычислять функцию $f(x)$ для многих различных значений x одновременно. В этом подразделе объясняется, как работает квантовый параллелизм и каковы некоторые из его ограничений.

Предположим, что $f(x) : 0,1 \rightarrow 0,1$ есть функция с однобитовой областью определения и однобитовым диапазоном значений. Чтобы понять, как эта

функция вычисляется на квантовом компьютере, удобно рассмотреть двухкубитовый квантовый компьютер, на вход которого подается состояние $|x, y\rangle$. С помощью подходящей последовательности логических элементов можно преобразовать это состояние в $|x, y \oplus f(x)\rangle$, где \oplus обозначает сложение по модулю 2. Первый регистр называется регистром данных, а второй — регистром значений. Обозначим преобразование, определяемое отображением $|x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$, как U_f , и заметим, что можно легко показать его унитарность. Если $y = 0$, то конечное состояние второго кубита есть просто значение $f(x)$. (В подразд. 3.2.5 мы покажем, что для данной классической схемы, вычисляющей f , существует квантовая схема со сравнимой эффективностью, выполняющая преобразование U_f на квантовом компьютере. Для наших целей ее можно рассматривать как черный ящик.)

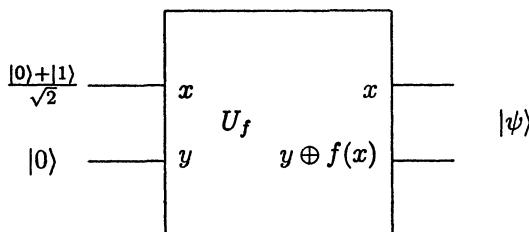


Рис. 1.17. Квантовая схема для одновременного вычисления $f(0)$ и $f(1)$. U_f — квантовая схема, которая преобразует входные данные вида $|x, y\rangle$ в $|x, y \oplus f(x)\rangle$.

Рассмотрим схему, показанную на рис. 1.17, которая применяет U_f к входному состоянию, не входящему в вычислительный базис. Регистр данных приготавливается в суперпозиции $(|0\rangle + |1\rangle)/\sqrt{2}$, которая может быть создана с помощью элемента Адамара, действующего на $|0\rangle$. Затем мы, применяя U_f , получаем состояние

$$\frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}. \quad (1.37)$$

Это замечательное состояние! Разные члены содержат информацию об $f(0)$ и $f(1)$; это почти то же самое, что вычислять $f(x)$ для двух значений x одновременно. Такая возможность называется «квантовым параллелизмом». В отличие от классического параллелизма, когда одновременно работает много схем вычисления $f(x)$, здесь используется одна схема $f(x)$, которая вычисляет функцию одновременно для многих значений x за счет способности квантового компьютера находиться в суперпозиции различных состояний.

Данную процедуру легко обобщить на функции от произвольного числа битов, используя обобщенную операцию, называемую *преобразованием Адамара* или иногда *преобразованием Уолша-Адамара*. Это просто n элементов Адамара, действующих параллельно на n кубитов. В качестве примера на рис. 1.18 показан случай $n = 2$ с кубитами, приготовленными в состоянии $|0\rangle$, что дает

$$\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}. \quad (1.38)$$

Запись $H^{\otimes 2}$ обозначает параллельное действие двух элементов Адамара, а « \otimes » — тензорное произведение. В более общем случае результатом выполнения преобразования Адамара над n кубитами, изначально находящимися в состоянии «все $|0\rangle$ », будет

$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle, \quad (1.39)$$

где суммирование проводится по всем возможным значениям x . Это действие мы обозначим как $H^{\otimes n}$. Иными словами, преобразование Адамара дает суперпозицию всех состояний вычислительного базиса с одинаковыми коэффициентами. Более того, оно делает это крайне эффективно, поскольку для получения суперпозиции 2^n состояний используется всего n элементов.

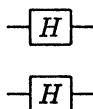


Рис. 1.18. Преобразование Адамара $H^{\otimes 2}$ над двумя кубитами.

Итак, квантовое параллельное вычисление функции $f(x)$ с n -битовым входом x и 1-битовым выходом может быть выполнено следующим образом. Приготавливаем $n + 1$ кубитов в состоянии $|0\rangle^{\otimes n}|0\rangle$, затем применяем к первым n кубитам преобразование Адамара, после чего задействуем квантовую схему, реализующую U_f . Это дает состояние

$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle|f(x)\rangle. \quad (1.40)$$

В некотором смысле квантовый параллелизм позволяет одновременно вычислять все возможные значения функции f , хотя, казалось бы, мы вычисляем f только один раз. Однако этим параллелизмом нельзя воспользоваться непосредственно. Измерение состояния в нашем примере с одним кубитом дает либо $|0, f(0)\rangle$, либо $|1, f(1)\rangle$! В общем случае измерение состояния $\sum_x |x, f(x)\rangle$ также дало бы $f(x)$ только для одного значения x . То же самое может легко сделать и классический компьютер! Чтобы от квантовых вычислений была польза, требуется несколько больше, чем просто квантовый параллелизм; нужно иметь возможность извлекать информацию о более чем одном значении $f(x)$ из суперпозиции состояний типа $\sum_x |x, f(x)\rangle$. В двух следующих подразделах мы рассмотрим примеры того, как это можно сделать.

1.4.3 Алгоритм Дойча

Чтобы продемонстрировать превосходство квантовых схем над классическими, достаточно немного модифицировать схему на рис. 1.17 с тем, чтобы реализовать алгоритм Дойча (на самом деле мы представляем упрощенный и

усовершенствованный вариант исходного алгоритма; см. разд. «История и дополнительная литература» в конце главы). В алгоритме Дойча квантовый параллелизм сочетается с таким явлением, как *интерференция*. Как и прежде, мы используем элемент Адамара для приготовления первого кубита в суперпозиции $(|0\rangle + |1\rangle)/\sqrt{2}$, но на этот раз приготовим второй кубит y как суперпозицию $(|0\rangle - |1\rangle)/\sqrt{2}$, применив элемент Адамара к состоянию $|1\rangle$. Проследим за состояниями, чтобы увидеть, что происходит в этой схеме, показанной на рис. 1.19.

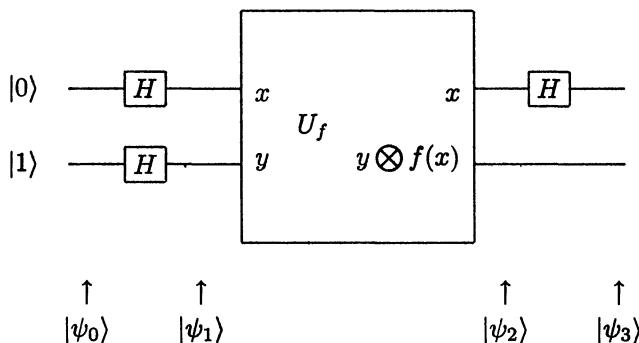


Рис. 1.19. Квантовая схема, реализующая алгоритм Дойча.

Входное состояние

$$|\psi_0\rangle = |01\rangle \quad (1.41)$$

пропускается через два элемента Адамара, что дает

$$|\psi_1\rangle = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right] \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]. \quad (1.42)$$

Простое рассуждение показывает, что если мы применим U_f к состоянию $|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$, то получим состояние $(-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$. Следовательно, применение U_f к $|\psi_1\rangle$ предоставляет нам две возможности:

$$\begin{aligned} |\psi_2\rangle &= \pm \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right] \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right], \text{ если } f(0) = f(1), \\ &= \pm \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right], \text{ если } f(0) \neq f(1). \end{aligned} \quad (1.43)$$

Таким образом, действие последнего элемента Адамара на первый кубит дает

$$\begin{aligned} |\psi_3\rangle &= \pm |0\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right], \text{ если } f(0) = f(1), \\ &= \pm |1\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right], \text{ если } f(0) \neq f(1). \end{aligned} \quad (1.44)$$

Учитывая, что $f(0) \oplus f(1)$ есть 0, если $f(0) = f(1)$, и 1 в противном случае, можно коротко переписать этот результат как

$$|\psi_3\rangle = \pm|f(0) \oplus f(1)\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right], \quad (1.45)$$

т. е. после измерения первого кубита мы можем узнать $f(0) \oplus f(1)$. Это весьма интересно: квантовая схема дала нам возможность определить *глобальное свойство* $f(x)$, а именно $f(0) \oplus f(1)$, при помощи только *одного* вычисления $f(x)$! Это быстрее, чем при использовании классического аппарата, где потребовалось бы как минимум два вычисления.

Данный пример подчеркивает различие между квантовым параллелизмом и классическими вероятностными алгоритмами. По наивности можно подумать, что состояние $|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle$ довольно близко соответствует результату работы вероятностного классического компьютера, который вычисляет $f(0)$ с вероятностью одна вторая или $f(1)$ с вероятностью одна вторая. Различие состоит в том, что для классического компьютера эти две альтернативы всегда являются взаимоисключающими, тогда как в квантовом компьютере они могут «*интерферировать*» друг с другом, что позволяет определить некоторое глобальное свойство функции f , используя нечто вроде элемента Адамара, как это было сделано в алгоритме Дойча. По сути, разработка многих квантовых алгоритмов сводится к хитроумному выбору функции и окончательного преобразования, позволяющих эффективно определять полезную глобальную информацию о функции — информацию, которую нельзя быстро получить на классическом компьютере.

1.4.4 Алгоритм Дойча-Йожа

Алгоритм Дойча — это простой частный случай более общего квантового алгоритма, который мы будем называть алгоритмом Дойча-Йожа. Решаемую им прикладную задачу, называемую задачей Дойча, можно описать как следующую игру. Алиса, находясь в Амстердаме, выбирает число x в интервале от 0 до $2^n - 1$ и посыпает его письмом Бобу в Бостон. Боб вычисляет некоторую функцию $f(x)$ и посыпает в ответ результат — либо 0, либо 1. При этом Боб обещает использовать функцию $f(x)$ одного из двух видов: либо *постоянную* для всех значений x , либо *сбалансированную*, т. е. равную 1 строго для половины всех возможных x и 0 для другой половины. Задача Алисы — достоверно определить, выбрал ли Боб постоянную или сбалансированную функцию, общаясь с ним как можно меньше. Как быстро она сможет достичь успеха?

В классическом случае Алиса может посыпать Бобу в каждом письме только одно значение x . При наихудшем развитии событий ей потребуется обратиться к Бобу не менее $2^n/2 + 1$ раз, поскольку она может получить $2^n/2$ нулей перед тем, как получит 1, что свидетельствует о сбалансированности функции Боба. Следовательно, наилучший детерминированный классический алгоритм, который она может использовать, требует $2^n/2 + 1$ запросов. Заметим, что в каждом письме Алиса посыпает Бобу n битов информации. Кроме того, в дан-

ном примере физическое расстояние используется для искусственного увеличения затрат на вычисление $f(x)$, но это не обязательно в задаче общего вида, где $f(x)$ сама по себе может быть сложной для вычисления.

Если бы Боб и Алиса могли обмениваться кубитами, а не только классическими битами, и если бы Боб согласился вычислять $f(x)$ с помощью унитарного преобразования U_f , то Алиса смогла бы достичь своей цели всего за один запрос к Бобу, используя описанный ниже алгоритм.

Как и в алгоритме Дойча, Алиса имеет n -кубитовый регистр для хранения своего запроса и однокубитовый регистр, который она предоставит Бобу для хранения ответа. Она начинает с приготовления своих регистров запроса и ответа в состоянии суперпозиции. Боб вычислит $f(x)$, используя квантовый параллелизм, и оставит результат в регистре ответа. Затем Алиса создаст интерференцию состояний суперпозиции, используя преобразование Адамара над регистром запроса, и закончит выполнением подходящего измерения, чтобы определить, была ли функция постоянной или сбалансированной.

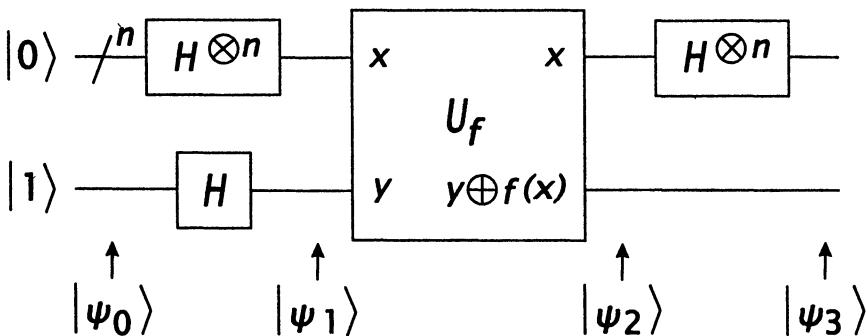


Рис. 1.20. Квантовая схема, реализующая обобщенный алгоритм Дойча-Йожа. Провод с наклонной чертой представляет набор из n кубитов по аналогии с общепринятыми техническими обозначениями.

Отдельные шаги алгоритма показаны на рис. 1.20. Давайте проследим за состояниями по этой схеме. Входное состояние

$$|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle \quad (1.46)$$

похоже на то, которое представлено формулой (1.41), но здесь регистр запроса описывает состояние n кубитов, каждый из которых приготовлен в состоянии $|0\rangle$. После преобразования Адамара над регистром запроса и применения элемента Адамара к регистру ответа мы имеем

$$|\psi_1\rangle = \sum_{x \in [0,1]^n} \frac{|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]. \quad (1.47)$$

Регистр запроса теперь содержит суперпозицию всех значений, а регистр ответа находится в равновзвешенной суперпозиции 0 и 1. Затем Боб вычисляет функцию f с помощью $U_f : |x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$, что дает

$$|\psi_2\rangle = \sum_x \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]. \quad (1.48)$$

Теперь у Алисы есть набор кубитов, в котором результат вычисления функции Боба сохранен в амплитуде суперпозиции. Далее она создает интерференцию членов суперпозиции, используя преобразование Адамара над регистром запроса. Чтобы определить результат преобразования Адамара, полезно сначала вычислить результат действия этого преобразования на состояние $|x\rangle$. Рассматривая отдельно случаи $x = 0$ и $x = 1$, мы видим, что для одного кубита $H|x\rangle = \sum_z (-1)^{xz}|z\rangle/\sqrt{2}$. Таким образом,

$$H^{\otimes n}|x_1, \dots, x_n\rangle = \frac{\sum_{z_1, \dots, z_n} (-1)^{x_1 z_1 + \dots + x_n z_n} |z_1, \dots, z_n\rangle}{\sqrt{2^n}}. \quad (1.49)$$

Более компактно это можно записать следующим образом:

$$H^{\otimes n}|x\rangle = \frac{\sum_z (-1)^{x \cdot z}|z\rangle}{\sqrt{2^n}}, \quad (1.50)$$

где $x \cdot z$ представляет собой побитовое скалярное произведение x и z по модулю 2. Используя это выражение совместно с (1.48), можно вычислить $|\psi_3\rangle$:

$$|\psi_3\rangle = \sum_z \sum_x \frac{(-1)^{x \cdot z + f(x)}|z\rangle}{2^n} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]. \quad (1.51)$$

Теперь Алиса наблюдает регистр запроса. Заметим, что амплитудой для состояния $|0\rangle^{\otimes n}$ является $\sum_x (-1)^{f(x)}/2^n$. Рассмотрим два возможных случая — постоянная f и сбалансированная f — чтобы выяснить, что происходит. В случае, когда $f(x)$ постоянна, амплитуда для $|0\rangle^{\otimes n}$ равна +1 или -1 в зависимости от того, какое постоянное значение принимает функция. Поскольку $|\psi_3\rangle$ имеет единичную длину, все остальные амплитуды должны быть нулевыми, и наблюдение даст нули для всех кубитов в регистре запроса. Если f сбалансирована, то положительный и отрицательный вклады в амплитуду для $|0\rangle^{\otimes n}$ взаимоуничтожаются, оставляя амплитуду нулевой, и измерение должно дать отличный от нуля результат хотя бы для одного кубита в регистре запроса. Итак, если Алиса получит при измерении все нули, то функция постоянна; в противном случае функция сбалансирована. Ниже приведено краткое изложение алгоритма Дойча-Йожа.

Алгоритм Дойча-Йожа

Вход. Черный ящик U_f выполняет преобразование $|x\rangle|y\rangle \rightarrow |x\rangle|y \otimes f(x)\rangle$ для $x \in 0, \dots, 2^n - 1$ и $f(x) \in 0, 1$. Предполагается, что $f(x)$ либо постоянна для всех значений x , либо сбалансирована, т. е. равна 1 строго для половины всех возможных x и 0 для другой половины.

Выход. 0 тогда и только тогда, когда f постоянна.

Время исполнения. Одно вычисление U_f . Всегда завершается успехом.

Процедура.

- | | | |
|----|--|--|
| 1. | $ 0\rangle^{\otimes n} 1\rangle$ | инициализация состояния |
| 2. | $\rightarrow \sum_{x \in [0,1]^n} \frac{ x\rangle}{\sqrt{2^n}} \left[\frac{ 0\rangle - 1\rangle}{\sqrt{2}} \right]$ | создание суперпозиции с использованием элементов Адамара |
| 3. | $\rightarrow \sum_x \frac{(-1)^{f(x)} x\rangle}{\sqrt{2^n}} \left[\frac{ 0\rangle - 1\rangle}{\sqrt{2}} \right]$ | вычисление функции f с использованием U_f |
| 4. | $\rightarrow \sum_z \sum_x \frac{(-1)^{x \cdot z + f(x)} z\rangle}{2^n} \left[\frac{ 0\rangle - 1\rangle}{\sqrt{2}} \right]$ | выполнение преобразования Адамара |
| 5. | $\rightarrow z$ | измерение для получения конечного результата z |

Мы показали, что квантовый компьютер может решать задачу Дойча путем однократного вычисления функции f в отличие от классического требования $2^n/2 + 1$ вычислений. Это выглядит впечатляюще, но нужно сделать несколько существенных оговорок. Во-первых, задача Дойча не особенно важна; у нее нет интересных приложений. Во-вторых, сравнение классических и квантовых алгоритмов в чем-то похоже на сравнение яблок с апельсинами, поскольку методы вычисления функции в обоих случаях очень разные. В-третьих, если Алисе разрешено использовать вероятностный классический компьютер, то попросив Боба вычислить $f(x)$ для нескольких случайно выбранных x , она может очень быстро определить с большой вероятностью, является ли f постоянной или сбалансированной. Возможно, этот вероятностный сценарий более реалистичен, чем рассмотренный нами детерминированный сценарий. Однако, несмотря на эти оговорки, алгоритм Дойча-Йожа содержит в себе зачатки еще более впечатляющих квантовых алгоритмов, и это объясняет попытку понять принципы, лежащие в основе его работы.

Упражнение 1.1 (вероятностный классический алгоритм). Пусть задача состоит не в том, чтобы достоверно отличить постоянную функцию от сбалансированной, а в том, чтобы сделать это с некоторой вероятностью ошибки $\epsilon < 1/2$. Какова эффективность наилучшего классического алгоритма, решающего такую задачу?

1.4.5 Классификация квантовых алгоритмов

Алгоритм Дойча-Йожа демонстрируют, что квантовые компьютеры могут решать некоторые вычислительные задачи намного эффективнее классических компьютеров. Однако, решаемая этим алгоритмом задача не имеет большого практического интереса. Существуют ли более интересные задачи, решение которых может быть получено с большей эффективностью при использовании квантовых алгоритмов? Каковы принципы, лежащие в основе таких алгоритмов? Каковы предельные ограничения на производительность квантового компьютера?

Говоря в самых общих чертах, есть три класса квантовых алгоритмов, имеющих преимущество над известными классическими алгоритмами. Во-первых, это класс алгоритмов, основанных на квантовой версии преобразования Фурье — инструменте, который широко используется и в классических алгоритмах. Примерами алгоритмов этого типа служат алгоритм Дойча-Йожа, а также алгоритмы Шора для задач факторизации и вычисления дискретного логарифма. Второй класс алгоритмов — это квантовые алгоритмы поиска. Третий класс алгоритмов — квантовое моделирование, при котором квантовый компьютер используется для моделирования квантовой системы. Сейчас мы кратко опишем каждый из этих классов алгоритмов, а затем суммируем то, что известно или предполагается относительно производительности квантовых компьютеров.

Квантовые алгоритмы, основанные на преобразовании Фурье

Дискретное преобразование Фурье обычно описывается как преобразование набора x_0, \dots, x_{N-1} из N комплексных чисел в набор комплексных чисел y_0, \dots, y_{N-1} , определяемый следующим образом:

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i j k / N} x_j. \quad (1.52)$$

Конечно, это преобразование широко применяется во многих отраслях знаний; задача, подвергнутая преобразованию Фурье, часто оказывается проще своего исходного варианта, что позволяет ее решить.

Польза преобразования Фурье оказалась настолько велика, что была разработана замечательная обобщенная теория преобразований Фурье, выходящая далеко за рамки определения (1.52). Эта теория содержит некоторые технические идеи из теории представлений конечных групп, и мы не будем пытаться ее здесь описывать.

Важно то, что преобразование Адамара, используемое в алгоритме Дойча-Йожа, является примером этого обобщенного класса преобразований Фурье. Более того, во многих других важных квантовых алгоритмах также используется преобразование Фурье того или иного типа.

Самые известные квантовые алгоритмы — быстрые алгоритмы Шора для задач факторизации и вычисления дискретного логарифма. Это два примера алгоритмов, которые основаны на преобразовании Фурье, определяемом в (1.52). Формула (1.52) выглядит не слишком квантовомеханической в том виде, как мы ее записали. Предположим, однако, что мы определяем линейное преобразование U над n кубитами по тому действию, которое оно оказывает на состояния вычислительного базиса $|j\rangle$, где $0 \leq j \leq 2^n - 1$:

$$|j\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i j k / 2^n} |k\rangle. \quad (1.53)$$

Можно проверить, что это преобразование является унитарным, и оно вполне может быть реализовано квантовой схемой. Более того, если мы запишем его действие на суперпозиции,

$$\sum_{j=0}^{2^n-1} x_j |j\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \left[\sum_{j=0}^{2^n-1} e^{2\pi i j k / 2^n} x_j \right] |k\rangle = \sum_{k=0}^{2^n-1} y_k |k\rangle, \quad (1.54)$$

то увидим, что это соответствует преобразованию Фурье (1.52) в векторной форме для случая $N = 2^n$.

Насколько быстро можно выполнять преобразование Фурье? Классическое быстрое преобразование Фурье требует порядка $N \log(N) = n2^n$ шагов для преобразования $N = 2^n$ чисел. На квантовом компьютере преобразование Фурье можно выполнить примерно за $\log(N)^n = n^2$ шагов — экспоненциальный выигрыш! Квантовая схема, которая это делает, рассматривается в гл. 5.

Этот результат, казалось бы, говорит о том, что квантовые компьютеры могут использоваться для очень быстрого выполнения преобразования Фурье над вектором с 2^n комплексными компонентами, что было бы фантастически полезно в широком спектре приложений. Однако это не совсем так; преобразование Фурье выполняется над информацией, «скрытой» в амплитудах квантового состояния. Эта информация недоступна для прямого измерения. Разумеется, препятствием служит то, что измерение выходного состояния вызывает коллапс каждого кубита в состояние $|0\rangle$ или $|1\rangle$, не позволяя нам непосредственно узнать результат преобразования y_k . Этот пример демонстрирует главную сложность разработки квантового алгоритма. С одной стороны, мы можем выполнять определенные вычисления над 2^n амплитудами, ассоциированными с n кубитами, гораздо более эффективно, чем это возможно на классическом компьютере, но, с другой стороны, результаты такого вычисления недоступны. Чтобы проявилась эффективность квантовых вычислений, требуется более искусственный подход.

К счастью, существует возможность использовать квантовое преобразование Фурье для эффективного решения ряда задач, которые, как считается, не имеют эффективного решения на классическом компьютере. К таким задачам относятся задача Дойча и задача Шора вычисления дискретного логарифма и факторизации. Поиски в этом направлении привели к открытию Китаевым метода решения задачи об абелевом стабилизаторе, а также к обобщению задачи о скрытой подгруппе (см. ниже).

Пусть f — такая функция из конечно порожденной группы G в конечное множество X , что ее значения постоянны на смежных классах по подгруппе K и различны для любой пары смежных классов. Используя квантовый черный ящик для выполнения унитарного преобразования $U|g\rangle|h\rangle = |g\rangle|h \oplus f(g)\rangle$, где $g \in G, h \in X$, а \oplus есть выбранная подходящим образом двоичная операция над X , найти множество образующих для K .

Алгоритм Дойча-Йожа, алгоритмы Шора, а также родственные им «экспоненциально быстрые» квантовые алгоритмы решают частные случаи этой задачи. Квантовое преобразование Фурье и его применения описаны в гл. 5.

Квантовые алгоритмы поиска

Представителем совершенно другого класса алгоритмов является квантовый алгоритм поиска, базовые принципы которого были сформулированы Гровером. Квантовый алгоритм поиска решает следующую задачу: при заданном пространстве поиска размера N и не известной заранее структуре содержащейся в нем информации найти элемент этого пространства, удовлетворяющий известному критерию. Сколько времени займет поиск элемента, удовлетворяющего этому критерию? В классическом случае такая задача требует приблизительно N операций, но квантовый алгоритм поиска позволяет решить ее с использованием приблизительно \sqrt{N} операций.

Квантовый алгоритм поиска обеспечивает только квадратичное ускорение в отличие от более впечатляющего экспоненциального ускорения, обеспечиваемого алгоритмами на основе квантового преобразования Фурье. Однако квантовый алгоритм поиска все равно представляет значительный интерес, поскольку основанные на поиске методы перебора в отличие от квантового преобразования Фурье могут применяться к очень широкому кругу задач. Квантовый алгоритм поиска и его применения описаны в гл. 6.

Квантовое моделирование

Моделирование встречающихся в природе квантовомеханических систем со всей очевидностью претендует на роль задачи, в решении которой могут, пренесясь квантовые компьютеры и которая считается трудной для классического компьютера. Трудности при моделировании квантовых систем общего вида на классических компьютерах обусловлены той же причиной, что и при моделировании квантовых компьютеров — количество комплексных чисел, необходимых для описания квантовой системы, в общем случае растет с увеличением размера системы *экспоненциально*, а не линейно, как для классических систем. В общем случае хранение квантового состояния системы с n различными компонентами на классическом компьютере требует порядка c^n битов памяти, где c — константа, зависящая от устройства моделируемой системы и желаемой точности моделирования.

Квантовый компьютер, напротив, может выполнять моделирование с использованием kn кубитов, где k , как и прежде, константа, зависящая от устройства моделируемой системы. Это позволяет квантовым компьютерам эффективно моделировать квантовомеханические системы, которые, как считается, нельзя эффективно смоделировать на классическом компьютере. Однако здесь необходима существенная оговорка: хотя квантовый компьютер может моделировать многие квантовые системы гораздо эффективнее классического, это не означает, что быстрое моделирование позволит получать желаемую информацию о квантовой системе. При измерении kn -кубитовая модель сколлапсирует в определенное состояние, дав только kn битов информации; c^n битов «скрытой информации», присутствующей в волновой функции, не доступны в полном объеме. Таким образом, ключом к практическому применению квантового моделирования является разработка методов, посредством которых можно эффективно извлекать желаемые ответы; как это делать — понятно лишь отчасти.

Несмотря на эту оговорку, квантовое моделирование с большой вероятностью станет важным применением квантовых компьютеров. Моделирование квантовых систем — это важная проблема во многих областях, особенно в квантовой химии, где вычислительные ограничения, налагаемые классическими компьютерами, затрудняют точное моделирование молекул даже среднего размера, не говоря уже об очень больших молекулах, встречающихся во многих важных биологических системах. Реализация более быстрого и точного моделирования таких систем может решающим образом повлиять на прогресс в других областях, где важны квантовые явления.

Возможно, что в будущем мы откроем физическое явление Природы, которое нельзя эффективно моделировать на квантовом компьютере. И это будет совсем не плохо, а даже замечательно! Как минимум, это заставит нас расширить свои вычислительные модели для охвата нового явления и сделать их более мощными, чем существующая модель квантовых вычислений. Вполне вероятно также, что с любым таким явлением будут связаны новые и очень интересные физические эффекты!

Квантовое моделирование можно применять и как общий метод изучения других квантовых алгоритмов; например, в разд. 6.2 мы объясним, что квантовый алгоритм поиска можно рассматривать как решение проблемы квантового моделирования. При таком подходе к проблеме становится намного легче понять происхождение квантового алгоритма поиска.

Наконец, квантовое моделирование позволяет вывести интересное и оптимистичное «квантовое следствие» из закона Мура. Вспомним: закон Мура утверждает, что производительность классических компьютеров, обеспечиваемая за одну и ту же цену, будет удваиваться примерно каждые два года. Предположим, однако, что мы моделируем на классическом компьютере квантовую систему, и хотим добавить к ней одиночный кубит (или более крупную систему). Это как минимум удваивает объем памяти, требуемой классическому компьютеру, чтобы хранить описание состояния квантовой системы, и в такой же (или большей) степени повышает затраты времени на моделирование ее динамики. Из данного наблюдения и вытекает квантовое следствие закона Мура, утверждающее, что квантовые компьютеры будут развиваться наравне с классическими, если к квантовому компьютеру каждые два года добавлять *один кубит*. Этот вывод не следует воспринимать слишком серьезно, поскольку до сих пор не ясно, какова истинная природа превосходства квантовых вычислений над классическими (если такое превосходство вообще имеет место). Тем не менее, это эвристическое утверждение помогает понять, почему нам следует интересоваться квантовыми компьютерами, и мы надеемся, что однажды они смогут превзойти наиболее мощные классические компьютеры, по крайней мере, для некоторых приложений.

Эффективность квантовых вычислений

Насколько эффективны квантовые компьютеры? Что придает им эту эффективность? Пока никто не знает ответов на эти вопросы, несмотря на наличие таких примеров, как факторизация, дающих серьезные основания полагать, что

квантовые компьютеры обладают большей производительностью, чем классические. Может оказаться, что квантовые компьютеры не эффективнее классических в том смысле, что любая задача, которая может быть эффективно решена на квантовом компьютере, может быть эффективно решена и на классическом компьютере. С другой стороны, со временем может быть доказано, что квантовые компьютеры намного эффективнее классических. Сейчас мы кратко изложим то, что известно об эффективности квантовых вычислений.

Классификацией сложности различных вычислительных задач, как классических, так и квантовых, занимается *теория сложности вычислений*, и чтобы понять, какова эффективность квантовых компьютеров, мы сначала рассмотрим некоторые общие идеи из этой теории. Наиболее фундаментальным понятием является понятие *класса сложности*. Класс сложности можно представить как совокупность вычислительных задач, имеющих некоторое общее свойство по отношению к вычислительным ресурсам, требуемым для их решения. Два из наиболее важных класса — это **P** и **NP**. Грубо говоря, **P** — это класс вычислительных задач, которые можно быстро решить на классическом компьютере. **NP** — это класс задач, решения которых можно быстро проверить на классическом компьютере. Чтобы понять различие между **P** и **NP**, рассмотрим задачу поиска простых делителей целого числа n . Как известно, пока не существует быстрого способа решения этой задачи на классическом компьютере, и есть основания полагать, что данная задача не входит в **P**. С другой стороны, если кто-то скажет вам, что некоторое число p есть делитель n , мы можем быстро проверить, так ли это, разделив n на p , поэтому факторизация — это задача, принадлежащая классу **NP**.

Очевидно, что **P** является подмножеством **NP**, так как возможность решения задачи подразумевает возможность проверки потенциальных решений. Неясно, однако, есть ли в **NP** задачи, не входящие в **P**. Возможно, самой важной нерешенной проблемой в теоретической информатике является определение того, различны ли эти два класса:

$$\mathbf{P} \neq \mathbf{NP}. \quad (1.55)$$

Большинство исследователей полагают, что **NP** содержит задачи, не входящие в **P**. В частности, существует важный подкласс задач **NP**, **NP**-полные задачи, который представляет особый интерес по двум причинам. Во-первых, есть тысячи задач, и среди них много крайне важных, которые известны как **NP**-полные. Во-вторых, любая **NP**-полнная задача является в некотором смысле не менее трудной, чем все другие задачи в **NP**. Точнее говоря, алгоритм решения конкретной **NP**-полнной задачи может быть адаптирован для решения любой другой задачи из **NP**, причем с небольшими издержками. В частности, если $\mathbf{P} \neq \mathbf{NP}$, то отсюда следует, что никакая **NP**-полнная задача не может быть эффективно решена на классическом компьютере.

Можно ли использовать квантовые компьютеры для быстрого решения всех задач из **NP** — неизвестно, несмотря на тот факт, что на них можно решать некоторые задачи (вроде факторизации), которые, как полагают многие, принадлежат **NP**, но не **P**. (Заметим, что **NP**-полнота факторизации не доказа-

на, иначе мы бы уже знали, как эффективно решать все задачи из **NP** при помощи квантовых компьютеров.) Было бы очень хорошо, если бы оказалось возможным эффективно решать на квантовом компьютере все задачи из **NP**. В этом направлении известен очень интересный отрицательный результат, который исключает использование простого варианта квантового параллелизма для решения всех задач из **NP**. В частности, один из подходов к проблеме решения задач из **NP** на квантовом компьютере состоит в попытке использовать какую-либо разновидность квантового параллелизма для параллельного поиска среди всех возможных решений. В разд. 6.6 мы покажем, что никакой подход, основанный на такой поисковой методологии, не может обеспечить эффективного решения всех **NP**-полных задач из **NP**. Невозможность применения такого подхода разочаровывает, но не исключает существования в задачах **NP** некоторой более глубокой структуры, которая позволит быстро решать их при помощи квантового компьютера.

P и **NP** — это лишь два из множества известных классов сложности. Другим важным классом сложности является **PSPACE**. Грубо говоря, **PSPACE** состоит из задач, которые можно решить при использовании ресурсов, небольших по пространственному размеру («малый» компьютер), но не обязательно по времени (допустимы «длинные» вычисления). Считается, что **PSPACE** строго больше, чем **P** и **NP** в совокупности, хотя это никогда не было доказано. Наконец, класс сложности **BPP** содержит задачи, которые могут быть решены с использованием вероятностных алгоритмов за полиномиальное время, если в решении допускается ограниченная вероятность ошибки (скажем, $1/4$). **BPP** широко признан (даже более, чем **P**) как класс задач, которые следует считать эффективно разрешимыми на классическом компьютере. Мы сосредоточимся здесь на **P**, а не на **BPP**, поскольку **P** изучен более подробно, однако многое похожих идей и выводов возникает и относительно **BPP**.

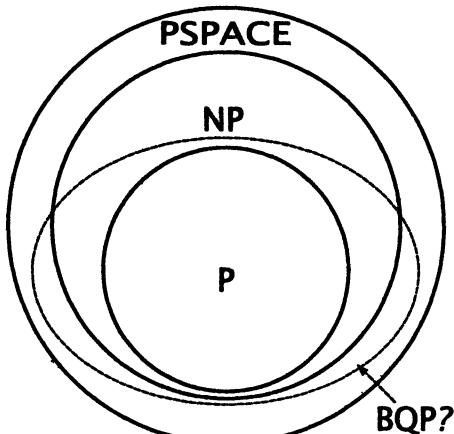


Рис. 1.21. Взаимосвязь между классическими и квантовыми классами сложности. Квантовые компьютеры могут быстро решить любую задачу из **P**, причем известно, что они не могут эффективно решать задачи вне **PSPACE**. Какое место между **P** и **PSPACE** занимают квантовые компьютеры — неизвестно, в частности, потому, что мы не знаем даже, больше ли **PSPACE**, чем **P**!

А как насчет квантовых классов сложности? Мы можем определить **BQP** как класс всех вычислительных задач, которые эффективно решаются на квантовом компьютере, когда допустима ограниченная вероятность ошибки. (Строго говоря, при таком определении **BQP** более подобен классическому классу сложности **BPP**, чем **P**, но сейчас мы игнорируем эту тонкость и будем рассматривать его как аналог **P**.) Как именно **BQP** соотносится с **P**, **NP** и **PSPACE** — пока неизвестно. Известно лишь, что квантовые компьютеры могут эффективно решать все задачи из **P**, но вне **PSPACE** нет таких задач, которые они могли бы решать эффективно. Это означает, что **BQP** находится где-то между **P** и **PSPACE**, как показано на рис. 1.21. Поэтому если доказать, что квантовые компьютеры строго эффективнее классических, то тогда **P** не равен **PSPACE**. Доказать последнее безуспешно пытались многие специалисты в области информатики, и это говорит о том, что доказательство превосходства квантовых компьютеров над классическими может оказаться нетривиальным, несмотря на многие доводы в пользу этого утверждения.

Дальнейшие рассуждения о предельной эффективности квантовых компьютеров мы отложим до тех пор, пока не начнем лучше понимать принципы, лежащие в основе быстрых квантовых алгоритмов; этой теме отведено значительное место во второй части книги. Но и сейчас уже ясно, что квантовая теория вычислений бросает интересный и серьезный вызов традиционным представлениям о вычислениях. Особую важность этому вызову придает то, что теоретическая модель квантовых вычислений считается экспериментально реализуемой, ибо, насколько мы знаем, эта теория согласуется с законами Природы. Если бы это было не так, то квантовые вычисления оставались бы просто еще одним математическим курьезом.

1.5 Экспериментальная обработка квантовой информации

Квантовые вычисления и квантовая информация — это замечательное теоретическое открытие, но его центральные понятия, такие как суперпозиция и запутанность, противоречат интуиции, формируемой повседневными наблюдениями за окружающим нас миром. Как доказать, что эти представления соответствуют действительности? Возможна ли экспериментальная реализация больших квантовых компьютеров? Есть ли какие-нибудь физические принципы, запрещающие их потенциальное масштабирование? Эти вопросы рассматриваются в двух следующих разделах. Мы начнем с обзора знаменитого эксперимента Штерна–Герлаха, который свидетельствует о существовании кубитов в Природе. Затем мы рассмотрим более широкую проблему практического построения систем обработки квантовой информации.

1.5.1 Эксперимент Штерна–Герлаха

Кубит является фундаментальным элементом в области квантовых вычислений и квантовой информации. Откуда мы знаем, что системы со свойствами

кубитов существуют в Природе? На момент написания книги накоплено громадное количество доказательств, но на заре квантовой механики кубитовая структура была совсем не очевидной, и люди бились над объяснением явлений, которые мы сейчас можем понять в терминах кубитов, т. е. в терминах двухуровневых квантовых систем.

Первый решающий (и очень известный) эксперимент, свидетельствующий о кубитовой структуре, был задуман в 1921 г. Штерном и проведен Герлахом в 1922 г. во Франкфурте. В оригинальном эксперименте Штерна–Герлаха «горячие» атомы из печи пролетали через магнитное поле, которое заставляло их отклоняться, после чего положение каждого атома регистрировалось (рис. 1.22). Оригинальный эксперимент проводился с атомами серебра, которые имеют сложную структуру, затушевывающую обсуждаемые эффекты. То, что описано ниже, в действительности относится к эксперименту 1927 г., проведенному с использованием атомов водорода. Основной наблюдаемый эффект тот же, но с атомами водорода легче следить за рассуждениями. Учтите, однако, что эта привилегия была недоступна людям в начале 20-х гг. XX в.; им требовалось проявить немало сообразительности, чтобы придумать объяснения более сложным эффектам, которые они наблюдали.

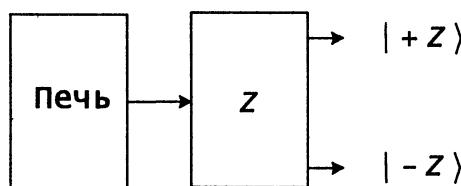


Рис. 1.22. Абстрактная схема эксперимента Штерна–Герлаха. Горячие атомы водорода из печи пролетают через магнитное поле, которое отклоняет их вверх ($|+ Z \rangle$) или вниз ($| - Z \rangle$)

Атомы водорода содержат протон и орбитальный электрон. Этот электрон можно рассматривать как слабый «электрический ток» вокруг протона.³ За счет этого электрического тока атом имеет магнитное поле; у каждого атома есть то, что физики называют «магнитным дипольным моментом». В результате каждый атом ведет себя как маленький стержневой магнит, ось которого совпадает с осью, вокруг которой вращается электрон. Если бросать такие магнитики через неоднородное магнитное поле, они будут отклоняться полем. Похожее отклонение атомов мы ожидаем увидеть в эксперименте Штерна–Герлаха.

Отклонение атома зависит как от магнитного дипольного момента атома — оси, вокруг которой вращается электрон, — так и от магнитного поля, создаваемого в устройстве Штерна–Герлаха. Мы не будем вдаваться в подробности; достаточно сказать, что сконструировав подходящим образом установку, можно добиться отклонения атома на величину, зависящую от \hat{z} -компоненты

³ Это верно только для возбужденных состояний. В основном состоянии атома водорода такой ток равен нулю, и соответственно равен нулю орбитальный магнитный момент атома.— Прим. ред.

магнитного дипольного момента атома, где \hat{z} есть некоторая фиксированная внешняя ось.

При проведении этого эксперимента нас поджидают два главных сюрприза. Прежде всего естественно ожидать, что у вылетающих из печи горячих атомов диполи ориентированы в произвольном направлении, и, следовательно, мы должны увидеть непрерывное распределение атомов во всем диапазоне углов их вылета. Вместо этого наблюдается *дискретный* набор углов, под которыми вылетают атомы. Физики смогли это объяснить, предположив, что магнитный дипольный момент атомов *квантуется*, т. е. принимает дискретные значения, кратные некоторой фундаментальной величине.

Наблюдение квантования в эксперименте Штерна–Герлаха явилось для физиков начала 20-х гг. неожиданным, но не таким уж удивительным, поскольку наличие эффектов квантования в других системах становилось к тому времени все более несомненным. Что стало настоящим сюрпризом, так это *количество* пиков, наблюдавшихся в эксперименте. Использовались такие атомы водорода, которые должны были иметь *нулевой* магнитный дипольный момент. В классической физике это удивительно само по себе, поскольку эквивалентно отсутствию орбитального движения электрона, но знания в области квантовой механики, накопленные к тому времени, допускали такую возможность. Поскольку атомы водорода в этом случае имели бы нулевой магнитный момент, ожидалось увидеть только один пучок атомов, и этот пучок не должен был отклоняться магнитным полем. Вместо этого наблюдались два пучка, один из которых отклонялся магнитным полем вверх, а другой — вниз!

Это загадочное раздвоение удалось объяснить, лишь постулировав, что с электроном в атоме водорода связана величина под названием *спин*. Спин не имеет никакого отношения к обычному вращательному движению электрона вокруг протона; это совершенно новая величина, связанная с самим электроном. Великий физик Гейзенберг сразу же оценил эту идею как «смелую», и она действительно смелая, поскольку вводит в Природу совершенно новую физическую величину. Было постулировано, что спин электрона вносит *дополнительный* вклад в магнитный дипольный момент атома водорода помимо того вклада, который обусловлен вращательным движением электрона.

Как правильно описать спин электрона? Для начала мы можем предположить, что спин определяется одним битом, указывающим на отклонение атома водорода вверх или вниз. Дополнительные экспериментальные результаты дают дополнительную информацию, позволяющую определить, насколько верна эта догадка. Представим себе оригинальную установку Штерна–Герлаха, показанную на рис. 1.22. На ее выходе имеются два пучка атомов $| -Z \rangle$ и $| +Z \rangle$. (Мы используем наглядную запись, похожую на квантовомеханическую, но вы, разумеется, можете использовать любую другую запись, которую предпочитаете.) Теперь предположим, что мы последовательно соединили две установки Штерна–Герлаха, как показано на рис. 1.23. Расположим их так, чтобы вторая установка была *поворнута боком*, и магнитное поле отклоняло атомы вдоль оси \hat{x} . В этом мысленном эксперименте мы блокируем выход $| -Z \rangle$ первой установки Штерна–Герлаха, а выход $| +Z \rangle$ направляем через вторую установ-

ку, ориентированную вдоль оси \hat{x} . На последнем выходе помещается детектор для измерения распределения атомов вдоль оси \hat{x} .

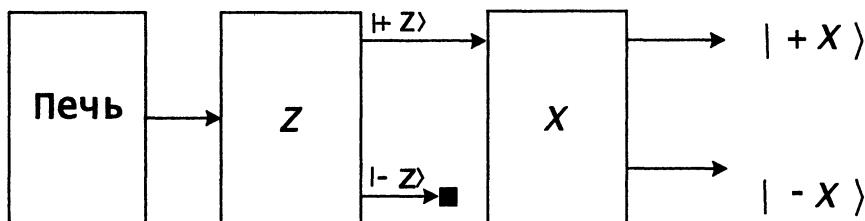


Рис. 1.23. Каскадные измерения Штерна–Герлаха

Классический магнитный дипольный момент, ориентированный в направлении $+\hat{z}$, не имеет чистого магнитного момента в направлении \hat{x} , поэтому можно ожидать, что на последнем выходе будет один центральный пик. Однако в эксперименте наблюдаются два пика одинаковой интенсивности! Похоже, что эти атомы имеют особенность, заключающуюся в наличии определенных магнитных моментов вдоль каждой оси, причем не зависящих друг от друга, т. е. возможно, что каждый атом, проходящий через вторую установку, находится в состоянии, которое можно записать как $|+Z\rangle|+X\rangle$ или $|+Z\rangle|-X\rangle$, отразив тот факт, что могут наблюдаться два значения спина.

Эту гипотезу можно проверить при помощи другого эксперимента (рис. 1.24) в котором один из пучков с предыдущего выхода пропускается через вторую $+\hat{z}$ -ориентированную установку Штерна–Герлаха. Если атомы сохраняют свою ориентацию $|+Z\rangle$, то на выходе следовало бы ожидать только одного пика. Однако на последнем выходе снова наблюдаются два пучка, причем одинаковой интенсивности.

Таким образом, напрашивается следующее заключение: вопреки классическим ожиданиям, состояние $|+Z\rangle$ состоит из равных частей состояний $|+X\rangle$ и $| - X \rangle$, а состояние $|+X\rangle$ состоит из равных частей состояний $|+Z\rangle$ и $| - Z \rangle$. К подобным заключениям можно прийти, если направить аппарат Штерна–Герлаха вдоль какой-нибудь другой оси, например, $+\hat{y}$.

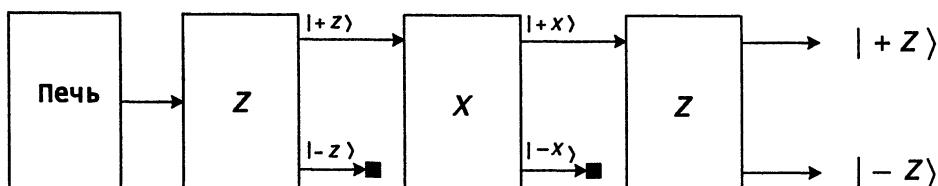


Рис. 1.24. Трехступенчатые каскадные измерения Штерна–Герлаха

Кубитовая модель дает простое объяснение этому экспериментально наблюдаемому поведению. Пусть $|0\rangle$ и $|1\rangle$ — состояния кубита. Выполним следующие присваивания:

$$|+Z\rangle \leftarrow |0\rangle \quad (1.56)$$

$$|-Z\rangle \leftarrow |1\rangle \quad (1.57)$$

$$|+X\rangle \leftarrow (|0\rangle + |1\rangle)/\sqrt{2} \quad (1.58)$$

$$|-X\rangle \leftarrow (|0\rangle - |1\rangle)/\sqrt{2}. \quad (1.59)$$

Тогда результаты каскадного эксперимента Штерна–Герлаха можно объяснить, предположив, что \hat{z} -установка измеряет спин (т. е. кубит) в вычислительном базисе $|0\rangle$, $|1\rangle$, а \hat{x} -установка измеряет спин относительно базиса $(|0\rangle + |1\rangle)/\sqrt{2}$, $(|0\rangle - |1\rangle)/\sqrt{2}$. Например, если в каскадном эксперименте $\hat{x} - \hat{y} - \hat{z}$ предположить, что на выходе первой установки Штерна–Герлаха спины находятся в состоянии $|+Z\rangle = |0\rangle = (|+X\rangle - |-X\rangle)/\sqrt{2}$, то вероятность получения после второй установки состояния $|+X\rangle$ равна $1/2$, как и вероятность получения $|-X\rangle$. Подобно этому, вероятность получения $|+Z\rangle$ на выходе третьей установки тоже равна $1/2$. Таким образом, кубитовая модель правильно предсказывает результаты каскадного эксперимента Штерна–Герлаха описанного типа.

Этот пример демонстрирует, почему кубиты можно считать правдоподобной моделью встречающихся в Природе систем. Конечно, он не дает абсолютной уверенности в том, что кубитовая модель правильно описывает спин электрона — требуется гораздо больше экспериментальных подтверждений. Тем не менее, эти и многие другие аналогичные эксперименты позволяют считать, что спин электрона лучше всего описывается кубитовой моделью. Более того, мы полагаем, что кубитовая модель (и ее обобщения на большие размерности — другими словами, квантовая механика) способна описать *любую* физическую систему. Теперь мы перейдем к вопросу о том, какие системы особенно подходят для обработки квантовой информации.

1.5.2 Перспективы практической обработки квантовой информации

Построение устройств обработки квантовой информации — это грандиозная задача для ученых и инженеров третьего тысячелетия. Сможем ли мы справиться с этой задачей? Решаема ли она вообще? Стоит ли за нее браться? Если да, то как достичь успеха? В этом разделе мы попытаемся дать краткие ответы на эти трудные и важные вопросы, которые будут подробно разбираться на протяжении всей книги.

Наиболее фундаментальный вопрос: есть ли какие-нибудь принципиальные моменты, не позволяющие реализовать те или иные способы обработки квантовой информации? Прежде всего, видятся два возможных препятствия: наличие шума может стать фундаментальным барьером на пути практической обработки квантовой информации и квантовая механика может оказаться ошибочной.

Несомненно, что шум серьезно мешает разработке устройств для практической обработки квантовой информации. Но является ли он *принципиально неустранимым* препятствием, которое навсегда исключает создание круп-

номасштабных устройств обработки квантовой информации? Из теории кодов, исправляющих квантовые ошибки, следует, что квантовый шум, оставаясь практической проблемой, которая требует решения, не представляет *принципиальной* проблемы. В частности, для квантовых вычислений справедлива *пороговая теорема*, которая утверждает, грубо говоря, что если шум в квантовом компьютере может быть снижен до некоторой постоянной «пороговой» величины, то коды, исправляющие квантовые ошибки, позволяют уменьшать его еще больше, по существу, *неограниченно* за счет небольшого усложнения вычислений. В пороговой теореме делается ряд предположений общего характера о природе и интенсивности шума в квантовом компьютере, а также относительно архитектуры квантового компьютера. Если эти условия выполнены, то эффекты шума можно довести до уровня, несущественного для квантовой обработки информации. Квантовый шум, исправление квантовых ошибок и пороговая теорема подробно рассматриваются в главах 8, 10 и 12.

Вторым препятствием, которое может помешать обработке квантовой информации является возможная ошибочность квантовой механики. Вообще, проверка справедливости квантовой механики (как релятивистской, так и нерелятивистской) является одной из причин интереса к построению устройств обработки квантовой информации. Никогда прежде мы не исследовали полностью контролируемые крупномасштабные квантовые системы, и не исключено, что Природа может преподнести здесь новые сюрпризы, которые не имеют адекватного объяснения в квантовой механике. Если это произойдет, то мы будем иметь дело с выдающимся открытием в истории науки, которое наверняка скажется на других областях науки и техники, как когда-то открытие квантовой механики, и также может повлиять на область квантовых вычислений и квантовой информации. Однако нельзя сказать заранее, приведет ли это к увеличению или уменьшению эффективности устройств обработки квантовой информации, или же оставит ее неизменной. Пока такие эффекты не найдены, у нас нет возможности узнать, как они могут повлиять на обработку информации, поэтому далее в этой книге мы опираемся на известные к настоящему времени факты и предполагаем, что квантовая механика дает полное и правильное описание мира.

Если даже принципиального препятствия для построения устройств обработки квантовой информации не существует, зачем нам тратить огромное количество времени и денег, пытаясь их создать? Несколько причин мы уже рассматривали: практические применения, такие как квантовая криптография и факторизация больших составных чисел; наконец, желание получить фундаментальные знания о Природе и обработке информации.

Это веские причины, и они оправдывают значительные затраты времени и средств на построение устройств квантовой обработки информации. Однако справедливости ради следует сказать, что для сопоставления возможностей устройств обработки квантовой и классической информации необходимо иметь более четкое представление об их относительной эффективности. Это, в свою очередь, требует дальнейшей теоретической работы в области квантовых вычислений и квантовой информации. В частности, интересно получить

окончательный ответ на вопрос «Эффективнее ли квантовые компьютеры по сравнению с классическими?». Даже если этот вопрос некоторое время останется открытым, было бы полезно иметь четкий «маршрут» из интересных приложений разных уровней сложности, чтобы помочь исследователям, нацеливающимся на экспериментальную реализацию обработки квантовой информации. История показывает, что технический прогресс часто стимулируется постановкой кратко- и среднесрочных задач, которые служат промежуточными ступенями для достижения отдаленных целей. Вспомним, что микропроцессоры сначала использовались в качестве контроллеров лифтов и других простых устройств, и лишь потом превратились в главную составляющую персональных компьютеров (а потом и многоного другого). Ниже мы наметим последовательность кратко- и среднесрочных задач для тех, кто заинтересован в достижении конечной цели — крупномасштабной обработки квантовой информации.

Известно на удивление много мелкомасштабных применений квантовых вычислений и квантовой информации. Не все они столь же блестательны, как алгоритм квантовой факторизации, но относительная простота реализации приложений малого масштаба делает их крайне важными в качестве самостоятельных среднесрочных задач.

Два элементарных процесса, совершенствование которых очень важно для квантовых вычислений и квантовой информации (а также представляет самостоятельный интерес) — это томография квантовых состояний и томография квантовых процессов. Томография квантовых состояний представляет собой метод определения квантового состояния системы, состоящий в повторном приготовлении одного и того же состояния и измерении его разными способами. Это позволяет преодолеть «скрытую» природу квантового состояния (как вы помните, состояние нельзя определить путем прямого измерения) и составить его полное описание. Томография квантовых процессов, будучи тесно связана с томографией квантовых состояний, претендует на большее, а именно, на полное описание *динамики* квантовой системы. Например, с ее помощью можно узнать характеристики некоторого квантового элемента и квантового канала связи или определить типы и амплитуды различных шумовых процессов в системе. Помимо очевидных применений в области квантовых вычислений и квантовой информации, томография квантовых процессов может стать важным диагностическим инструментом, помогающим описывать и совершенствовать базовые операции в любых областях науки и техники, где существенны квантовые эффекты. Томография квантовых состояний и томография квантовых процессов подробнее описываются в гл. 8.

Большой интерес представляют также различные базовые коммуникационные операции. Мы уже упоминали о квантовой криптографии и квантовой телепортации. Первая из них, по-видимому, будет полезна в практических приложениях, включающих передачу небольших объемов информации (ключа) с большой секретностью. Применение квантовой телепортации вызывает больше вопросов. Как мы увидим в гл. 12, телепортация может быть исключительно полезна для передачи квантовых состояний между удаленными узлами сети в присутствии шума. Идея состоит в том, чтобы сосредоточить усилия на пере-

даче ЭПР-пар между узлами, намеревающимися связываться друг с другом. ЭПР-пары могут искажаться в процессе передачи, но специальные протоколы «очищения запутанности» могут затем «очищать» эти пары, позволяя использовать их для телепортации квантовых состояний из одного места в другое. Фактически, протоколы на основе очищения запутанности и телепортации превосходят более традиционные технологии исправления квантовых ошибок в том, что касается обеспечения свободной от шумов передачи кубитов.

А как насчет применений среднего масштаба? Многообещающим среднемасштабным применением устройств обработки квантовой информации является моделирование квантовых систем. Для моделирования квантовой системы, содержащей всего несколько десятков «кубитов» (или их эквивалента в терминах какой-либо другой базовой системы); не хватит ресурсов даже самых больших суперкомпьютеров. Поучительно выполнить простое вычисление. Предположим, что у нас есть система с 50 кубитами. Чтобы описать ее состояние, требуется $2^{50} \approx 10^{15}$ комплексных амплитуд. Если амплитуды хранятся со 128-битовой точностью, то для каждой амплитуды требуется 256 битов, или 32 байта. В сумме это составляет 32×10^{15} байтов, или примерно 32 тысячи терабайтов информации, что значительно превышает возможности существующих компьютеров и примерно соответствует объему памяти, которого можно ожидать у суперкомпьютеров во втором десятилетии двадцать первого века, если закон Мура останется в силе. Для 90 кубитов при том же уровне точности требуется 32×10^{27} байтов, для хранения которых, даже если представлять биты одиночными атомами, нужны килограммы вещества.

Насколько полезным будет квантовое моделирование? По всей видимости традиционные методы по-прежнему будут использоваться для определения элементарных свойств материалов, например, энергии связи и основных спектроскопических характеристик. Однако после того, как основные свойства будут хорошо поняты, квантовое моделирование должно найти широкое применение в качестве «лаборатории» для конструирования новых молекул и проверки их свойств. Для тестирования всего разнообразия возможных структур молекулы в традиционной лаборатории может потребоваться много разного оборудования и материалов — химикатов, детекторов и т. д. На квантовом компьютере все это оборудование можно смоделировать программно, что наверняка окажется намного дешевле и быстрее. Конечно, окончательное конструирование и тестирование необходимо выполнять с использованием реальных физических систем; однако квантовые компьютеры могут обеспечить изучение гораздо большего числа потенциальных структур и тем самым добиваться лучшего конечного результата. Интересно отметить, что такие «прямые» расчеты для разработки новых молекул пробовали проводить и на классических компьютерах; однако эти попытки имели ограниченный успех из-за огромных требований к вычислительным ресурсам, необходимым для моделирования квантовой механики на классическом компьютере. Следует ожидать, что в относительно недалеком будущем квантовые компьютеры справятся с этим гораздо лучше.

А как насчет крупномасштабных применений? Помимо квантового моделирования и квантовой криптографии в больших объемах, их известно отно-

сительно немного: факторизация больших чисел, вычисление дискретных логарифмов и квантовый поиск. Интерес к первым двум обусловлен главным образом тем *негативным* эффектом, который они могут дать: ограничение надежности существующих криптографических систем с открытым ключом. (Они также могут представлять значительный практический интерес для математиков, занимающихся этими проблемами просто из любопытства.) Таким образом, факторизация и вычисление дискретного логарифма вряд ли будут важны как самостоятельные приложения в долгосрочной перспективе. Квантовый поиск может широко использоваться из-за большого практического значения поисковой эвристики; некоторые возможные применения мы рассмотрим в гл. 6. Было бы хорошо найти другие крупномасштабные применения устройств обработки квантовой информации. Это основная задача на будущее!

Как же воплотить рассмотренную иерархию применений в реальных физических системах? Для малых масштабов (уровня нескольких кубитов) уже предложено несколько устройств обработки квантовой информации. Возможно, самыми легкими в реализации являются те из них, которые основаны на *оптических* технологиях, т. е. на использовании электромагнитного излучения. Для элементарных манипуляций с фотонами подходят простые устройства типа зеркал и светоделительных пластинок. Интересно, что основная трудность состоит в выдаче одиночных фотонов по требованию; вместо этого экспериментаторы решили использовать схемы, где одиночные фотоны генерируются время от времени случайным образом, и ждать наступления такого события. При помощи таких оптических технологий были реализованы квантовая криптография, сверхплотное кодирование и квантовая телепортация. Главное достоинство оптических технологий в том, что фотоны проявляют себя как наиболее стабильные носители квантовомеханической информации. Главный недостаток — фотоны не взаимодействуют друг с другом непосредственно. Взаимодействие необходимо осуществлять через какое-то промежуточное звено, например, атом, а это вносит дополнительные шумы и усложняет эксперимент. Таким образом, *реальное* взаимодействие двух фотонов есть двухступенчатый процесс: первый фотон взаимодействует с атомом, который, в свою очередь, взаимодействует со вторым фотоном.

Альтернативная схема основана на методах захвата различных типов атомов: существуют *ионные ловушки*, где в ограниченном пространстве заключено небольшое количество заряженных атомов, и *ловушки нейтральных атомов* для захвата незаряженных атомов. В схемах обработки квантовой информации, основанных на атомных ловушках, для хранения кубитов используются атомы. Электромагнитное излучение в этих схемах тоже используется, но совсем не так, как при «оптическом» подходе. Фотоны применяются здесь для манипулирования информацией, хранящейся в атомах, а не как самостоятельные элементы хранения информации. Однокубитовые квантовые элементы можно реализовать, воздействуя импульсами электромагнитного излучения на отдельные атомы. Соседние атомы могут взаимодействовать друг с другом посредством, например, дипольных сил, обеспечивающих работу многокубитовых квантовых элементов. Более того, взаимодействие соседних атомов можно

модифицировать, воздействуя на них подходящими импульсами электромагнитного излучения. Это позволяет выбирать элементы, которые реализуются в системе. Наконец, для осуществления квантовых измерений в таких системах подходит хорошо известный метод *квантовых переходов*, который позволяет исключительно точно проводить измерения в вычислительном базисе, используемом для квантовых вычислений.

Другой класс схем обработки квантовой информации основан на *ядерном магнитном резонансе*, часто называемом по начальным буквам — ЯМР. В таких схемах квантовая информация хранится в *ядерном спине* атомов, входящих в молекулу, а манипулирование этой информацией осуществляется при помощи электромагнитного излучения. Использование таких схем сопряжено со специфическими трудностями, поскольку в ЯМР невозможно обращаться напрямую к отдельным ядрам. Вместо этого используется гигантское число (как правило, порядка 10^{15}) практически одинаковых молекул, находящихся в растворе. Электромагнитные импульсы воздействуют на образец, заставляя каждую молекулу реагировать примерно одним и тем же образом. Каждую молекулу следует рассматривать как независимый компьютер, а образец в целом — как совокупность огромного числа компьютеров, работающих параллельно (в классическом смысле). Обработка квантовой информации при помощи ЯМР сопряжена с тремя специфическими трудностями, которые сильно отличают ее от других схем обработки квантовой информации. Во-первых, молекулы обычно приготавливают путем приведения их в равновесное состояние при комнатной температуре, которая настолько высока по сравнению с типичной энергией переворота спина, что спины приобретают почти полностью случайную ориентацию. Из-за этого начальное состояние становится значительно более «шумным», чем было бы желательно для обработки квантовой информации. Преодоление этого шума представляет собой интересную задачу, которую мы рассмотрим в гл. 7. Вторая проблема в том, что класс измерений, которые могут выполняться при исследовании ЯМР, не содержит большинства общих измерений, которые нам хотелось бы выполнять при обработке квантовой информации. Тем не менее, измерений этого класса достаточно для многих задач по обработке квантовой информации. В-третьих, поскольку при использовании ЯМР к молекулам нельзя обращаться по отдельности, может возникнуть вопрос — как же манипулировать отдельными кубитами? К счастью, разные ядра в молекуле могут иметь разные свойства, что позволяет обращаться к ним по отдельности, или, по крайней мере, с таким разрешением, которого достаточно для выполнения операций, необходимых при квантовых вычислениях.

В существующих предложениях можно найти многие из элементов, требуемых для осуществления крупномасштабной обработки квантовой информации: в ионной ловушке можно прекрасно приготавливать состояния и проводить квантовые измерения над небольшим числом кубитов; с помощью ЯМР можно реализовать великолепную динамику в малых молекулах; технология производства твердотельных систем позволяет отлично масштабировать конструкции. Объединение всех этих элементов в одну систему стало бы большим шагом на пути к гипотетическому квантовому компьютеру. К сожалению, все эти си-

стемы очень различаются, и от больших квантовых компьютеров нас отделяют многие и многие годы. Однако мы считаем, что наличие всех этих свойств у существующих (пусть и различных) систем служит хорошим предзнаменованием, указывающим на возможность появления в далекой перспективе процессоров для крупномасштабной обработки квантовой информации. Более того, это наводит на мысль о целесообразности развития *гибридных* конструкций, сочетающих в себе лучшие черты двух или более существующих технологий. Например, сейчас ведется большая работа по захвату атомов в *электромагнитных резонаторах*. Это позволяет гибко манипулировать атомом внутри резонатора при помощи оптических методов, а также открывает возможность управления одиночными атомами в реальном масштабе времени с использованием обратной связи такими способами, которые недоступны в традиционных атомных ловушках.

В заключение заметим, что обработку квантовой информации ни в коем случае нельзя считать просто еще одной технологией обработки информации. Например, есть соблазн отмахнуться от квантовых вычислений, посчитав их очередной технологической модой в эволюции компьютера, которая со временем пройдет, так было с другими модными идеями, скажем, памятью на цилиндрических магнитных доменах, широко рекламировавшейся в начале 80-х гг. XX в. как следующее большое достижение в технологии запоминающих устройств. Это будет ошибкой, поскольку квантовые вычисления представляют собой *абстрактную парадигму* обработки информации, которая может иметь множество *различных* технических реализаций. Можно сравнивать два разных предложения по квантовым вычислениям в отношении их технологических достоинств, как сравнивают «хорошее» предложение с «плохим», но даже очень посредственное предложение по квантовому компьютеру в качественном отношении радикально отличается от самого замечательного проекта классического компьютера.

1.6 Квантовая информация

В области квантовых вычислений и квантовой информации термин «квантовая информация» имеет два разных значения. Во-первых, он применяется в качестве общего названия для всех видов деятельности, связанных с обработкой информации на основе квантовой механики. В этом значении он охватывает квантовые вычисления, квантовую телепортацию, теорему о невозможности копирования, и, по существу, все другие темы этой книги.

Во втором значении термин «квантовая информация» гораздо более специализирован: он относится к изучению *элементарных* задач по обработке квантовой информации. Например, он обычно не охватывает построение квантовых алгоритмов, поскольку детали конкретных квантовых алгоритмов выходят за рамки «элементарных». Во избежание путаницы мы будем использовать термин «квантовая теория информации» для этой более специализированной области параллельно с широко распространенным термином «(классическая) теория информации» для описания соответствующей классической области.

Конечно, термин «квантовая теория информации» имеет свой недостаток — можно подумать, что речь идет только о теоретическом рассмотрении! Естественно, это не так, экспериментальная демонстрация элементарных процессов, изучаемых в квантовой теории информации, представляет большой интерес.

Назначение этого раздела — дать введение в основные идеи квантовой теории информации. Даже будучи ограниченной элементарными задачами по обработке квантовой информации, эта теория может выглядеть для начинающего набора из множества как будто не связанных друг с другом предметов, подпадающих под рубрику «квантовая теория информации». Отчасти это объясняется тем, что данная дисциплина все еще находится в состоянии разработки, и пока не ясно, как стыкуются все ее элементы. Однако мы можем выделить несколько фундаментальных целей, придающих единство работе над квантовой теорией информации:

- 1. Определение элементарных классов статических ресурсов в квантовой механике.** Примером служит кубит. Другой пример — бит; классическая физика представляет собой частный случай квантовой физики, поэтому не следует удивляться, что элементарные статические ресурсы, используемые в классической теории информации, должны иметь большее значение в квантовой теории информации. Еще одним примером элементарного класса статических ресурсов является состояние Белла, разделенное между двумя удаленными друг от друга сторонами.
- 2. Определение элементарных классов динамических процессов в квантовой механике.** Простой пример — запоминание, т. е. способность сохранять квантовое состояние на протяжении некоторого периода времени. Менее тривиальными процессами являются передача квантовой информации между двумя сторонами — Алисой и Бобом; копирование (или попытка копирования) квантового состояния, а также защита обрабатываемой квантовой информации от влияния шума.
- 3. Определение затрат ресурсов на реализацию элементарных динамических процессов.** Например, какие минимальные ресурсы требуются для надежной передачи квантовой информации между двумя сторонами при использовании канала связи с шумом?

Подобные задачи ставятся и в классической теории информации; однако квантовая теория информации шире классической, поскольку она включает в себя все статические и динамические элементы классической теории, а также дополнительные статические и динамические элементы.

Далее в этом разделе рассматриваются некоторые вопросы, изучаемые в квантовой теории информации. В каждом случае указываются фундаментальные статические и динамические элементы, а также требования к ресурсам. Мы начнем с примера, который покажется очень знакомым специалистам по классической теории информации: проблемы передачи классической информации по квантовому каналу. Затем мы приступим к изучению новых статических

и динамических процессов квантовой механики, таких как исправление квантовых ошибок, различение квантовых состояний и преобразование запутанности. Глава завершается некоторыми размышлениями о применении инструментов квантовой теории информации в области квантовых вычислений и квантовой информации.

1.6.1 Квантовая теория информации: примеры задач

Классическая информация в квантовых каналах

Фундаментальными результатами классической теории информации являются теорема о кодировании для канала без шума и теорема о кодировании для канала с шумом, доказанные Шенноном. Теорема о кодировании для канала без шума устанавливает, сколько битов требуется для хранения информации, выдаваемой источником информации, а теорема о кодировании для канала с шумом устанавливает, какое количество информации можно надежно передать по каналу связи в присутствии помех.

Что мы понимаем под *источником информации*? Определение этого понятия является фундаментальной проблемой классической и квантовой теорий информации, к которой мы будем неоднократно возвращаться. Пока что дадим такое предварительное определение: источник классической информации описывается набором вероятностей $p_j, j = 1, 2, \dots, d$. Каждое обращение к источнику приводит к выдаче «буквы» j , выбираемой случайным образом с вероятностью p_j независимо от предыдущих обращений к источнику. Например, если источник представляет собой английский текст, то числа j могут соответствовать буквам алфавита и знакам препинания, а вероятности p_j — давать относительные частоты, с которыми различные буквы встречаются в обычном английском тексте. Хотя на самом деле в английском языке буквы не встречаются независимо, для наших целей это будет достаточно хорошим приближением.

Обычный английский текст в значительной степени избытен, и этой избыточностью можно воспользоваться для *сжатия* текста. Например, буква «е» встречается в обычном английском тексте гораздо чаще буквы «з». Следовательно, в хорошем алгоритме сжатия английского текста для представления буквы «е» будет использоваться меньше битов информации, чем для представления буквы «з». Теорема Шеннона о кодировании для канала без шума определяет, насколько хорошо можно заставить работать такой алгоритм сжатия. Точнее говоря, эта теорема утверждает следующее: классический источник, описываемый вероятностями p_j , может быть сконструирован так, что результат каждого обращения к источнику можно представить в среднем при помощи $H(p_j)$ битов информации, где $H(p_j) \equiv -\sum_j p_j \log(p_j)$ есть функция распределения вероятностей источника, называемая *энтропией Шеннона*. Более того, теорема о кодировании для канала без шума устанавливает, что попытка представить источник при помощи меньшего числа битов приведет к большой вероятно-

сти ошибки при развертывании текста. (В гл. 12 эта теорема рассматривается намного подробнее.)

Теорема Шеннона о кодировании для канала без шума служит хорошим примером одновременного достижения всех перечисленных выше целей, стоящих перед теорией информации. Определены два статических ресурса (цель номер 1): бит и источник информации. Определен двухэтапный динамический процесс (цель 2) — сжатие данных от источника информации и последующее их развертывание для восстановления информации. Наконец, найден количественный критерий для определения ресурсов (цель 3), потребляемых оптимальным алгоритмом сжатия данных.

Второй значительный результат Шеннона — теорема о кодировании информации для канала с шумом — устанавливает, какое количество информации может быть надежно передано по каналу в присутствии помех. Предположим, в частности, что мы хотим передать информацию, выдаваемую некоторым источником, в другое место по каналу с шумом, которое может находиться в другой точке пространства или времени — в последнем случае речь идет о хранении информации в присутствии шума. В обоих случаях идея состоит в том, чтобы закодировать выдаваемую информацию при помощи кодов, исправляющих ошибки, так, чтобы любой шум, внесенный каналом, можно было устраниить на другом конце этого канала. В кодах, исправляющих ошибки, это достигается за счет введения в посылаемую по каналу информацию избыточности, достаточной для того, чтобы даже после искажения некоторой части информации можно было восстановить исходное сообщение. Предположим, например, что по каналу с шумом передаются одиночные биты, а шум в канале таков, что для достижения надежной передачи каждый бит, выдаваемый источником, необходимо перед пересылкой по каналу кодировать двумя битами. Говорят, что такой канал имеет *пропускную способность* в половину бита, поскольку каждое обращение к каналу можно использовать для надежной доставки примерно половины бита информации. Шенноновская теорема о кодировании для канала с шумом дает общую процедуру для вычисления пропускной способности произвольного канала с шумом.

В теореме Шеннона о кодировании для канала с шумом также достигаются все три стоящие перед теорией информации цели, о которых говорилось выше. Используются два типа статических ресурсов (цель 1) — источник информации и биты, пересылаемые по каналу, и три динамических процесса (цель 2). Основной процесс — это шум в канале. Чтобы уменьшить шум, мы выполняем дополняющие друг друга процедуры кодирования и декодирования состояния, применяя код, исправляющий ошибки. Для заданной модели шума теорема Шеннона устанавливает, какую избыточность должна внести оптимальная схема исправления ошибок, чтобы достичь надежной передачи информации (цель 3).

В обеих теоремах о кодировании Шеннон ограничился хранением выходных данных источника информации в классических системах — битах и им подобных. В квантовой теории информации встает естественный вопрос — что произойдет, если изменить среду хранения так, чтобы классическая информа-

ция передавалась при помощи квантовых состояний. Например, Алиса может захотеть сжать некоторую классическую информацию, выдаваемую источником, и передать сжатую информацию Бобу, который затем развернет ее. Если в качестве среды хранения сжатой информации используется квантовое состояние, то теорема Шеннона о кодировании для канала без шума неприменима для определения оптимального алгоритма сжатия и развертывания. Например, интересно узнать, позволяет ли использование кубитов получить лучшее сжатие, чем в классическом случае. В гл. 12 мы разберем этот вопрос и докажем, что на самом деле кубиты не обеспечивают никакого существенного выигрыша в объеме данных, требуемых для передачи информации по каналу без шума.

Естественно, что следующим шагом является исследование проблемы передачи классической информации по квантовому каналу с *шумом*. В идеале нам нужен результат, который позволял бы определять *пропускную способность* такого канала применительно к передаче информации. Вычисление пропускной способности — это очень хитроумная работа по нескольким причинам. Квантовая механика, используя непрерывное пространство, дает нам огромное разнообразие моделей шума, и совсем не очевидно, как приспособить классические методы исправления ошибок для борьбы с этим шумом. Можно ли, например, получить выигрыш, если кодировать классическую информацию при помощи *запутанных* состояний и передавать их затем друг за другом по каналу с шумом? Или, может быть, выгодно проводить декодирование при помощи запутанных измерений? В гл. 12 мы докажем *теорему ХШВ* (*Холево-Шумахера-Вестморленда*), которая устанавливает нижний предел пропускной способности такого канала. Вообще, принято считать, что теорема ХШВ дает точное значение пропускной способности, хотя полного доказательства этого до сих пор неизвестно! Под вопросом остается только возможность использования кодирования при помощи запутанных состояний для увеличения пропускной способности сверх нижнего предела, установленного теоремой ХШВ. Все известные на сегодня факты свидетельствуют, что это не поможет увеличить пропускную способность, но определение истинности или ложности такого предположения пока остается интересной открытой проблемой квантовой теории информации.

Квантовая информация в квантовых каналах

Конечно, классическая информация — это не единственный статический ресурс, доступный в квантовой механике. Квантовые состояния сами являются естественным статическим ресурсом, даже более естественным, чем классическая информация. Рассмотрим различные квантовые аналоги теорем Шеннона о кодировании применительно к сжатию и развертыванию квантовых состояний.

Сначала нам нужно определить квантовое понятие источника информации по аналогии с классическим определением. Как и в классическом случае, это можно сделать несколькими разными способами, но для определенности мы остановимся на предварительном варианте, считая, что квантовый источник описывается набором вероятностей p_j и соответствующих квантовых состояний

$|\psi_j\rangle$. Каждое обращение к источнику дает состояние $|\psi_j\rangle$ с вероятностью p_j , причем разные обращения к источнику не зависят друг от друга.

Можно ли сжать выходные данные такого квантовомеханического источника? Рассмотрим случай источника кубитов, который выдает состояние $|0\rangle$ с вероятностью p и состояние $|1\rangle$ с вероятностью $1 - p$. По существу, он ничем не отличается от классического источника, выдающего одиничный бит 0 с вероятностью p или 1 с вероятностью $1 - p$, поэтому неудивительно, что с помощью подобных методов можно сжать источник так, что для хранения сжатой информации потребуется только $H(p, 1 - p)$ кубитов, где $H(\cdot)$ — снова функция энтропии Шеннона.

А если источник выдает состояние $|0\rangle$ с вероятностью p и состояние $(|0\rangle + |1\rangle)/\sqrt{2}$ с вероятностью $1 - p$? Стандартные методы сжатия классических данных больше не применимы, поскольку в общем случае мы не можем различать состояния $|0\rangle$ и $(|0\rangle + |1\rangle)/\sqrt{2}$. Можно ли по-прежнему выполнять операцию сжатия какого-либо типа?

Оказывается, что сжатие некоторого типа возможно даже в этом случае. Интересно, что оно может перестать быть *безошибочным* в том смысле, что квантовые состояния на выходе источника могут слегка искажаться процедурой сжатия-развертывания. Тем не менее, мы требуем, чтобы это искажение становилось очень малым и, в конце концов, пренебрежимо малым при переходе к сжатию больших блоков выходных данных источника. Чтобы количественно охарактеризовать искажения, введем для алгоритма сжатия меру *совпадения* (*fidelity*), которое определяет среднее искажение, вносимое этим алгоритмом. Идея сжатия квантовых данных состоит в том, что сжатые данные должны восстанавливаться с очень большой точностью. Рассматривайте меру совпадения как аналог вероятности корректного выполнения развертывания — в пределе больших длин блоков она должна стремиться к 1, что означает отсутствие ошибок.

Теорема Шумахера о кодировании для канала без шума устанавливает, какое количество ресурсов требуется для сжатия квантовых данных при условии, что источник можно восстановить с точностью, близкой к 1. В случае источника, выдающего ортогональные квантовые состояния $|\psi_j\rangle$ с вероятностями p_j , теорема Шумахера сводится к утверждению о том, что возможно сжатие не более, чем до классического предела $H(p_j)$. Однако, в более общем случае неортогональных состояний, выдаваемых источником, теорема Шумахера устанавливает до какого предела их можно сжать. Оказывается, что здесь нужно использовать *не* шенноновскую энтропию $H(p_j)$, а новую энтропийную величину — *энтропию фон Неймана!* Энтропия фон Неймана совпадает с энтропией Шеннона тогда и только тогда, когда состояния $|\psi_j\rangle$ ортогональны. В противном случае энтропия фон Неймана для источника p_j , $|\psi_j\rangle$ в общем случае строго *меньше* чем энтропия Шеннона $H(p_j)$. Так, например, в случае источника, который выдает состояние $|0\rangle$ с вероятностью p и $(|0\rangle + |1\rangle)/\sqrt{2}$ с вероятностью $1 - p$, можно надежно произвести сжатие с использованием меньшего, чем $H(p, 1 - p)$, числа кубитов в расчете на одно обращение к источнику!

Основную причину такого уменьшения требуемых ресурсов достаточно легко понять. Предположим, что источник, выдающий состояния $|0\rangle$ с вероятностью p и $(|0\rangle+|1\rangle)/\sqrt{2}$ с вероятностью $1-p$, использует большое число раз n . Тогда по закону больших чисел источник с большой вероятностью выдаст примерно np копий $|0\rangle$ и $n(1-p)$ копий $(|0\rangle+|1\rangle)/\sqrt{2}$. Это можно записать в виде

$$|0\rangle^{\otimes np} \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}} \right)^{\otimes n(1-p)}, \quad (1.60)$$

с точностью до перестановки используемых систем. Раскроем скобки в формуле (1.60). Поскольку $n(1-p)$ велико, можно снова использовать закон больших чисел и сделать вывод, что каждое слагаемое будет произведением, в котором примерно половина членов $|0\rangle$ и половина $|1\rangle$. Иначе говоря, произведение множителей $|0\rangle + |1\rangle$ можно с хорошей точностью аппроксимировать суперпозицией состояний вида

$$|0\rangle^{\otimes n(1-p)/2} |1\rangle^{\otimes n(1-p)/2}. \quad (1.61)$$

Следовательно, выдаваемое источником состояние можно аппроксимировать суперпозицией членов вида

$$|0\rangle^{\otimes n(1+p)/2} |1\rangle^{\otimes n(1-p)/2}. \quad (1.62)$$

Сколько существует состояний данного вида? Грубо говоря, это число сочетаний из n по $n(1+p)/2$, что по формуле Стирлинга равно $N \equiv 2^{nH[(1+p)/2, (1-p)/2]}$. Тогда простой метод сжатия будет заключаться в том, чтобы пометить все состояния вида (1.62) как $|c_1\rangle \dots |c_N\rangle$. Над n кубитами, выданными источником, можно выполнить унитарное преобразование, которое переводит $|c_j\rangle$ в $|j\rangle |0\rangle^{\otimes n-nH[(1+p)/2, (1-p)/2]}$, поскольку j есть $nH[(1+p)/2, (1-p)/2]$ -битовое число. Операция сжатия состоит в том, чтобы выполнить это унитарное преобразование и отбросить последние $n-nH[(1+p)/2, (1-p)/2]$ кубитов, оставив сжатое состояние из $nH[(1+p)/2, (1-p)/2]$ кубитов. Для развертывания мы добавляем к сжатому состоянию состояние $|0\rangle^{\otimes n-nH[(1+p)/2, (1-p)/2]}$ и выполняем обратное унитарное преобразование.

Эта процедура сжатия и развертывания квантовых данных требует памяти в размере $H[(1+p)/2, (1-p)/2]$ кубитов на одно обращение к источнику, что при $p > 1/3$ дает улучшение по сравнению с $H(p, 1-p)$ кубитами, которых мы могли бы наивно ожидать согласно теореме Шеннона о кодировании для канала без шума. Фактически, как мы увидим в гл. 12 теорема Шумахера о кодировании для канала без шума дает несколько лучшую оценку, однако такое более сильное сжатие возможно по той же причине, что и в приведенном примере: мы используем тот факт, что состояния $|0\rangle$ и $(|0\rangle+|1\rangle)/\sqrt{2}$ неортогональны. С интуитивной точки зрения эти состояния содержат некоторую избыточность, поскольку оба имеют компоненту в направлении $|0\rangle$, что приводит к большему физическому сходству, чем получалось бы для ортогональных состояний. Именно этой избыточностью мы воспользовались в только что описанном алгоритме кодирования, и она же используется в полном доказательстве теоремы Шумахера о кодировании для канала с шумом. Заметим, что ограничение

$p > 1/3$ возникает из-за того, что при $p \leq 1/3$ данный алгоритм не использует избыточность состояний: в результате мы фактически приходим к *увеличению* избыточности! Конечно, это особенность конкретного алгоритма, который мы выбрали, и в общем решении сжатие данных достигается за счет гораздо более рационального использования избыточности.

Теорема Шумахера о кодировании для канала без шума является аналогом теоремы Шеннона о кодировании для канала без шума применительно к сжатию и развертыванию квантовых состояний. Можно ли найти аналог теоремы Шеннона о кодировании для канала с шумом? Благодаря использованию теории кодов, исправляющих квантовые ошибки, в этом важном вопросе достигнут большой прогресс, но полного аналога до сих пор не найдено. Некоторые сведения о том, что известно о пропускной способности квантового канала, приводятся в гл. 12.

Квантовая различимость

Все рассмотренные нами динамические процессы — сжатие, развертывание, шум, кодирование и декодирование с использованием кодов, исправляющих ошибки, есть как в классической, так и в квантовой теории информации. Однако введение новых типов информации, таких как квантовые состояния, расширяет класс динамических процессов за рамки тех, что рассматриваются в классической теории информации. Хорошим примером является проблема различения квантовых состояний. Мы привыкли, что в классическом случае есть возможность различать неодинаковые элементы информации, по крайней мере, в принципе. Конечно, на практике смазанная буква «*a*» на странице может быть трудноотличима от буквы «*o*», но в принципе возможно достоверно различать два различных варианта.

В квантовомеханическом случае, напротив, *не* всегда можно различить произвольные состояния. Например, не существует такого процесса, допускаемого квантовой механикой, который бы позволил надежно различать состояния $|0\rangle$ и $(|0\rangle+|1\rangle)/\sqrt{2}$. Строгое доказательство этого факта требует инструментов, которых у нас пока нет (см. гл. 2), но на примерах очень легко убедиться, что это различение невозможно. Предположим, например, что мы пытаемся различить два состояния путем измерения в вычислительном базисе. Если у нас есть состояние $|0\rangle$, то измерение будет давать 0 с вероятностью 1. Но когда мы измеряем $(|0\rangle+|1\rangle)/\sqrt{2}$, измерение дает 0 с вероятностью $1/2$ и 1 с вероятностью $1/2$. Таким образом, хотя результат 1 подразумевает, что состоянием должно быть $(|0\rangle+|1\rangle)/\sqrt{2}$ (поскольку состояния $|0\rangle$ здесь быть не может), по результату 0 мы никак не можем идентифицировать квантовое состояние.

Эта неразличимость неортогональных квантовых состояний лежит в основе квантовых вычислений и квантовой информации. Она составляет суть нашего утверждения о том, что квантовое состояние содержит скрытую информацию, недоступную для измерения, и тем самым играет ключевую роль в квантовых алгоритмах и квантовой криптографии. Одной из центральных проблем квантовой теории информации является разработка мер для количественного определения степени различимости неортогональных квантовых состояний:

этой теме посвящена значительная часть глав 9 и 12. В этом введении мы ограничимся указанием на два интересных аспекта неразличимости — ее связи с возможностью передачи информации со скоростью, превышающей скорость света, и применению в «квантовых деньгах».

Предположим, что мы сможем различать произвольные квантовые состояния. Покажем, что отсюда следует возможность связи со скоростью, превышающей скорость света, при помощи запутанности. Пусть Алиса и Боб имеют общую запутанную пару кубитов в состоянии $(|00\rangle + |11\rangle)/\sqrt{2}$. Тогда, если Алиса проводит измерение в вычислительном базисе, состоянием после измерения будет $|0\rangle$ с вероятностью $1/2$ и $|1\rangle$ с вероятностью $1/2$. Но предположим, что Алиса измеряет в базисе $|+\rangle, |-\rangle$. Вспомните, что $|0\rangle = (|+\rangle + |-\rangle)/\sqrt{2}$, а $|1\rangle = (|+\rangle - |-\rangle)/\sqrt{2}$. Простые алгебраические выкладки показывают, что начальное состояние системы Алисы и Боба можно переписать как $|0\rangle = (|++\rangle + |--\rangle)/\sqrt{2}$. Следовательно, если Алиса измеряет в базисе $|+\rangle, |-\rangle$, то состоянием системы Боба после измерения будет $|+\rangle$ или $|-\rangle$ с вероятностью $1/2$. Пока все это элементарная квантовая механика. Но если бы Боб имел доступ к устройству, которое может различать четыре состояния $|0\rangle, |1\rangle, |+\rangle$ и $|-\rangle$, то он мог бы сказать, измеряла ли Алиса в вычислительном базисе или в базисе $|+\rangle, |-\rangle$. Более того, он мог бы получить эту информацию *мгновенно*, как только Алиса провела измерение, что позволило бы Алисе и Бобу осуществлять связь быстрее света! Конечно, мы знаем, что невозможно различать неортогональные квантовые состояния; этот пример показывает, что данное ограничение тесно связано с другими физическими законами, которым, как мы полагаем, подчиняется мир.

Неразличимость неортогональных квантовых состояний не всегда является препятствием. Иногда она может быть полезна. Представьте, что банк выпустил банкноты с впечатанным (классическим) серийным номером и последовательностью кубитов, каждый из которых находится либо в состоянии $|0\rangle$, либо в состоянии $(|0\rangle + |1\rangle)/\sqrt{2}$. Никто, кроме банка, не знает, какая последовательность этих двух состояний внедрена в банкноту, и банк ведет список, в котором серийные номера сопоставляются с внедренными состояниями. Банкноту невозможно подделать абсолютно точно, поскольку потенциальный фальшивомонетчик не может с достоверностью определить состояние кубитов в исходной банкноте, не разрушив их. Получив банкноту, продавец (или уполномоченное лицо) может проверить ее подлинность, позвонив в банк, сообщив серийный номер и спросив, какая последовательность состояний была внедрена в банкноту, а затем измерив кубиты в базисе $|0\rangle, |1\rangle$ или $(|0\rangle + |1\rangle)/\sqrt{2}, (|0\rangle - |1\rangle)/\sqrt{2}$, как указано банком. С вероятностью, экспоненциально стремящейся к единице с ростом числа проверенных кубитов, любой потенциальный фальшивомонетчик будет выявлен на этой стадии! Эта идея лежит в основе множества других квантовых криптографических протоколов, и демонстрирует, какую пользу может приносить неразличимость неортогональных квантовых состояний.

Упражнение 1.2. Объясните, как использовать устройство, правильно идентифицирующее одно из двух поданных на его вход неортогональных квантовых состояний $|\psi\rangle$ или $|\varphi\rangle$, для построения другого устройства, копирующего состо-

яния $|\psi\rangle$ и $|\varphi\rangle$ в нарушение теоремы о невозможности копирования. И наоборот, объясните, как использовать устройство для копирования с целью различия неортогональных квантовых состояний.

Создание и преобразование запутанности

Запутанность представляет собой еще один элементарный статический ресурс квантовой механики. Его свойства поразительно отличаются от свойств ресурсов, знакомых, главным образом, по классической теории информации, и они еще не очень хорошо поняты; максимум, что у нас есть — это неполная подборка результатов, относящихся к запутанности. Рассмотрим здесь хотя бы две теоретико-информационные проблемы, связанные с запутанностью.

Создание запутанности — это простой динамический процесс, изучаемый в квантовой теории информации. Сколькими кубитами должны обменяться две стороны, чтобы создать заданное запутанное состояние, разделенное между ними, при условии, что перед этим они не разделяли никакой запутанности? Второй динамический процесс, который представляет интерес — это *преобразование запутанности* из одной формы в другую. Предположим, например, что состояние Белла разделено между Алисой и Бобом и они хотят преобразовать его в запутанное состояние какого-то другого типа. Какие ресурсы им потребуются для выполнения этой задачи? Смогут ли они это сделать, не устанавливая связи? Достаточно ли только классической связи? Если необходима квантовая связь, то сколько понадобится квантовых передач?

Поиск ответов на эти и более сложные вопросы о создании и преобразовании запутанности приводит к формированию самостоятельной захватывающей области исследований, а также обещает облегчить понимание таких задач, как квантовые вычисления. Например, распределенное квантовое вычисление можно рассматривать просто как метод создания запутанности между двумя и более сторонами; тогда нижние пределы количества передач, необходимых для выполнения такого распределенного квантового вычисления, определяются **нижними** пределами количества передач, которое требуется для создания подходящих запутанных состояний.

1.6.2 Квантовая информация в более широком контексте

Мы дали лишь самое поверхностное представление о квантовой теории информации. В части III этой книги квантовая теория информации рассматривается гораздо подробнее, особенно в гл. 11, где речь идет о фундаментальных свойствах энтропии в квантовой и классической теории информации, и в гл. 12, где основное внимание уделяется чисто квантовой теории информации.

Квантовая теория информации представляет собой наиболее абстрактную часть области квантовых вычислений и квантовой информации, а в некотором смысле и наиболее фундаментальную. Развитие квантовой теории информации и, в конечном счете, всей сферы квантовых вычислений и квантовой информации стимулирует следующие вопросы. *Что делает возможным обработку*

квантовой информации? Что разделяет квантовый и классический миры? Какие ресурсы, недоступные в классическом мире, могут использоваться в квантовых вычислениях? Существующие ответы на эти вопросы туманны и неполны; но мы надеемся, что в грядущие годы туман все-таки сможет рассеяться, и мы получим четкое представление о возможностях и ограничениях обработки квантовой информации.

Задача 1.1 (диалог Фейнмана с Гейтсом). Придумайте дружелюбную дискуссию (примерно из 2000 слов) между Биллом Гейтсом и Ричардом Фейнманом, происходящую сейчас и посвященную будущему вычислений. (*Комментарий.* Возможно, вам стоит прочитать всю книгу, прежде чем приступить к этому вопросу. См. ниже разд. «История и дополнительная литература», где приведены указания к одному из возможных ответов.)

Задача 1.2. Какое самое значительное открытие сделано к настоящему времени в области квантовых вычислений и квантовой информации? Напишите очерк (примерно из 2000 слов) об этом открытии для образованной, но непрофессиональной аудитории. (*Комментарий.* Как и в случае предыдущей задачи, вам, возможно, стоит прочесть всю книгу, прежде чем отвечать на поставленный вопрос.)

История и дополнительная литература

Большая часть материала этой главы рассматривается более подробно в последующих главах. В связи с этим, приведенные ниже исторические ссылки и дополнительная литература относятся лишь к материалу, который в этих главах не затрагивается.

Чтобы показать, как развивалась область квантовых вычислений и квантовой информации, требуется дать широкий обзор истории многих других областей. В настоящей главе мы попытались это сделать, но много базового материала неизбежно пришлось опустить из-за нехватки места (и компетенции). Приводимые ниже рекомендации направлены на то, чтобы исправить это упущение.

Об истории квантовой механики рассказывалось во многих изданиях. Мы особенно рекомендуем выдающиеся работы Пэ [309, 310, 311]. Из этих трех наиболее прямое отношение к развитию квантовой механики имеет [310]; однако приводимые Пэ биографии Эйнштейна [309] и Бора [311] также содержат много интересного материала, хотя и на менее сложном уровне. Возникновение технологий, основанных на квантовой механике, описано Мильбурном [285, 286]. Безусловно стоит прочитать изумительную работу Тьюринга по основам информатики [388]. Ее можно найти в ценной исторической коллекции, которую представляют собой книги Дэвиса [113], Хофтадтера [189] и Пенроуза [316], содержащие занимательные и информативные обсуждения основ информатики. Биографии пятидесяти ведущих специалистов по информатике, приведенные у Шаша и Лецера [362], проливают свет на многие различные аспекты истории этой дисциплины. Наконец, удивительно много исторической информации содержится во впечатительной серии книг Кнута [224, 225, 226].

Блестящие работы Шеннона [353], заложившие основы теории информации (перепечатаны также в [378]) — отличный материал для чтения. Книга Маквилльямса и Слоуна [296] не только представляет собой превосходный учебник по кодам, исправляющим ошибки, но и содержит невероятное количество полезной исторической информации. Подобна ей книга Ковера и Томаса [106] — великолепный учебник по теории информации с обширными историческими сведениями. В большом томе [379] под редакцией Слоуна и Винера представлено собрание работ Шеннона вместе с множеством полезных исторических заметок. Полезная коллекция репринтов по теории информации собрана Слепяном [363]. Криптография — это древнее искусство с запутанной и часто интересной историей. Книга Кана [207] представляет собой гигантский труд по истории криптографии, содержащий изобилие информации. По более свежим разработкам мы рекомендуем книги Менезеса, Ван Ооршота и Ванстоуна [298], Шнейера [351], а также Диффи и Ландау [127].

Квантовую телепортацию открыли Беннет, Брассард, Крепо, Йожа, Перес и Вутерс [23], а позже она была экспериментально реализована в самых разных формах: с использованием оптических методов (Боши, Бранка, Де Мартини, Харди и Попеску [29]), поляризации фотонов (Баумейстер, Пан, Меттл, Эйбл, Вайнфуртэр и Цайлингер [66]), «сжатых» состояний света (Фурусава, Зоренсен, Браунштейн, Фукс, Кимбл и Пользик [155]) и ЯМР (Нильсен, Нилл и Лафлам [306]).

Задача Дойча была сформулирована Дойчем [117], и в той же работе приведено ее однобитовое решение. Обобщение на n -битовый случай было дано Дойчем и Йожа [126]. Алгоритмы, предложенные в этих работах, впоследствии были значительно усовершенствованы Кливом, Экертом, Маккиавелло и Моща [80], а также независимо от них Таппом в его неопубликованной работе. В этой главе мы представили усовершенствованную версию алгоритма, которая очень хорошо вписывается в контекст задачи о скрытой подгруппе, обсуждаемой в гл. 5. Первоначальный алгоритм Дойча работал только вероятностным образом; Дойч и Йожа усовершенствовали его, получив детерминированный вариант, но их метод требовал двух вычислений функции в отличие от усовершенствованных алгоритмов, представленных в этой главе. Тем не менее, на эти алгоритмы по-прежнему принято ссылаться как на алгоритм Дойча и алгоритм Дойча-Йожа в память о двух огромных шагах вперед: конкретной демонстрации Дойчем того факта, что квантовый компьютер потенциально может работать быстрее классического компьютера, и общению, сделанному Дойчем и Йожа, которое впервые продемонстрировало аналогичное расхождение в масштабах времени, требуемого для решения задачи.

Превосходное обсуждение эксперимента Штерна–Герлаха можно найти в стандартных учебниках по квантовой механике, таких как учебники Сакураи [346], Фейнмана, Лейтона и Сендса (том III) [151], а также Кохена–Танноуджи, Диу и Лалоэ [107, 108].

Задача 1.1 была предложена в замечательной статье Рахима [332].

Глава 2

ВВЕДЕНИЕ В КВАНТОВУЮ МЕХАНИКУ

Я вовсе не физик, но знаю, что к чему.

Попай-моряк

Квантовая механика — настоящая черная магия.

Альберт Эйнштейн

Квантовая механика — наиболее точное и полное из известных описаний нашего мира. Она также является основой для понимания принципов квантовых вычислений и обработки квантовой информации. В данной главе приводятся все необходимые для этого сведения. Никаких предварительных знаний о квантовой механике для понимания этой главы не требуется.

Несмотря на репутацию сложной для восприятия науки, изучить квантовую механику легко. Такая репутация возникла из-за трудности усвоения некоторых несущественных для ее понимания *применений*, например определения структуры сложных молекул, мы их обсуждать не будем. Единственное необходимое условие для усвоения данного введения в квантовую механику — минимальное знакомство с линейной алгеброй. Читатель, обладающий соответствующими познаниями, сможет за несколько часов научиться решать простейшие квантовомеханические задачи.

Тот, кто знаком с основами квантовой механики, может бегло просмотреть эту главу, чтобы ознакомиться с используемыми здесь обозначениями (по большей части совпадающими с общепринятыми) и освежить в памяти материал. Те же читатели, которые не изучали данный предмет, должны внимательно прочитать эту главу и попытаться выполнить все упражнения. При возникновении сложностей с той или иной задачей следует продолжить чтение и вернуться к этой задаче позже.

Глава начинается с разд. 2.1, где приведены необходимые сведения из линейной алгебры. При этом предполагается знакомство читателя с элементарной линейной алгеброй, но вводятся принятые у физиков обозначения, которые несколько отличаются от используемых в большинстве вводных курсов по данному предмету. Разд. 2.2 посвящен основным постулатам квантовой механики и содержит все ее фундаментальные принципы. Приведено большое количество простых упражнений, позволяющих лучше усвоить материал. В оставшейся части этой главы (да и всей книги) этот материал разъясняется уже

без привлечения каких-либо новых физических принципов. В разд. 2.3 объясняется идея *сверхплотного кодирования* — удивительного примера обработки квантовой информации, сочетающего в простой конструкции сразу несколько постулатов квантовой механики. В разд. 2.4 и 2.5 описаны мощные математические средства — *оператор плотности*, *расширение до чистого состояния* и *разложение Шмидта*, которые особенно полезны при изучении квантовых вычислений и квантовой информации. Знакомство с ними поможет закрепить понимание элементарной квантовой механики. Наконец, в разд. 2.6 изучен вопрос о выходе квантовой механики за пределы обычного «классического» понимания того, как устроен наш мир.

2.1 Линейная алгебра

Эта книга написана настолько же для того, чтобы беспокоить и досаждать, насколько и для того, чтобы наставлять.

Б. Хоффман¹

Жизнь комплексна — у нее есть и действительная, и мнимая компоненты.

Неизвестный

Линейная алгебра изучает векторные пространства и линейные операции в них. Для хорошего понимания квантовой механики необходимо уверенно разбираться в элементарной линейной алгебре. В этом разделе мы введем основные понятия линейной алгебры и опишем стандартные обозначения, которые используются для этих понятий в квантовой механике. Эти обозначения отображены на рис. 2.1: в левой колонке — квантовомеханические символы, в правой — их описание в терминах линейной алгебры. Взгляните на таблицу, чтобы понять, сколько терминов из правой колонки вам знакомо.

По нашему мнению, главным препятствием при знакомстве с постулатами квантовой механики являются не сами постулаты, а достаточно большое количество терминов из линейной алгебры, необходимое для их понимания. Вместе с необычными обозначениями Дирака, используемыми физиками в квантовой механике, это может (ошибочно!) показаться совершенно пугающим. Поэтому мы советуем не знакомому с квантовой механикой читателю бегло просмотреть следующий ниже материал, стараясь усвоить лишь самое необходимое. После этого стоит приступить к изучению основного материала главы — постулатов квантовой механики, — возвращаясь по мере надобности к изучению необходимых алгебраических понятий и обозначений.

Основными объектами линейной алгебры являются *векторные пространства*. Для нас наибольший интерес представляет пространство \mathbb{C}^n , т. е. множество n -элементных наборов комплексных чисел: (z_1, \dots, z_n) . Элементы век-

¹ Хоффман Б. О векторах

торного пространства называются *векторами*; иногда мы будем использовать для векторов матричные обозначения

$$\begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix}. \quad (2.1)$$

В векторном пространстве определена операция *сложения* для пары векторов. В пространстве \mathbf{C}^n операция сложения вводится следующим образом:

$$\begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix} + \begin{bmatrix} z'_1 \\ \vdots \\ z'_n \end{bmatrix} \equiv \begin{bmatrix} z_1 + z'_1 \\ \vdots \\ z_n + z'_n \end{bmatrix}; \quad (2.2)$$

здесь в правой части имеется в виду обычное сложение комплексных чисел. Определим операцию *умножения вектора на скаляр*. В пространстве \mathbf{C}^n эта операция задается тождеством

$$z \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix} \equiv \begin{bmatrix} zz_1 \\ \vdots \\ zz_n \end{bmatrix}, \quad (2.3)$$

где z — *скаляр*, т. е. комплексное число, а в правой части подразумевается обычное перемножение комплексных чисел. Физики иногда называют комплексные числа *c-числами*.

Поскольку мы собираемся применять линейную алгебру в квантовой механике, будем придерживаться обозначений, принятых в этом разделе физики. Стандартное квантовомеханическое обозначение для вектора в векторном пространстве выглядит как

$$|\psi\rangle. \quad (2.4)$$

Символ ψ является просто меткой для вектора (подойдет любая метка, но мы обычно будем использовать простые метки: ψ , φ и т. п.). Обозначение $|\cdot\rangle$ используется, чтобы показать, что объект является вектором. Объект $|\psi\rangle$ целиком иногда называют *кет-вектором*, но мы не будем часто использовать такую терминологию.

Векторное пространство содержит также *нулевой вектор*, обозначим его символом « 0 ». Он обладает следующим свойством: $|v\rangle + 0 = |v\rangle$ для любого вектора $|v\rangle$. Обратите внимание, что мы не используем кет-обозначение для нулевого вектора — это будет единственным исключением. Причина заключается в том, что в дальнейшем окажется удобным использовать очевидное обозначение $|0\rangle$ для другого объекта. Операция умножения на скаляр удовлетворяет условию $z0 = 0$ для любого комплексного числа z . Для удобства мы будем писать (z_1, \dots, z_n) , чтобы обозначить вектор-столбец с элементами z_1, \dots, z_n .

В пространстве \mathbf{C}^n нулевым элементом является вектор $(0, 0, \dots, 0)$. *Векторным подпространством* векторного пространства V называется такое подмножество W множества V , которое замкнуто относительно операций сложения и умножения на скаляр, т. е. также является векторным пространством.

Обозначение	Описание
z^*	Число, комплексно-сопряженное с числом z ; $(1+i)^* = 1-i$
$ \psi\rangle$	Вектор (также используется название <i>кет-вектор</i>)
$\langle\psi $	Вектор, <i>двойственный</i> вектору $ \psi\rangle$ (также используется название <i>бра-вектор</i>)
$\langle\varphi \psi\rangle$	Скалярное произведение векторов $ \varphi\rangle$ и $ \psi\rangle$
$ \varphi\rangle \otimes \psi\rangle$	Тензорное произведение векторов $ \varphi\rangle$ и $ \psi\rangle$
$ \varphi\rangle \psi\rangle$	Сокращенное обозначение для тензорного произведения векторов $ \varphi\rangle$ и $ \psi\rangle$
A^*	Матрица, комплексно-сопряженная с матрицей A
A^T	Матрица, получаемая из матрицы A транспонированием
A^\dagger	Матрица, эрмитово-сопряженная с матрицей A , $A^\dagger = (A^T)^*$
$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^\dagger$	$= \begin{bmatrix} a^* & c^* \\ b^* & d^* \end{bmatrix}$
$\langle\varphi A \psi\rangle$	Скалярное произведение векторов $ \varphi\rangle$ и $A \psi\rangle$, другими словами, скалярное произведение векторов $A^\dagger \varphi\rangle$ и $ \psi\rangle$

Рис. 2.1. Перечень основных стандартных квантовомеханических обозначений (обычно называемых обозначениями Дирака) для понятий из курса линейной алгебры

2.1.1 Базисы и линейная независимость

Порождающим множеством векторного пространства называют такой набор векторов $|v_1\rangle, \dots, |v_n\rangle$, что любой вектор $|v\rangle$ данного векторного пространства может быть представлен в виде линейной комбинации $|v\rangle = \sum_i a_i |v_i\rangle$ векторов из этого набора. Например, в качестве порождающего множества векторного пространства \mathbf{C}^2 можно взять набор из двух векторов

$$|v_1\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |v_2\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad (2.5)$$

поскольку любой вектор

$$|v\rangle = \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} \quad (2.6)$$

в пространстве \mathbf{C}^2 может быть записан в виде линейной комбинации $|v\rangle = a_1|v_1\rangle + a_2|v_2\rangle$ векторов $|v_1\rangle$ и $|v_2\rangle$. Мы будем говорить, что векторы $|v_1\rangle$ и $|v_2\rangle$ *порождают* векторное пространство \mathbf{C}^2 .

Вообще говоря, в векторном пространстве можно выбрать различные порождающие множества. Например, в пространстве \mathbf{C}^2 пара векторов

$$|v_1\rangle \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}; \quad |v_2\rangle \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \quad (2.7)$$

также является порождающим множеством, поскольку произвольный вектор $|v\rangle = (a_1, a_2)$ может быть представлен в виде линейной комбинации векторов $|v_1\rangle$ и $|v_2\rangle$:

$$|v\rangle = \frac{a_1 + a_2}{\sqrt{2}}|v_1\rangle + \frac{a_1 - a_2}{\sqrt{2}}|v_2\rangle. \quad (2.8)$$

Ненулевые векторы $|v_1\rangle, \dots, |v_n\rangle$ называются *линейно зависимыми*, если существует такой набор комплексных чисел a_1, \dots, a_n (причем по крайней мере одно из чисел a_i отлично от нуля), что

$$a_1|v_1\rangle + a_2|v_2\rangle + \dots + a_n|v_n\rangle = 0. \quad (2.9)$$

Векторы называются *линейно независимыми*, если они не являются линейно зависимыми. Можно показать, что в любых двух порождающих векторное пространство V наборах линейно независимых векторов содержится одинаковое число векторов. Будем называть любой такой набор *базисом* пространства V . Нас будут интересовать только *конечномерные* векторные пространства, в которых существует конечный базис. Количество элементов в базисе мы будем называть *размерностью* пространства V . Существует много интересных и частную непростых вопросов, связанных с бесконечномерными векторными пространствами, однако мы не будем их касаться.

Упражнение 2.1 (линейная зависимость). Покажите, что векторы $(1, -1)$, $(1, 2)$ и $(2, 1)$ являются линейно зависимыми.

2.1.2 Линейные операторы и матрицы

Линейным оператором, отображающим векторное пространство V в векторное пространство W , называется линейная по своему аргументу функция $A: V \rightarrow W$:

$$A \left(\sum_i a_i |v_i\rangle \right) = \sum_i a_i A(|v_i\rangle). \quad (2.10)$$

Вместо $A(|v\rangle)$ будем использовать обозначение $A|v\rangle$. Будем называть линейный оператор действующим *на* векторном пространстве V , если он переводит V в V . Важным линейным оператором в пространстве V является *тождественный оператор* I_V , определяемый соотношением $I_V|v\rangle \equiv |v\rangle$ для любого вектора $|v\rangle$. Мы будем опускать индекс « V » и обозначать тождественный оператор просто I , если это не может привести к путанице. Другим важным оператором является *нулевой оператор*, для которого используется символ « 0 ». Он отображает все векторы в нулевой вектор $(0|v\rangle \equiv 0)$. Из соотношения (2.10) легко видеть, что если знать значения линейного оператора на всех векторах базиса, то можно определить его значение для любого аргумента.

Пусть V , W и X – векторные пространства, $A: V \rightarrow W$ и $B: W \rightarrow X$ – линейные операторы. Будем использовать обозначение BA для *композиции* операторов B и A (определение: $(BA)(|v\rangle) \equiv B(A(|v\rangle))$). Напомним, что обозначение $BA|v\rangle$ является сокращением для $(BA)(|v\rangle)$.

Удобнее всего научиться работать с линейными операторами в *матричном представлении*. В действительности описания на языках матриц и линейных операторов полностью эквивалентны. Быть может, описание на языке матриц для кого-то более привычно. Чтобы осознать взаимосвязь между этими двумя описаниями, полезно сначала понять, что матрица A размера $m \times n$ с элементами A_{ij} является линейным оператором, соответствующим отображению из векторного пространства \mathbb{C}^n в пространство \mathbb{C}^m : матрица A просто умножается на вектор-столбец из \mathbb{C}^n . Точнее говоря, утверждение, что матрица A — линейный оператор, означает справедливость равенства

$$A \left(\sum_i a_i |v_i\rangle \right) = \sum_i a_i A |v_i\rangle, \quad (2.11)$$

где умножение на A понимается в матричном смысле. Очевидно, что это равенство выполняется тождественно.

Мы только что убедились, что матрицы можно рассматривать как линейные операторы. Можно ли записать линейные операторы в матричном представлении? Оказывается, можно — и сейчас мы объясним, как это делается. Эта эквивалентность двух подходов оправдывает повторяющееся на протяжении всей книги смешивание терминов из теории матриц и теории линейных операторов. Пусть $A: V \rightarrow W$ — линейное отображение из пространства V в пространство W , $|v_1\rangle, \dots, |v_m\rangle$ — базис в V , а $|w_1\rangle, \dots, |w_n\rangle$ — базис в W . Тогда для любого j из диапазона $1, \dots, m$ существуют такие комплексные числа A_{1j}, \dots, A_{nj} , что

$$A|v_j\rangle = \sum_i A_{ij} |w_i\rangle. \quad (2.12)$$

Говорят, что матрица с элементами A_{ij} задает *матричное представление* оператора A . Матричное представление полностью эквивалентно оператору A , и мы будем на равных использовать матричное представление и подход с точки зрения абстрактных операторов. Однако обратите внимание: чтобы установить связь между матрицами и линейными операторами, следует задать базисы в пространствах V и W .

Упражнение 2.2 (матричные представления). Пусть V — векторное пространство с базисными векторами $|0\rangle$ и $|1\rangle$, A — такое линейное отображение из V в V , что $A|0\rangle = |1\rangle$, $A|1\rangle = |0\rangle$. Запишите матричное представление оператора A , используя базис $|0\rangle, |1\rangle$ в пространстве аргументов и базис $|0\rangle, |1\rangle$ в пространстве значений. Придумайте базисы, которые приведут к другому матричному представлению оператора A .

Упражнение 2.3 (матричное представление произведения операторов). Пусть A — линейный оператор, отображающий векторное пространство V в векторное пространство W , B — линейный оператор, отображающий W в векторное пространство X ; $|v_i\rangle, |w_j\rangle$ и $|x_k\rangle$ — соответственно базисы в пространствах V, W и X . Покажите, что матричное представление линейного отображения BA представляет собой произведение матриц, отвечающих матричным представлениям отображений A и B , записанных в соответствующих базисах.

Упражнение 2.4 (матричное представление для тождественного преобразования). Покажите, что матричное представление тождественного оператора в векторном пространстве V имеет вид матрицы, в которой на главной диагонали стоят единицы, а все остальные элементы — нули (предполагается, что для аргумента и значения оператора используется один и тот же базис). Такая матрица называется *единичной*.

2.1.3 Матрицы Паули

Мы будем часто использовать четыре *матрицы Паули*. Это матрицы размера 2×2 , которые имеют разные обозначения. Матрицы Паули и используемые для них обозначения представлены на рис. 2.2. Указанные матрицы настолько полезны в теории квантовых вычислений и квантовой информации, что мы настоятельно рекомендуем вам запомнить их, обратив особое внимание на приведенные ниже задачи и упражнения, где они используются.

$$\begin{aligned}\sigma_0 \equiv I &\equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & \sigma_1 \equiv \sigma_x \equiv X &\equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\ \sigma_2 \equiv \sigma_y \equiv Y &\equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} & \sigma_3 \equiv \sigma_z \equiv Z &\equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\end{aligned}$$

Рис. 2.2. Матрицы Паули Иногда матрицами Паули называют только X , Y и Z , опуская матрицу I .

2.1.4 Скалярное произведение

Скалярное произведение является функцией, отображающей множество пар векторов во множество комплексных чисел. Сейчас нам будет удобно записывать скалярное произведение векторов $|v\rangle$ и $|w\rangle$ как $(|v\rangle, |w\rangle)$. Это обозначение не является стандартным для квантовой механики; в педагогических целях обозначение будет изредка использоваться в этой главе. Стандартное квантово-механическое обозначение для скалярного произведения $(|v\rangle, |w\rangle)$ выглядит как $\langle v|w\rangle$, где $|v\rangle$ и $|w\rangle$ — векторы в исходном пространстве со скалярным произведением, а через $|v\rangle$ обозначен *вектор, двойственный* вектору $|v\rangle$. Это — *линейный функционал* (линейное отображение) из пространства V во множество комплексных чисел \mathbb{C} , определенный соотношением $\langle v|(|w\rangle) \equiv \langle v|w\rangle \equiv (|v\rangle, |w\rangle)$. Вскоре мы увидим, что в матричном представлении двойственному вектору соответствует вектор-строка.

Функция (\cdot, \cdot) из $V \times V$ в \mathbb{C} является скалярным произведением, если она удовлетворяет следующим условиям:

1. функция (\cdot, \cdot) линейна по второму аргументу, т. е.

$$\left(|v\rangle, \sum_i \lambda_i |w_i\rangle \right) = \sum_i \lambda_i (|v\rangle, |w_i\rangle); \quad (2.13)$$

$$2. (|v\rangle, |w\rangle) = (\langle w|, \langle v|)^*;$$

$$3. (\langle v|, \langle v|) \geq 0, \text{ причем равенство достигается тогда и только тогда, когда } |\psi\rangle = 0.$$

Например, в пространстве \mathbb{C}^n скалярное произведение можно определить следующим образом:

$$((y_1, \dots, y_n), (z_1, \dots, z_n)) \equiv \sum_i y_i^* z_i = [y_1^* \dots y_n^*] \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix}. \quad (2.14)$$

Векторное пространство с заданным на нем скалярным произведением называется *пространством со скалярным произведением* (либо унитарным или эрмитовым пространством).

Упражнение 2.5. Проверьте, что определенная выше функция (\cdot, \cdot) является скалярным произведением в пространстве \mathbb{C}^n .

Упражнение 2.6. Покажите, что скалярное произведение (\cdot, \cdot) всегда антилинейно по первому аргументу:

$$\left(\sum_i \lambda_i |w_i\rangle, |v\rangle \right) = \sum_i \lambda_i^* (\langle w_i|, \langle v|). \quad (2.15)$$

В работах по квантовой механике постоянно встречается понятие *гильбертова пространства*. В конечномерных комплексных векторных пространствах (с которыми мы только и будем иметь дело) гильбертово пространство — то же самое, что и пространство со скалярным произведением. Далее мы будем считать эти термины равнозначными, отдавая предпочтения термину «гильбертово пространство». В случае бесконечной размерности гильбертovы пространства удовлетворяют дополнительным условиям, кроме тех, которым удовлетворяют пространства со скалярным произведением, но эти подробности нам не нужны.

Векторы $|w\rangle$ и $|v\rangle$ называют *ортогональными*, если их скалярное произведение равно нулю. Например, векторы $|w\rangle \equiv (1, 0)$ и $|v\rangle \equiv (0, 1)$ ортогональны в смысле скалярного произведения, определенного соотношением (2.14). Определим норму вектора $|v\rangle$ следующим образом:

$$\| |v\rangle \| \equiv \sqrt{\langle v|v \rangle}. \quad (2.16)$$

Вектор $|v\rangle$ называют *единичным вектором*, если $\| |v\rangle \| = 1$. В этом случае мы также будем говорить о векторе $|v\rangle$ как о *нормированном*. Под *нормированием* вектора, имеются в виду деление вектора на его норму, т. е. $|v\rangle / \| |v\rangle \|$ — *нормированный вид* вектора $|v\rangle$ для любого ненулевого вектора $|v\rangle$. Набор векторов $|i\rangle$ называется *ортонормированным*, если все векторы в нем единичные и

любые два различных вектора ортогональны, т. е. $\langle i|j \rangle = \delta_{ij}$ для всех индексов i и j , $i \neq j$.

Упражнение 2.7. Проверьте, что векторы $|w\rangle \equiv (1, 1)$ и $|v\rangle \equiv (1, -1)$ ортогональны. Как выглядят эти векторы в нормированном виде?

Пусть $|w_1\rangle, \dots, |w_d\rangle$ — базис некоторого векторного пространства V со скалярным произведением. Для получения ортонормированного базисного набора векторов $|v_1\rangle, \dots, |v_d\rangle$ часто используют метод, известный под названием *ортогонализации Грама–Шмидта*. Введем определение $|v_1\rangle \equiv |w_1\rangle / \| |w_1\rangle \|$, и для $1 \leq k \leq d - 1$ определим $|v_{k+1}\rangle$ по индукции:

$$|v_{k+1}\rangle \equiv \frac{|w_{k+1}\rangle - \sum_{i=1}^k \langle v_i | w_{k+1} \rangle |v_i\rangle}{\| |w_{k+1}\rangle - \sum_{i=1}^k \langle v_i | w_{k+1} \rangle |v_i\rangle \|}. \quad (2.17)$$

Нетрудно проверить, что векторы $|v_1\rangle, \dots, |v_d\rangle$ образуют ортонормированный набор, который также является базисом для пространства V . Таким образом, в любом векторном пространстве конечной размерности d со скалярным произведением существует ортонормированный базис $|v_1\rangle, \dots, |v_d\rangle$.

Упражнение 2.8. Докажите, что при ортогонализации Грама–Шмидта действительно получается ортонормированный базис в пространстве V .

В дальнейшем, говоря о матричном представлении линейного оператора, мы всегда будем иметь в виду матричное представление для ортонормированных базисов в пространствах аргументов и значений оператора. Будем также считать (если не оговорено обратное), что, когда пространство аргументов совпадает с пространством значений оператора, в них используется один и тот же базис.

С учетом этих соглашений скалярное произведение удобно записать в матричном представлении. Пусть $|w\rangle = \sum_i w_i |i\rangle$ и $|v\rangle = \sum_j v_j |j\rangle$ — представления векторов $|w\rangle$ и $|v\rangle$ в ортонормированном базисе $|i\rangle$. Тогда, поскольку $\langle i|j \rangle = \delta_{ij}$, имеем

$$\langle v|w \rangle = \left(\sum_i v_i |i\rangle, \sum_j w_j |j\rangle \right) = \sum_{i,j} v_i^* w_j \delta_{ij} = \sum_i v_i^* w_i \quad (2.18)$$

$$= [v_1^* \dots v_n^*] \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix}. \quad (2.19)$$

Таким образом, скалярное произведение двух векторов равно скалярному произведению матричных представлений этих векторов, если представления записаны в одном и том же ортонормированном базисе. Кроме того, можно видеть, что двойственный вектор $\langle v|$ можно интерпретировать как вектор-строку с компонентами, являющимися комплексно-сопряженными с соответствующими компонентами представления $|v\rangle$ в виде вектора-столбца.

Для представления линейных операторов существует полезный способ, использующий скалярное произведение — он называется *представлением с по-*

мощью тензорного произведения. Пусть $|v\rangle$ — вектор в пространстве V со скалярным произведением, а $|w\rangle$ — вектор в пространстве W со скалярным произведением. Определим $|w\rangle\langle v|$ как линейный оператор, отображающий V в W по следующему правилу:

$$(|w\rangle\langle v_i|)(|v'\rangle) \equiv |w\rangle\langle v|v'\rangle = \langle v|v'\rangle|w\rangle. \quad (2.20)$$

Это уравнение наилучшим образом подходит к нашей системе обозначений, согласно которой выражение $|w\rangle\langle v|v'\rangle$ может в принципе иметь одно из двух значений: мы будем использовать его для указания результата действия *оператора* $|w\rangle\langle v|$ на вектор $|v'\rangle$; также можно считать это результатом умножения вектора $|w\rangle$ на комплексное число $\langle v|v'\rangle$. Наши определения подобраны таким образом, что эти два возможных значения всегда совпадают. Действительно, мы определяем первое значение в терминах второго.

Можно взять линейную комбинацию тензорных произведений $|w_i\rangle\langle v_i|$ очевидным образом. По определению, $\sum_i a_i|w_i\rangle\langle v_i|$ — линейный оператор, который, действуя на вектор $|v'\rangle$, дает результат $\sum_i a_i|w_i\rangle\langle v_i|v'\rangle$.

Продемонстрируем удобство такого представления. Пусть $|i\rangle$ — ортонормированный базис в векторном пространстве V , тогда произвольный вектор $|v\rangle$ может быть записан в виде $|v\rangle = \sum_i v_i|i\rangle$, где v_i — комплексные числа. Заметим, что $\langle i|v\rangle = v_i$, поэтому имеет место соотношение

$$\left(\sum_i |i\rangle\langle i| \right) |v\rangle = \sum_i v_i|i\rangle = |v\rangle \quad (2.21)$$

Поскольку последнее равенство выполняется для всех векторов $|v\rangle$, получим

$$\sum_i |i\rangle\langle i| = I. \quad (2.22)$$

Это уравнение известно как *условие полноты*. Одно из применений такого условия — дать возможность представить любой оператор в терминах тензорного произведения. Пусть $A: V \rightarrow W$ — линейный оператор, $|v_i\rangle$ — ортонормированный базис в пространстве V , $|w_j\rangle$ — ортонормированный базис в пространстве W . Используя условие полноты дважды, мы получим соотношение

$$A = I_W A I_V \quad (2.23)$$

$$= \sum_{i,j} |w_j\rangle\langle w_j| A |v_i\rangle\langle v_i| \quad (2.24)$$

$$= \sum_{i,j} \langle w_j| A |v_i\rangle |w_j\rangle\langle v_i|, \quad (2.25)$$

т. е. тензорное представление для оператора A . Из этого уравнения также следует, что оператор A содержит матричный элемент $\langle w_j| A |v_i\rangle$ в i -й колонке и j -й строке (при базисах $|v_i\rangle$ в пространстве аргументов и $|w_j\rangle$ в пространстве результатов).

Вторым применением, иллюстрирующим ценность условия полноты, является *неравенство Коши–Шварца*. Этот важный результат обсуждается во вставке 2.1.

Вставка 2.1. Неравенство Коши–Шварца

Неравенство Коши–Шварца — важное геометрическое утверждение о гильбертовых пространствах. Оно заключается в следующем: для любых двух векторов $|v\rangle$ и $|w\rangle$ выполняется неравенство $|\langle v|w\rangle|^2 \leq \langle v|v\rangle\langle w|w\rangle$. Чтобы проверить это, проведем ортогонализацию Грама–Шмидта и построим такой ортонормированный базис $|i\rangle$ в векторном пространстве, что первый вектор этого базиса будет равен $|w\rangle/\sqrt{\langle w|w\rangle}$. Используя условие полноты ($\sum_i |i\rangle\langle i| = I$) и опуская некоторые неотрицательные слагаемые, получим

$$\langle v|v\rangle\langle w|w\rangle = \sum_i \langle v|i\rangle\langle i|v\rangle\langle w|w\rangle \quad (2.26)$$

$$\geq \frac{\langle v|w\rangle\langle w|v\rangle}{\langle w|w\rangle} \langle w|w\rangle \quad (2.27)$$

$$= \langle v|w\rangle\langle w|v\rangle = |\langle v|w\rangle|^2, \quad (2.28)$$

что и требовалось доказать. Нетрудно заметить, что неравенство превращается в равенство тогда и только тогда, когда векторы $|v\rangle$ и $|w\rangle$ линейно зависимы, т. е. $|v\rangle = z|w\rangle$ или $|w\rangle = z|v\rangle$, где z — некоторая скалярная величина.

Упражнение 2.9 (операторы Паули и тензорное произведение). Матрицы Паули (см. рис. 2.2) можно рассматривать как операторы в ортонормированном базисе $|0\rangle$, $|1\rangle$ в двумерном гильбертовом пространстве. Запишите каждый из операторов Паули в терминах тензорного произведения.

Упражнение 2.10. Пусть $|v_i\rangle$ — ортонормированный базис в пространстве V со скалярным произведением. Как выглядит матричное представление для оператора $|v_j\rangle\langle v_k|$ в базисе $|v_i\rangle$?

2.1.5 Собственные векторы и собственные значения

Собственный вектор линейного оператора A , действующего в векторном пространстве, — такой ненулевой вектор $|v\rangle$, что $A|v\rangle = v|v\rangle$, где v — комплексное число, называемое *собственным числом* оператора A , соответствующим собственному вектору $|v\rangle$. Часто удобно использовать v одновременно и для метки собственного вектора в обозначениях Дирака, и для соответствующего этому вектору собственного числа. Мы предполагаем, что читатель знаком с элементарными свойствами собственных чисел и собственных векторов, в частности умеет находить их с использованием характеристического уравнения. *Характеристическим многочленом* называют функцию $c(\lambda) \equiv \det |A - \lambda I|$, где $\det |Z|$ — определитель матрицы Z ; можно показать, что характеристический многочлен

зависит только от оператора A , но не от конкретного матричного представления для A . Решения *характеристического уравнения* $c(\lambda) = 0$ — собственные числа оператора A . Согласно основной теореме алгебры, у каждого многочлена с комплексными коэффициентами имеется хотя бы один комплексный корень, поэтому у любого оператора A есть хотя бы одно собственное число и соответствующий ему собственный вектор. *Собственным пространством*, соответствующим собственному числу v , называют дополненное нулевым вектором множество всех собственных векторов, которые имеют собственное значение v . Это множество является векторным подпространством в векторном пространстве, где действует оператор A .

Оператор A имеет *диагональный вид*, если он записан как $A = \sum_i \lambda_i |i\rangle\langle i|$, где векторы $|i\rangle$ образуют ортонормированный набор собственных векторов оператора A , а λ_i — соответствующие им собственные числа. Оператор называют *диагонализируемым*, если его можно записать в диагональном виде. В следующем разделе мы найдем простой набор необходимых и достаточных условий приведения оператора в гильбертовом пространстве к диагональному виду. В качестве примера может служить матрица Паули Z , которая имеет *диагональный вид*:

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1| \quad (2.29)$$

(матричное представление записывается для ортонормированных векторов $|0\rangle$ и $|1\rangle$). Представление в *диагональном виде* называют также *спектральным разложением*.

Если собственное пространство имеет размерность больше единицы, то можно сказать, что оно *вырождено*. Например, у матрицы

$$A \equiv \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad (2.30)$$

существует двумерное собственное пространство, соответствующее собственному значению 2. Собственные векторы $(1, 0, 0)$ и $(0, 1, 0)$ называются *вырожденными*, поскольку это линейно-независимые собственные векторы оператора A , отвечающие одному и тому же собственному значению.

Упражнение 2.11 (спектральное разложение матриц Паули). Найдите собственные векторы, собственные числа и приведите к диагональному виду матрицы Паули X , Y и Z .

Упражнение 2.12. Докажите, что матрицу

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \quad (2.31)$$

нельзя преобразовать в диагональную форму.

2.1.6 Сопряженные и эрмитовы операторы

Пусть A — линейный оператор, действующий в гильбертовом пространстве V . Оказывается, существует единственный оператор A^\dagger , действующий также в пространстве V , такой, что для любых векторов $|v\rangle, |w\rangle \in V$ справедливо соотношение

$$(\langle v|, A|w\rangle) = (A^\dagger|v\rangle, |w\rangle). \quad (2.32)$$

Оператор A^\dagger называется *эрмитово-сопряженным* (или просто *сопряженным*) к оператору A . Из этого определения следует, что $(AB)^\dagger = B^\dagger A^\dagger$. По определению, сопряженным к вектору $|v\rangle$ является вектор $\langle v|$, т. е. $\langle v|^\dagger \equiv \langle v|$. Из этого определения вытекает, что $(A|v\rangle)^\dagger = \langle v|A^\dagger$.

Упражнение 2.13. Покажите для двух произвольных векторов $|w\rangle$ и $|v\rangle$, что $(\langle w|v\rangle)^\dagger = \langle v|w\rangle$.

Упражнение 2.14 (антилинейность сопряженного оператора). Покажите, что операция сопряжения антилинейна, т. е.

$$\left(\sum_i a_i A_i \right)^\dagger = \sum_i a_i^* A_i^\dagger. \quad (2.33)$$

Упражнение 2.15. Покажите, что $(A^\dagger)^\dagger = A$.

В матричном представлении эрмитово сопряжение означает транспонирование и комплексное сопряжение матрицы: $A^\dagger \equiv (A^*)^T$ (здесь символ * означает комплексное сопряжение, T — операцию транспонирования). Например,

$$\begin{bmatrix} 1+3i & 2i \\ 1+i & 1-4i \end{bmatrix}^\dagger = \begin{bmatrix} 1-3i & 1-i \\ -2i & 1+4i \end{bmatrix}. \quad (2.34)$$

Оператор A , совпадающий со своим эрмитово-сопряженным оператором, называется *эрмитовым* или *самосопряженным*. Важным классом эрмитовых операторов являются *проекторы*. Пусть W — k -мерное векторное подпространство векторного пространства V . Проведя ортогонализацию Грамма–Шмидта, можно построить такой ортонормированный базис $|1\rangle, \dots, |k\rangle$ пространства V , что $|1\rangle, \dots, |k\rangle$ — ортонормированный базис пространства W . По определению, оператор

$$P \equiv \sum_{i=1}^k |i\rangle\langle i| \quad (2.35)$$

есть *проекtor* на подпространство W . Легко проверить, что это определение не зависит от выбора ортонормированного базиса $|1\rangle, \dots, |k\rangle$ в пространстве W . Из (2.20) следует, что для любого вектора v оператор $|v\rangle\langle v|$ эрмитов, поэтому оператор P также эрмитов ($P^\dagger = P$). Мы будем часто для краткости говорить о «векторном пространстве» P , имея в виду пространство, на которое оператор P проектирует исходное пространство V . *Ортогональным дополнением* оператора P будем называть оператор $Q \equiv I - P$. Легко видеть, что Q —

проектор на векторное пространство, натянутое на векторы $|k+1\rangle, \dots, |d\rangle$, и его мы также будем называть *ортогональным дополнением* пространства P (и соответственно обозначать через Q).

Упражнение 2.16. Покажите, что для любого проектора P выполняется равенство $P^2 = P$.

Оператор A называется *нормальным*, если $AA^\dagger = A^\dagger A$. Очевидно, что любой эрмитов оператор является нормальным. Есть замечательная теорема, характеризующая нормальные операторы, согласно которой оператор является нормальным тогда и только тогда, когда он приводится к диагональному виду. Это — *теорема о спектральном разложении*, ее доказательство приведено во вставке 2.2.

Упражнение 2.17. Покажите, что нормальная матрица является эрмитовой тогда и только тогда, когда все ее собственные значения действительны.

Матрица U называется *унитарной*, если $U^\dagger U = I$. Аналогично оператор U унитарный, если $U^\dagger U = I$. Легко проверить, что оператор является унитарным тогда и только тогда, когда любое его матричное представление унитарно. Унитарный оператор также удовлетворяет условию $UU^\dagger = I$, следовательно U — нормальный оператор и для него существует спектральное разложение. С геометрической точки зрения унитарные операторы важны, поскольку они сохраняют скалярное произведение векторов. Действительно, пусть $|v\rangle$ и $|w\rangle$ — векторы. Тогда скалярное произведение векторов $U|v\rangle$ и $U|w\rangle$ равно скалярному произведению $|v\rangle$ и $|w\rangle$:

$$(U|v\rangle, U|w\rangle) = \langle v|U^\dagger U|w\rangle = \langle v|I|w\rangle = \langle v|w\rangle. \quad (2.36)$$

Из этого факта вытекает следующее красивое представление в виде тензорного произведения для произвольного унитарного оператора U . Пусть $|v_i\rangle$ — ортонормированный базис, а $|w_i\rangle \equiv U|v_i\rangle$. Тогда набор $|w_i\rangle$ также является ортонормированным базисом, поскольку унитарные операторы сохраняют скалярное произведение. Заметим, что $U = \sum_i |w_i\rangle\langle v_i|$. Наоборот: если $|v_i\rangle$ и $|w_i\rangle$ — два ортонормированных базиса, то легко проверить, что оператор $U \equiv \sum_i |w_i\rangle\langle v_i|$ — унитарный.

Упражнение 2.18. Покажите, что любое собственное число унитарной матрицы по модулю равно единице, т. е. может быть записано в виде $e^{i\theta}$, где θ — некоторое действительное число.

Упражнение 2.19 (свойства матриц Паули). Покажите, что матрицы Паули являются эрмитовыми и унитарными.

Упражнение 2.20 (замена базиса). Пусть A' и A'' — матричные представления оператора A , действующего в векторном пространстве V в двух разных ортонормированных базисах ($|v_i\rangle$ и $|w_i\rangle$). Элементы матриц A' и A'' равны $A'_{ij} = \langle v_i|A|v_j\rangle$, $A''_{ij} = \langle w_i|A|w_j\rangle$. Как связаны между собой матрицы A' и A'' ?

Особенно важный частный случай эрмитовых операторов — *неотрицательно определенные операторы*. Оператор A называют неотрицательно определенным, если для любого вектора $|v\rangle$ число $(|v\rangle, A|v\rangle)$ является действительным и неотрицательным. Если $(|v\rangle, A|v\rangle) > 0$ для любого вектора $|v\rangle \neq 0$, будем

называть оператор A *положительно определенным*. В упр. 2.24 предлагается доказать, что любой неотрицательно определенный оператор является эрмитовым, поэтому в спектральном разложении такого оператора $\sum_i \lambda_i |i\rangle\langle i|$ все собственные числа λ_i неотрицательны.

Упражнение 2.21. Повторите доказательство теоремы о спектральном разложении, приведенное во вставке 2.2, для случая эрмитова оператора M , упрощая доказательство в тех местах, где это возможно.

Упражнение 2.22. Докажите, что два собственных вектора эрмитова оператора, соответствующие разным собственным значениям, ортогональны.

Упражнение 2.23. Покажите, что все собственные числа проектора P равны 0 или 1.

Упражнение 2.24. Докажите, что неотрицательно определенный оператор является эрмитовым. (Указание: покажите, что произвольный оператор A может быть записан в форме $A = B + iC$, где B и C — эрмитовы операторы.)

Упражнение 2.25. Покажите, что для любого оператора A оператор $A^\dagger A$ является неотрицательно определенным.

2.1.7 Тензорное произведение

Тензорное произведение — особый способ получения из векторных пространств «большего» векторного пространства. Эта конструкция является очень важной для понимания квантовой механики систем, состоящих из нескольких частиц. Приводимое ниже описание несколько абстрактно и, возможно, не знакомому с понятием тензорного произведения читателю будет не так просто во все вникнуть. В этом случае можно пропустить данный подраздел при первом чтении и вернуться к нему в дальнейшем, когда в квантовомеханических задачах будет использоваться понятие тензорного произведения.

Пусть V и W — векторные пространства размерности m и n соответственно. Для удобства предположим, что пространства V и W являются гильбертовыми. Тогда $V \otimes W$ (читается «тензорное произведение V и W ») — пространство размерности mn . Элементы пространства $V \otimes W$ представляют собой линейные комбинации «тензорных произведений» $|v\rangle \otimes |w\rangle$ векторов $v \in V$ и $w \in W$. Если $|i\rangle$ и $|j\rangle$ — ортонормированные базисы в пространствах V и W , то $|i\rangle \otimes |j\rangle$ — базис в пространстве $V \otimes W$. Мы часто будем использовать обозначения $|v\rangle|w\rangle$, $|v, w\rangle$ и даже $|vw\rangle$ вместо $|v\rangle \otimes |w\rangle$. Например, если V — двумерное векторное пространство с базисными векторами $|0\rangle$ и $|1\rangle$, то $|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle$ — элемент пространства $V \otimes V$.

Вставка 2.2. Спектральное разложение

Теорема 2.1 (о спектральном разложении). Любой нормальный оператор M , действующий в векторном пространстве V , является диагональным в некотором ортонормированном базисе пространства V . Обратно: любой приводимый к диагональному виду оператор является нормальным.

Доказательство. Второе утверждение — по существу простое упражнение, поэтому докажем только первое утверждение. Применим индукцию по размерности d пространства V . В случае $d = 1$ все очевидно. Пусть λ — собственное число оператора M , P — проектор на собственное пространство, соответствующее собственному числу λ , Q — проектор на ортогональное дополнение к нему. Тогда $M = (P + Q)M(P + Q) = PMP + QMP + PMQ + QMQ$. Очевидно, что $PMP = \lambda P$. Далее, $QMP = 0$, поскольку оператор M переводит подпространство P в себя. Кроме того, $PMQ = 0$. Чтобы доказать этот факт, возьмем вектор $|v\rangle$ из подпространства P . Тогда $MM^\dagger|v\rangle = M^\dagger M|v\rangle = \lambda M^\dagger|v\rangle$. Поэтому вектор $M^\dagger|v\rangle$ — собственный с собственным числом λ и, следовательно, лежит в подпространстве P . Из этого заключаем, что $QM^\dagger P = 0$. Если применить к этому равенству операцию сопряжения, получим $PMQ = 0$. Поэтому $M = PMP + QMQ$. Теперь докажем, что оператор QMQ является нормальным. Действительно, $QM = QM(P + Q) = QMQ$, следовательно $QM^\dagger = QM^\dagger(P + Q) = QM^\dagger Q$. Тогда (учитывая, что оператор M — нормальный, а $Q^2 = Q$), имеем

$$QMQQM^\dagger Q = QMQM^\dagger Q \quad (2.37)$$

$$= QMM^\dagger Q \quad (2.38)$$

$$= QM^\dagger MQ \quad (2.39)$$

$$= QM^\dagger QMQ \quad (2.40)$$

$$= QM^\dagger QQMQ, \quad (2.41)$$

так что оператор QMQ является нормальным. По индукции заключаем, что QMQ — диагональный оператор в некотором ортонормированном базисе пространства Q , а относительно оператора PMP уже было доказано, что он диагональный в некотором базисе пространства P . Отсюда следует, что $M = PMP + QMQ$ — диагональный оператор в некотором базисе пространства V . ■

Для представления в виде тензорного произведения это означает, что оператор M может быть записан в виде $M = \sum_i \lambda_i |i\rangle\langle i|$, где λ_i — собственные числа оператора M , $|i\rangle$ — ортонормированный базис в V , а любой вектор из набора $|i\rangle$ является собственным вектором оператора M , соответствующим собственному числу λ_i . В терминах проекторов это можно представить как $M = \sum_i \lambda_i P_i$, где λ_i — собственные числа оператора M , P_i — проектор на собственное пространство оператора M , соответствующее собственному числу λ_i . Эти проекторы удовлетворяют условию полноты $\sum_i P_i = I$ и образуют ортонормальный набор: $P_i P_j = \delta_{ij} P_i$.

По определению тензорное произведение обладает следующими основными свойствами:

1. для любого скаляра z и векторов $v \in V, w \in W$ имеет место равенство

$$z(|v\rangle \otimes |w\rangle) = (z|v\rangle) \otimes |w\rangle = |v\rangle \otimes (z|w\rangle); \quad (2.42)$$

2. для любых векторов $|v_1\rangle, |v_2\rangle \in V, w \in W$ справедливо соотношение

$$(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle; \quad (2.43)$$

3. для любых векторов $|v\rangle \in V, |w_1\rangle, |w_2\rangle \in W$ выполняется равенство

$$|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle. \quad (2.44)$$

Как описать линейные операторы, действующие в пространстве $V \otimes W$? Пусть $|v\rangle$ и $|w\rangle$ — векторы в пространствах V и W , A и B — линейные операторы соответственно в пространствах V и W . Тогда можно определить линейный оператор $A \otimes B$, действующий в пространстве $V \otimes W$, следующим образом:

$$(A \otimes B)(|v\rangle \otimes |w\rangle) \equiv A|v\rangle \otimes B|w\rangle. \quad (2.45)$$

Результат действия оператора $A \otimes B$ на остальных векторах пространства $V \otimes W$ определяется естественным образом с учетом линейности, т. е.

$$A \otimes B \left(\sum_i a_i (|v_i\rangle \otimes |w_i\rangle) \right) \equiv \sum_i a_i (A|v_i\rangle \otimes B|w_i\rangle). \quad (2.46)$$

Можно показать, что такое определение корректно задает оператор $A \otimes B$, действующий на пространстве $V \otimes W$. Понятие тензорного произведения двух операторов обобщается естественным образом на случай операторов $A: V \rightarrow V'$, $B: W \rightarrow W'$, когда пространство аргументов не совпадает с пространством значений. Действительно, произвольный линейный оператор C , отображающий $V \otimes W$ в $V' \otimes W'$, может быть представлен в виде линейной комбинации тензорных произведений операторов, отображающих V в V' и W в W' :

$$C = \sum_i c_i A_i \otimes B_i, \quad (2.47)$$

где по определению

$$\left(\sum_i c_i A_i \otimes B_i \right) |v\rangle \otimes |w\rangle \equiv \sum_i c_i A_i |v\rangle \otimes B_i |w\rangle. \quad (2.48)$$

Скалярные произведения в пространствах V и W можно использовать для определения скалярного произведения в пространстве $V \otimes W$ по следующей формуле:

$$\left(\sum_i a_i |v_i\rangle \otimes |w_i\rangle, \sum_j b_j |v'_j\rangle \otimes |w'_j\rangle \right) = \sum_{i,j} a_i^* b_j \langle v_i | v'_j \rangle \langle w_i | w'_j \rangle. \quad (2.49)$$

Можно показать, что задаваемая этой формулой функция действительно обладает всеми свойствами скалярного произведения. Получившееся пространство $V \otimes W$ со скалярным произведением наследует всю остальную знакомую нам структуру: сопряжение операторов, унитарные, нормальные и эрмитовы операторы.

Все приведенные выше рассуждения были довольно абстрактными. Их можно сделать более конкретными, если перейти к удобному матричному представлению, известному как *кронекерово произведение матриц*. Пусть A — матрица размера $m \times n$, B — матрица $p \times q$. Тогда имеется следующее матричное представление:

$$A \otimes B \equiv \underbrace{\begin{bmatrix} A_{11}B & A_{12}B & \dots & A_{1n}B \\ A_{21}B & A_{22}B & \dots & A_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ A_{m1}B & A_{m2}B & \dots & A_{mn}B \end{bmatrix}}_{nq} \}_{mp}. \quad (2.50)$$

В этом представлении через $A_{ij}B$ и т. п. обозначены подматрицы $p \times q$, пропорциональные матрице B (с коэффициентами пропорциональности A_{ij} и т. п.). Например, тензорное произведение векторов $(1, 2)$ и $(2, 3)$ есть вектор

$$\begin{bmatrix} 1 \\ 2 \end{bmatrix} \otimes \begin{bmatrix} 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 1 \times 2 \\ 1 \times 3 \\ 2 \times 2 \\ 2 \times 3 \end{bmatrix} = \begin{bmatrix} 2 \\ 3 \\ 4 \\ 6 \end{bmatrix}. \quad (2.51)$$

Тензорное произведение матриц Паули X и Y равно

$$X \otimes Y = \begin{bmatrix} 0 \cdot Y & 1 \cdot Y \\ 1 \cdot Y & 0 \cdot Y \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \\ 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \end{bmatrix}. \quad (2.52)$$

Наконец, введем полезное обозначение $|\psi\rangle^{\otimes k}$, соответствующее k раз тензорно перемноженному с самим собой вектору $|\psi\rangle$. Например, $|\psi\rangle^{\otimes 2} = |\psi\rangle \otimes |\psi\rangle$. Аналогичное обозначение используется для операторов, действующих на пространствах тензорных произведений.

Упражнение 2.26. Пусть $|\psi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. Запишите в явном виде векторы $|\psi\rangle^{\otimes 2}$ и $|\psi\rangle^{\otimes 3}$, используя обозначения вида $|0\rangle|1\rangle$ и кронекерово произведение.

Упражнение 2.27. Вычислите матричное представление тензорных произведений следующих операторов Паули: а) X и Z ; б) I и X ; в) X и I . Обладает ли тензорное произведение свойством коммутативности?

Упражнение 2.28. Покажите, что операции транспонирования, комплексного сопряжения и эрмитова сопряжения дистрибутивны относительно тензорного произведения:

$$(A \otimes B)^* = A^* \otimes B^*; \quad (A \otimes B)^T = A^T \otimes B^T; \quad (A \otimes B)^\dagger = A^\dagger \otimes B^\dagger. \quad (2.53)$$

Упражнение 2.29. Покажите, что тензорное произведение двух унитарных операторов есть унитарный оператор.

Упражнение 2.30. Покажите, что тензорное произведение двух эрмитовых операторов — эрмитов оператор.

Упражнение 2.31. Покажите, что тензорное произведение двух неотрицательно определенных операторов — неотрицательно определенный оператор.

Упражнение 2.32. Покажите, что тензорное произведение двух проекторов — проектор.

Упражнение 2.33. Оператор Адамара на одном кубите может быть записан следующим образом:

$$H = \frac{1}{\sqrt{2}} [(|0\rangle + |1\rangle)\langle 0| + (|0\rangle - |1\rangle)\langle 1|]. \quad (2.54)$$

Прямыми вычислением проверьте, что преобразование Адамара на n кубитах ($H^{\otimes n}$) может быть записано в виде

$$H^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x,y} (-1)^{x \cdot y} |x\rangle\langle y|. \quad (2.55)$$

Выпишите в явном виде матричное представление для $H^{\otimes 2}$.

2.1.8 Операторные функции

Можно ввести много важных функций от операторов и матриц. Вообще говоря, если задана функция f , отображающая множество комплексных чисел в себя, то можно определить соответствующую матричную функцию на нормальных матрицах (или некотором подклассе, например на эрмитовых матрицах) следующим образом. Пусть $A = \sum_a a|a\rangle\langle a|$ — спектральное разложение для оператора A . Обозначим $f(A) \equiv \sum_a f(a)|a\rangle\langle a|$. Легко видеть, что функция $f(A)$ определена однозначно. Эту процедуру можно использовать, например, для нахождения квадратного корня из неотрицательно определенного оператора, логарифма положительно определенного оператора, экспоненты нормального оператора. Так,

$$\exp(\theta Z) = \begin{bmatrix} e^\theta & 0 \\ 0 & e^{-\theta} \end{bmatrix}, \quad (2.56)$$

поскольку собственные векторы Z равны $|0\rangle$ и $|1\rangle$.

Упражнение 2.34. Найдите квадратный корень и логарифм матрицы

$$\begin{bmatrix} 4 & 3 \\ 3 & 4 \end{bmatrix}. \quad (2.57)$$

Упражнение 2.35 (экспонента от матриц Паули). Пусть \vec{v} — произвольный действительный трехмерный вектор единичной длины, θ — действительное число. Докажите, что

$$\exp(i\theta\vec{v} \cdot \vec{\sigma}) = \cos(\theta)I + i\sin(\theta)\vec{v} \cdot \vec{\sigma}, \quad (2.58)$$

где $\vec{v} \cdot \vec{\sigma} = \sum_{i=1}^3 v_i \sigma_i$. Это упражнение обобщается в задаче 2.1.

Другой важной функцией, действующей на матрицах, является *след* матрицы. Следом квадратной матрицы A называется сумма ее диагональных элементов:

$$\text{tr}(A) \equiv \sum_i A_{ii}. \quad (2.59)$$

Нетрудно заметить, что след *цикличен* ($\text{tr}(AB) = \text{tr}(BA)$) и *линеен* ($\text{tr}(A+B) = \text{tr}(A) + \text{tr}(B)$, $\text{tr}(zA) = z \text{tr}(A)$), где A и B — произвольные матрицы, z — комплексное число. Из свойства цикличности следует, что след матрицы инвариантен относительно унитарного преобразования сопряжения $A \rightarrow UAU^\dagger$, поскольку $\text{tr}(UAU^\dagger) = \text{tr}(U^\dagger UA) = \text{tr}(A)$. Поэтому можно определить след *оператора* A как след какого-нибудь матричного представления A . Инвариантность следа относительно преобразования сопряжения гарантирует, что след оператора определен корректно.

Рассмотрим пример, в котором используется понятие следа. Пусть $|\psi\rangle$ — единичный вектор, A — произвольный оператор. Для вычисления $\text{tr}(A|\psi\rangle\langle\psi|)$ используем ортогонализацию Грама–Шмидта, чтобы дополнить вектор $|\psi\rangle$ до ортонормированного базиса $|i\rangle$, в котором $|\psi\rangle$ является первым элементом. Тогда получим

$$\text{tr}(A|\psi\rangle\langle\psi|) = \sum_i \langle i | A | \psi \rangle \langle \psi | i \rangle \quad (2.60)$$

$$= \langle \psi | A | \psi \rangle. \quad (2.61)$$

Тот факт, что $\text{tr}(A|\psi\rangle\langle\psi|) = \langle \psi | A | \psi \rangle$, очень полезен при вычислении следа оператора.

Упражнение 2.36. Покажите, что у всех матриц Паули, кроме I , след равен нулю.

Упражнение 2.37 (неизменность следа при циклических перестановках сомножителей). Покажите, что для любых двух линейных операторов A и B

$$\text{tr}(AB) = \text{tr}(BA). \quad (2.62)$$

Упражнение 2.38 (линейность следа). Покажите, что для любых двух линейных операторов A и B справедливо равенство

$$\text{tr}(A+B) = \text{tr}(A) + \text{tr}(B), \quad (2.63)$$

а для произвольного комплексного числа z

$$\text{tr}(zA) = z \text{tr}(A). \quad (2.64)$$

Упражнение 2.39 (скалярное произведение Гильберта–Шмидта в пространстве операторов). Очевидно, что множество L_V линейных операторов, действующих в гильбертовом пространстве V , является векторным пространством, т. е. 1) сумма двух линейных операторов есть линейный оператор; 2) если A — линейный оператор, а z — комплексное число, то оператор zA также линейный; 3) существует нулевой оператор 0. В векторном пространстве L_V есть также естественное скалярное произведение, так что L_V можно считать гильбертовым.

1. Покажите, что функция (\cdot, \cdot) на пространстве $L_V \times L_V$, определенная соотношением

$$(A, B) \equiv \text{tr}(A^\dagger B), \quad (2.65)$$

задает скалярное произведение. Это скалярное произведение называют *скалярным произведением Гильберта–Шмидта* или *следовым скалярным произведением*.

2. Покажите, что если размерность пространства V равна d , то размерность пространства L_V равна d^2 .
3. Постройте ортонормированный базис в гильбертовом пространстве L_V , состоящий из эрмитовых операторов.

2.1.9 Коммутатор и антакоммутатор

Коммутатор операторов A и B определяется соотношением

$$[A, B] \equiv AB - BA. \quad (2.66)$$

Если $[A, B] = 0$, т. е. $AB = BA$, то операторы A и B называют *коммутирующими* друг с другом. Аналогично *антакоммутатор* операторов A и B определяется следующим образом:

$$\{A, B\} \equiv AB + BA; \quad (2.67)$$

оператор A *антакоммутирует* с B , если $\{A, B\} = 0$. Оказывается, что многие важные свойства пары операторов связаны со значениями их коммутатора и антакоммутатора. Возможно, наиболее полезное соотношение — это связь между коммутатором и возможностью *одновременного приведения к диагональному виду* эрмитовых операторов A и B , т. е. возможностью одновременного представления их в виде $A = \sum_i a_i |i\rangle\langle i|$, $B = \sum_i b_i |i\rangle\langle i|$, где $|i\rangle$ — некоторый общий набор ортонормированных собственных векторов для операторов A и B .

Теорема 2.2 (об одновременном приведении к диагональному виду). Пусть A и B — эрмитовы операторы. В этом случае $[A, B] = 0$ тогда и только тогда, когда существует такой ортонормированный базис, что оба оператора A и B являются диагональными в этом базисе. Следовательно, можно сказать, что A и B одновременно приводятся к *диагональному виду*.

Это утверждение связывает коммутатор двух операторов, который обычно легко вычислить, с возможностью одновременного приведения к диагональному виду — свойством, *a priori* довольно сложно поддающимся проверке. Например,

$$[X, Y] = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} - \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad (2.68)$$

$$= 2i \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \quad (2.69)$$

$$= 2iZ, \quad (2.70)$$

т. е. матрицы X и Y не коммутируют. Как можно было убедиться, выполнив упражнение 2.11, у матриц X и Y нет общих собственных векторов, что и следует из теоремы об одновременном приведении к диагональному виду.

Доказательство. Вы можете (и это, безусловно, следует сделать) легко проверить, что если A и B — диагональные матрицы в одном и том же ортонормированном базисе, то $[A, B] = 0$. Докажем обратное утверждение. Пусть $|a, j\rangle$ — ортонормированный базис для собственного пространства V_a оператора A , которое соответствует собственному числу a ; индекс « j » используется, чтобы обозначить возможное вырождение. Заметим, что

$$AB|a, j\rangle = BA|a, j\rangle = aB|a, j\rangle, \quad (2.71)$$

следовательно $B|a, j\rangle$ — элемент собственного пространства V_a . Пусть P_a — проекtor на пространство V_a , введем обозначение $B_a \equiv P_a B P_a$. Легко заметить, что ограничение оператора B_a на пространство V_a является эрмитовым оператором в V_a , и поэтому имеет спектральное разложение по ортонормированному набору собственных векторов, на которые натянуто пространство V_a . Обозначим эти векторы через $|a, b, k\rangle$, где a и b соответствуют собственным числам операторов A и B_a , а k — дополнительный индекс, позволяющий учесть возможное вырождение оператора B_a . Отметим, что $B|a, b, k\rangle$ лежит в пространстве V_a , так что $B|a, b, k\rangle = P_a B|a, b, k\rangle$. Более того, $P_a|a, b, k\rangle = |a, b, k\rangle$, следовательно

$$B|a, b, k\rangle = P_a B P_a|a, b, k\rangle = b|a, b, k\rangle. \quad (2.72)$$

Можно сделать вывод, что $|a, b, k\rangle$ — собственный вектор оператора B с собственным числом b , поэтому $|a, b, k\rangle$ — ортонормированный набор собственных векторов одновременно для операторов A и B , порождающий все пространство V , в котором действуют операторы A и B . Следовательно, операторы A и B могут быть одновременно приведены к диагональному виду. ■

Упражнение 2.40 (коммутационные соотношения для матриц Паули). Проверьте коммутационные соотношения

$$[X, Y] = 2iZ; \quad [Y, Z] = 2iX; \quad [Z, X] = 2iY. \quad (2.73)$$

То же самое можно записать элегантным способом, используя антисимметричный по трем индексам тензор ε_{jkl} ($\varepsilon_{jkl} = 0$, кроме $\varepsilon_{123} = \varepsilon_{231} = \varepsilon_{312} = 1$, $\varepsilon_{321} = \varepsilon_{213} = \varepsilon_{132} = -1$):

$$[\sigma_j, \sigma_k] = 2i \sum_{l=1}^3 \epsilon_{jkl} \sigma_l. \quad (2.74)$$

Упражнение 2.41 (антикоммутационные соотношения для матриц Паули). Проверьте антикоммутационные соотношения

$$\{\sigma_i, \sigma_j\} = 0, \quad (2.75)$$

где $i, j = 1, 2, 3$, $i \neq j$. Проверьте также, что

$$\sigma_i^2 = I \quad (2.76)$$

для $i = 0, 1, 2, 3$.

Упражнение 2.42. Проверьте, что

$$AB = \frac{[A, B] + \{A, B\}}{2}. \quad (2.77)$$

Упражнение 2.43. Покажите, что

$$\sigma_j \sigma_k = \delta_{jk} I + \sum_{l=1}^3 \epsilon_{jkl} \sigma_l. \quad (2.78)$$

Упражнение 2.44. Пусть $[A, B] = 0$, $\{A, B\} = 0$, A — обратимая матрица. Покажите, что $B = 0$.

Упражнение 2.45. Покажите, что $[A, B]^\dagger = [B^\dagger, A^\dagger]$.

Упражнение 2.46. Покажите, что $[A, B] = -[B, A]$.

Упражнение 2.47. Пусть A и B — эрмитовы операторы. Покажите, что оператор $i[A, B]$ также является эрмитовым.

2.1.10 Полярное разложение и разложение по сингулярным числам

Полярное разложение и разложение по сингулярным числам представляют собой полезные способы разложения линейных операторов на более простые части. Например, они позволяют представить линейные операторы общего вида как произведения унитарных операторов и неотрицательно определенных операторов. Пока мы еще не слишком хорошо освоились со структурой линейных операторов общего вида, нам лучше знакомо устройство унитарных и неотрицательно определенных операторов. Полярное разложение и разложение по сингулярным числам позволяют применять эти знания для лучшего понимания устройства линейных операторов общего вида.

Теорема 2.3 (о полярном разложении). Пусть A — линейный оператор, действующий в векторном пространстве V . Тогда существуют такие унитарный оператор U и неотрицательно определенные операторы J и K , что

$$A = UJ = KU, \quad (2.79)$$

причем операторы J и K определены единственным образом: $J \equiv \sqrt{A^\dagger A}$, $K \equiv \sqrt{AA^\dagger}$. Кроме того, если A — обратимый оператор, то оператор U также определен однозначно.

Назовем выражение $A = UJ$ *левым полярным разложением* оператора A , а выражение $A = KU$ — *правым полярным разложением*. Довольно часто мы будем опускать слова «левый» и «правый», говоря просто о «полярном разложении», поскольку из контекста обычно ясно, о каком именно разложении идет речь.

Доказательство. Оператор $J \equiv \sqrt{A^\dagger A}$ является неотрицательно определенным, поэтому для него существует спектральное разложение: $J = \sum_i \lambda_i |i\rangle\langle i|$ ($\lambda_i \geq 0$). Введем обозначение: $|\psi_i\rangle \equiv A|i\rangle$. Непосредственно проверяется, что $\langle\psi_i|\psi_i\rangle = \lambda_i^2$. Рассмотрим теперь только те i , для которых $\lambda_i \neq 0$. Для таких i рассмотрим векторы $|e_i\rangle \equiv |\psi_i\rangle/\lambda_i$, которые, как нетрудно видеть, являются единичными. Более того, они попарно ортогональны, поскольку если $i \neq j$, то $\langle e_i|e_j\rangle = \langle i|A^\dagger A|j\rangle/\lambda_i\lambda_j = \langle i|J^2|j\rangle/\lambda_i\lambda_j = 0$.

Мы рассмотрели такие i , для которых $\lambda_i \neq 0$. Теперь воспользуемся процедурой ортогонализации Грама–Шмидта, чтобы дополнить набор $|e_i\rangle$ до ортонормированного базиса, который мы также обозначим $|e_i\rangle$. Определим унитарный оператор $U \equiv \sum_i |e_i\rangle\langle i|$. При $\lambda_i \neq 0$ справедливо $UJ|i\rangle = \lambda_i|e_i\rangle = |\psi_i\rangle = A|i\rangle$. При $\lambda_i = 0$ получим $UJ|i\rangle = 0 = |\psi_i\rangle$. Таким образом, мы доказали, что операторы A и UJ дают одинаковые результаты при действии на векторы из базиса $|i\rangle$, следовательно, $A = UJ$.

Оператор J определен однозначно, поскольку при умножении равенства $A = UJ$ слева на $A^\dagger = JU^\dagger$ получим $J^2 = A^\dagger A$, откуда следует, что $J = \sqrt{A^\dagger A}$. Легко доказать, что если оператор A обратим, то J также обратим, поэтому оператор U однозначно определяется с помощью уравнения $U = AJ^{-1}$. Доказательство для правого полярного разложения проводится аналогично: $A = UJ = UJU^\dagger U = KU$, где $K \equiv UJU^\dagger$ — неотрицательно определенный оператор. Поскольку $AA^\dagger = KUU^\dagger K = K^2$, можно заключить, что $K = \sqrt{AA^\dagger}$, что и требовалось доказать. ■

При разложении по сингулярным числам используются одновременно полярное разложение и теорема о спектральном разложении.

Следствие 2.4 (разложение по сингулярным числам) Пусть A — квадратная матрица. Тогда существуют такие унитарные матрицы U и V и диагональная матрица D с неотрицательными числами на диагонали, что

$$A = UDV. \quad (2.80)$$

Диагональные элементы матрицы D называют *сингулярными числами* матрицы A .

Доказательство. Запишем полярное разложение для матрицы A : $A = SJ$, где S — унитарная, а J — неотрицательно определенная матрица. Согласно теореме о спектральном разложении, $J = TDT^\dagger$, причем T — унитарная матрица, D — диагональная с неотрицательными числами на диагонали. Для завершения доказательства следует ввести обозначения $U \equiv ST$, $V \equiv T^\dagger$. ■

Упражнение 2.48. Как выглядит полярное разложение для неотрицательно определенной матрицы P ? Для унитарной матрицы U ? Для эрмитовой матрицы H ?

Упражнение 2.49. Запишите полярное разложение для нормальной матрицы в представлении с помощью тензорного произведения.

Упражнение 2.50. Укажите левое и правое полярные разложения для матрицы

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}. \quad (2.81)$$

2.2 Постулаты квантовой механики

Понимание начинается с нашего неприятия мира таким, каким он кажется.

А. Кэй

Наиболее непостижимым свойством мира является его постижимость.

Альберт Эйнштейн

Квантовая механика — математическая конструкция для построения физических теорий. Сама по себе квантовая механика не сообщает, каким физическим законам подчинена та или иная физическая система, однако она дает математические конструкции и понятия для формулировки этих законов. В нескольких следующих разделах содержится полное описание основных постулатов квантовой механики, задающих связь между физическим миром и математическим формализмом этой дисциплины.

Постулаты квантовой механики были получены в результате долгого процесса проб и (по большей части) ошибок, который в значительной степени заключался в угадывании и нашупывании исходных положений теории. Не удивляйтесь, что мотивировки постулатов не всегда достаточно ясные; даже специалисты считают постулаты квантовой механики удивительными. Ознакомившись с несколькими следующими разделами, необходимо понять, как и когда следует применять эти постулаты.

2.2.1 Пространство состояний

Первый постулат квантовой механики устанавливает место действия квантовомеханических процессов. Это уже знакомое нам из линейной алгебры гильбертово пространство.

Постулат 1. С каждой изолированной физической системой связывается комплексное векторное пространство со скалярным произведением (т. е. гильбертово пространство), которое называется *пространством состояний* систе-

мы. Система полностью описывается *вектором состояния*, который представляет собой единичный вектор в пространстве состояний системы.

Квантовая механика не говорит нам ни о том, как именно устроено пространство состояний для заданной физической системы, ни о том, каков вектор состояния данной системы. Указание этого для *конкретной* системы — непростая задача, для решения которой физики разработали множество сложных и красивых правил. Так, существует замечательная теория, называемая квантовой электродинамикой (сокращенно КЭД), которая описывает взаимодействие атомов и света. Один из аспектов КЭД — показать, какие пространства состояний следует использовать, чтобы дать квантовое описание атомов и света. Мы не будем касаться таких сложных теорий, как КЭД (кроме тех случаев, когда они применяются к физическим реализациям, см. гл. 7), поскольку наша основная задача — разобраться с общей схемой, предлагаемой квантовой механикой. Для этого достаточно сделать несколько очень простых (и обоснованных) предположений относительно пространств состояний систем, которые мы будем изучать, и придерживаться их.

Простейшей квантовомеханической системой (и при этом системой, которая будет чаще всего использоваться) является *кубит*. Пространство состояний кубита двумерно. Обозначим базисные векторы в нем как $|0\rangle$ и $|1\rangle$. Тогда произвольный вектор состояния в этом пространстве может быть представлен в виде

$$|\psi\rangle = a|0\rangle + b|1\rangle, \quad (2.82)$$

где a и b — комплексные числа. Поэтому условие единичности вектора $|\psi\rangle$ ($\langle\psi|\psi\rangle = 1$) эквивалентно условию $|a|^2 + |b|^2 = 1$. Условие $\langle\psi|\psi\rangle = 1$ часто называют *условием нормировки* для векторов состояний.

Будем использовать кубит как основную квантовомеханическую систему. Далее (гл. 7) мы узнаем, что существуют реальные физические системы, которые могут быть описаны с использованием кубитов. Пока же нам достаточно рассматривать кубит как абстрактный объект, не указывая его конкретных реализаций. В наших обсуждениях всегда будет применяться ортонормированный базис из векторов $|0\rangle$ и $|1\rangle$, который следует считать зафиксированным заранее. Неформально говоря, состояния $|0\rangle$ и $|1\rangle$ аналогичны двум значениям 0 и 1, которые может принимать бит. При этом кубит отличается от бита тем, что первый может находиться в *суперпозиции* двух основных состояний (т. е. в состоянии вида $a|0\rangle + b|1\rangle$), и тогда невозможно утверждать с определенностью ни то, что кубит находится в состоянии $|0\rangle$, ни то, что он находится в состоянии $|1\rangle$.

Введем полезный термин, связанный с описанием квантовых состояний. Будем говорить, что линейная комбинация $\sum_i \alpha_i |\psi_i\rangle$ — суперпозиция состояний $|\psi_i\rangle$ с амплитудой α_i для состояния $|\psi_i\rangle$. Например, состояние

$$\frac{|0\rangle - |1\rangle}{\sqrt{2}} \quad (2.83)$$

есть суперпозиция состояний $|0\rangle$ и $|1\rangle$ с амплитудой $1/\sqrt{2}$ для состояния $|0\rangle$ и амплитудой $-1/\sqrt{2}$ для состояния $|1\rangle$.

2.2.2 Эволюция

Как будет меняться со временем состояние $|\psi\rangle$ квантовомеханической системы? Описание такого изменения задается следующим постулатом.

Постулат 2. Эволюция замкнутой квантовой системы описывается *унитарным преобразованием*. Другими словами, состояние $|\psi\rangle$ системы в момент времени t_1 связано с ее состоянием $|\psi'\rangle$ в момент t_2 посредством унитарного оператора U , зависящего только от моментов времени t_1 и t_2 :

$$|\psi'\rangle = U|\psi\rangle. \quad (2.84)$$

Квантовая механика не только не дает ответа на вопрос, о том, как устроено пространство состояний или квантовое состояние *конкретной* системы, но и не сообщает, какой оператор U описывает квантовомеханическую динамику реальной системы. Она просто «гарантирует» надежное средство описания замкнутой квантовомеханической системы. Возникает очевидный вопрос: какие унитарные операторы было бы естественно рассмотреть? В случае одиночного кубита оказывается, что *любой* унитарный оператор может быть реализован в некоторой реальной системе.

Рассмотрим несколько примеров унитарных операторов для одиночного кубита, которые играют важную роль в квантовых вычислениях и обработке квантовой информации. Выше было приведено несколько примеров таких операторов — матрицы Паули (подразд. 2.1.3), квантовые элементы (гл. 1). Как отмечалось в подразд. 1.3.1, матрицу X часто называют квантовым NOT по аналогии с классическим логическим элементом отрицания NOT. Матрицы Паули X и Y также называют матрицами *изменения бита* и *переворачивания фазы*: матрица X переводит $|0\rangle$ в $|1\rangle$ и $|1\rangle$ в $|0\rangle$, поэтому естественно говорить, что она изменяет бит; матрица Z оставляет вектор $|0\rangle$ неизменным, а $|1\rangle$ переводит в $-|1\rangle$, появляющийся дополнительный множитель -1 называют *фазовым множителем*, что оправдывает термин «переворачивание фазы». В подразд. 2.2.7 содержится дальнейшее обсуждение использования термина «фаза».

Другим интересным оператором является элемент Адамара, обозначаемый символом H . Он определяется следующим образом: $H|0\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}$, $H|1\rangle \equiv (|0\rangle - |1\rangle)/\sqrt{2}$; в матричном представлении это выглядит как

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \quad (2.85)$$

Упражнение 2.51. Проверьте, что оператор Адамара H является унитарным.

Упражнение 2.52. Докажите, что $H^2 = I$.

Упражнение 2.53. Чему равны собственные числа и собственные векторы оператора H ?

Для использования постулата 2 необходимо, чтобы описываемая система была замкнутой. Иными словами, она не должна взаимодействовать каким-

либо образом с другими системами. В действительности же все системы (кроме Вселенной в целом) взаимодействуют с какими-то системами. Тем не менее существуют интересные системы, которые могут быть с хорошей точностью описаны как замкнутые и эволюция которых таким образом с хорошей точностью задается унитарным оператором. Заметим также, что в принципе любая открытая система может быть описана как часть большей замкнутой системы (Вселенной), эволюция которой может быть задана унитарным оператором. Ниже будут введены новые средства для описания эволюции открытых систем, однако пока мы будем изучать только поведение замкнутых систем.

Постулат 2 показывает, как связаны между собой состояния замкнутой квантовой системы в два разных момента времени. Можно указать уточненный вариант этого постулата, который описывает эволюцию квантовой системы в дифференциальной форме. Из этого уточненного постулата мы восстановим постулат 2. Однако прежде чем сформулировать по-новому постулат, хотелось бы отметить два обстоятельства. Во-первых, оператор H , который вводится в постулате 2' и используется в дальнейшем, не совпадает с введенным выше оператором Адамара. Во-вторых, в постулате 2' используется аппарат дифференциальных уравнений. Заверяем читателей, не очень хорошо знакомых с теорией дифференциальных уравнений, что она не понадобится нигде в нашей книге, кроме некоторых разделов гл. 7, где обсуждаются конкретные физические реализации систем обработки квантовой информации.

Постулат 2'. Эволюция состояния замкнутой квантовой системы во времени описывается *уравнением Шредингера*

$$i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle. \quad (2.86)$$

В этом уравнении \hbar — физическая постоянная, называемая *постоянной Планка*, и ее значение подлежит определению в эксперименте. Нас не будет интересовать ее точное значение. У теоретиков принято включать множитель \hbar в состав оператора H , что фактически означает приравнивание этого множителя к единице. Буквой H обозначен фиксированный для данной системы эрмитов оператор, называемый *гамильтонианом замкнутой системы*.

Если известен гамильтониан системы (предполагается, что значение постоянной \hbar определено), можно получить полное представление о динамике системы (по крайней мере в принципе). Вообще говоря, нахождение гамильтониана (необходимого для описания конкретной физической системы) — очень сложная задача; значительная часть задач физики XX в. заключалась именно в этом; для решения указанной задачи требуется большое количество данных, определяемых в экспериментах. С нашей точки зрения конкретный вид гамильтониана, необходимого для описания атомов в той или иной конфигурации, — *детализация*, которая должна обсуждаться в физических теориях, построенных в рамках квантовой механики, а не в теории квантовой механики как таковой. В большей части материала о квантовых вычислениях и обработке квантовой информации гамильтонианы рассматриваться не будут. Когда они все-таки будут обсуждаться, мы будем просто начинать с утверждения, что

некоторая матрица является гамильтонианом системы, не пытаясь оправдать использование именно такого гамильтониана.

Поскольку гамильтониан является эрмитовым оператором, для него существует спектральное разложение:

$$H = \sum_E E |E\rangle\langle E| \quad (2.87)$$

с собственными числами E и соответствующими нормированными собственными векторами $|E\rangle$. Состояния $|E\rangle$ обычно называют *энергетическими уровнями* или *стационарными состояниями*, а числа E — *энергиями состояний* $|E\rangle$. Наименьшая энергия из набора E — *энергия основного состояния* системы, а соответствующее стационарное состояние (или собственное пространство, если данной энергии отвечает несколько независимых векторов) — *основное состояние*. Состояния $|E\rangle$ называют стационарными потому, что их эволюция во времени сводится к умножению на числовую множитель, равный по модулю единице:

$$|E\rangle \rightarrow \exp(-iEt/\hbar)|E\rangle. \quad (2.88)$$

Рассмотрим следующий пример. Пусть одиночный кубит описывается гамильтонианом

$$H = \hbar\omega X. \quad (2.89)$$

В этом уравнении ω — параметр, который в принципе должен быть определен экспериментально. Не следует специально беспокоиться об этом параметре — в данный момент мы хотим показать, какие типы гамильтонианов появляются в теории квантовых вычислений и обработки квантовой информации. Очевидно, что стационарные состояния у этого гамильтониана будут такими же, как и у оператора X , а именно: $(|0\rangle + |1\rangle)/\sqrt{2}$ и $(|0\rangle - |1\rangle)/\sqrt{2}$, при этом соответствующие им энергии равны $\hbar\omega$ и $-\hbar\omega$. Таким образом, основным является состояние $(|0\rangle - |1\rangle)/\sqrt{2}$, а энергия основного состояния равна $-\hbar\omega$.

Какова связь между гамильтоновым описанием динамики (постулат 2') и описанием через унитарные операторы (постулат 2)? Ответ мы узнаем, если выпишем решение уравнения Шредингера. Легко проверить, что оно имеет вид

$$|\psi(t_2)\rangle = \exp\left[\frac{-iH(t_2 - t_1)}{\hbar}\right] |\psi(t_1)\rangle = U(t_1, t_2) |\psi(t_1)\rangle, \quad (2.90)$$

где введено обозначение

$$U(t_1, t_2) \equiv \exp\left[\frac{-iH(t_2 - t_1)}{\hbar}\right]. \quad (2.91)$$

Вскоре можно будет убедиться, что этот оператор является унитарным, а также что любой унитарный оператор U может быть представлен в виде $U = \exp(iK)$, где K — некоторый эрмитов оператор. Таким образом, существует соответствие между описанием динамики в разные моменты времени с использованием унитарных операторов и дифференциальным описанием с использова-

нием гамильтонианов. В большей части нашей книги мы будем использовать первое из этих двух описаний.

Упражнение 2.54. Пусть A и B — коммутирующие эрмитовы операторы. Докажите, что $\exp(A)\exp(B) = \exp(A+B)$. (*Указание:* Используйте результаты, полученные в подразд. 2.1.9.)

Упражнение 2.55. Докажите, что оператор $U(t_1, t_2)$, определенный в уравнении (2.91), является унитарным.

Упражнение 2.56. Используя спектральное разложение, покажите, что для любого унитарного оператора U оператор $K \equiv -i \log(U)$ является эрмитовым, а следовательно, $U = \exp(iK)$ для некоторого эрмитова оператора K .

В теории квантовых вычислений и обработки квантовой информации мы часто будем говорить о *применении* того или иного унитарного оператора для конкретной квантовой системы. Например, при обсуждении квантовых схем будет рассмотрен вопрос о действии унитарного элемента X на одиночный кубит. Не противоречит ли это введенному выше тезису о том, что унитарные операторы описывают эволюцию замкнутой квантовой системы? В конце концов ведь если говорится, что мы применяем унитарный оператор, то подразумевается, что существует внешнее «мы», взаимодействующее с квантовой системой, т. е. система не является замкнутой.

Примером подобной ситуации является фокусировка лазерного луча на атоме. Напряженно потрудившись, можно написать гамильтониан, задающий систему атом–лазер. Интересна следующая особенность такого гамильтониана. Если рассматривать эффекты, относящиеся только к атому, то оказывается, что поведение атома почти полностью, хотя и не идеально, описывается другим гамильтонианом — *гамильтонианом атома*. Он содержит члены, связанные с интенсивностью и другими параметрами лазера, которые можно изменять. Все выглядит так, как если бы эволюция атома описывалась гамильтонианом, который можно менять, хотя атом и не является замкнутой системой.

В заключение отметим, что во многих случаях оказывается возможным написать *переменный во времени* гамильтониан квантовой системы, который зависит от параметров, находящихся под управлением экспериментатора. Таким образом, система не является замкнутой, но эволюционирует в соответствии с уравнением Шредингера с зависящим от времени гамильтонианом (по крайней мере с хорошей точностью).

Итак, в качестве начального приближения мы будем часто описывать эволюцию квантовомеханических систем с использованием унитарных операторов, даже если эти системы не замкнутые. Главное исключение — квантовое измерение — рассматривается в следующем подразделе. В дальнейшем более подробно будет исследован вопрос об отклонении от эволюции, описываемой унитарными операторами, связанном с взаимодействием с другими системами, так, что можно будет более точно понять динамику реальных квантовых систем.

2.2.3 Квантовые измерения

Выше был введен постулат о том, что эволюция замкнутой квантовой системы описывается унитарным оператором. С эволюцией системы, которая не взаимодействует с остальным окружающим миром, все в порядке. Однако экспериментаторам и их приборам, другими словами, — внешней физической системе — следует наблюдать за данной системой, чтобы определить, что происходит внутри нее. В таком случае система перестает быть замкнутой, а ее эволюция уже не обязательно описывается унитарным оператором. Для описания такой ситуации введем постулат 3 о воздействии измерений на квантовые системы.

Постулат 3. Квантовые измерения описываются набором $\{M_m\}$ *операторов измерения*. Это операторы, действующие в пространстве состояний системы, подлежащей измерению. Индекс обозначает результаты измерения, которые могут получиться в эксперименте. Если непосредственно перед этим квантовая система находилась в состоянии $|\psi\rangle$, то вероятность того, что в результате измерения будет получен результат m , задается выражением

$$p(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle, \quad (2.92)$$

а после измерения система будет находиться в состоянии

$$\frac{M_m |\psi\rangle}{\sqrt{\langle \psi | M_m^\dagger M_m | \psi \rangle}}. \quad (2.93)$$

Операторы измерения удовлетворяют *условию полноты*

$$\sum_m M_m^\dagger M_m = I. \quad (2.94)$$

Условие полноты означает, что сумма вероятностей различных исходов измерения равна единице.

$$1 = \sum_m p(m) = \sum_m \langle \psi | M_m^\dagger M_m | \psi \rangle. \quad (2.95)$$

Справедливость этого уравнения для всех $|\psi\rangle$ эквивалентна выполнению условия полноты. Однако условие полноты проще проверять непосредственно, поэтому оно и введено в качестве отдельного утверждения в постулат 3.

Простым, но важным примером измерения является *измерение кубита в вычислительном базисе*. Это измерение над одиночным кубитом с двумя возможными результатами, определяемыми двумя операторами измерения: $M_0 = |0\rangle\langle 0|$, $M_1 = |1\rangle\langle 1|$. Заметим, что каждый из операторов измерения является эрмитовым и что $M_0^2 = M_0$, $M_1^2 = M_1$. Следовательно, условие полноты выполнено: $I = M_0^\dagger M_0 + M_1^\dagger M_1 = M_0 + M_1$. Пусть измеряемое состояние задается вектором $|\psi\rangle = a|0\rangle + b|1\rangle$. Тогда вероятность получения результата 0 определяется формулой

$$p(0) = \langle \psi | M_0^\dagger M_0 | \psi \rangle = \langle \psi | M_0 | \psi \rangle = |a|^2. \quad (2.96)$$

Аналогичным образом, вероятность получения результата 1 представляется формулой $p(1) = |b|^2$. После измерения вектор состояния будет равен

$$\frac{M_0|\psi\rangle}{|a|} = \frac{a}{|a|}|0\rangle \quad (2.97)$$

или

$$\frac{M_1|\psi\rangle}{|b|} = \frac{b}{|b|}|1\rangle. \quad (2.98)$$

Из подразд. 2.2.7 следует, что на множители вида $a/|a|$, равные по модулю единице, можно в сущности не обращать внимания, поэтому два последних выражения фактически сводятся к $|0\rangle$ и $|1\rangle$, как это описывалось в гл. 1.

Является ли постулат 3 столь же фундаментальным, как и предыдущие? Ведь измерительные устройства являются квантовомеханическими системами. Поэтому подлежащая измерению квантовая система и измерительное устройство вместе входят в состав большей изолированной квантовомеханической системы. (Возможно, для получения полностью изолированной системы в нее потребуется включить не только систему, над которой производится измерение, и измерительное устройство, но и еще какие-то объекты,— ключевой момент состоит в том, что в принципе это можно сделать.) В соответствии с постулатом 2 эволюция этой большой системы описывается унитарным оператором. Можно ли вывести постулат 3 как следствие из этого описания? Несмотря на многочисленные исследования на данную тему, между физиками по-прежнему нет полного согласия относительно того, возможно ли это. Мы собираемся придерживаться сугубо прагматичного подхода: на практике бывает ясно, когда применять постулат 2, а когда — постулат 3, так что не обязательно заботиться о выводе одного постулата из другого.

В следующих нескольких подразделах мы будем применять постулат 3 для ряда элементарных, но весьма полезных сценариев измерений. Так, подраздел 2.2.4 посвящен изучению проблемы *различения* нескольких квантовых состояний. В подразд. 2.2.5 раскрывается особый случай применения постулата 3 — *проективные измерения*, или измерения фон Неймана. В подразд. 2.2.6 речь идет о другом случае применения постулата 3, известном как *POVM*-измерения. Во многих введениях в квантовую механику обсуждаются только проективные измерения, а полное обсуждение постулата 3 или POVM-элементов опускается. По этой причине мы включили вставку 2.5, где исследуется отношение между разными классами описываемых нами измерений..

Упражнение 2.57 (последовательные измерения эквивалентны одному измерению). Пусть $\{L_l\}$ и $\{M_m\}$ — два набора операторов измерений. Покажите, что последовательное выполнение измерения, задаваемого операторами $\{L_l\}$, и операторами $\{M_m\}$, физически эквивалентно одному измерению, задаваемому операторами $\{N_{lm}\}$, где $N_{lm} \equiv M_m L_l$.

2.2.4 Различение квантовых состояний

Важным применением постулата 3 является задача *различения квантовых состояний*. В классическом мире разные состояния объекта обычно различимы. Например, при падении монеты мы всегда можем различить, выпал орел или решка. В квантовой механике ситуация гораздо сложнее. В разд. 1.6 приведен правдоподобный аргумент, почему нельзя различить неортогональные состояния. Опираясь на постулат 3, можно продемонстрировать этот факт более убедительно.

Различимость, как и многие идеи в квантовых вычислениях и обработке квантовой информации, проще всего понять, на примере игры с двумя участниками — Алисой и Бобом. Алиса выбирает состояние $|\psi_i\rangle$ ($1 \leq i \leq n$) из некоторого фиксированного набора состояний, известного обоим участникам. Она передает состояние $|\psi_i\rangle$ Бобу, цель которого — определить индекс i этого состояния.

Предположим, что состояния $|\psi_i\rangle$ образуют ортонормированный набор. Тогда Боб может *различить* эти состояния с помощью квантового измерения, операторы которого задаются следующим образом: $M_i \equiv |\psi_i\rangle\langle\psi_i|$ — по одному на каждый индекс i , — а также дополнительный оператор измерения M_0 , равный квадратному корню из неотрицательно определенного оператора $I - \sum_{i \neq 0} |\psi_i\rangle\langle\psi_i|$. Эти операторы удовлетворяют условию полноты, и если приготовлено состояние $|\psi_i\rangle$, то $p(i) = \langle\psi_i|M_i|\psi_i\rangle = 1$, т. е. результат i получается с единичной вероятностью. Следовательно, можно с уверенностью различить ортонормированные состояния $|\psi_i\rangle$.

Напротив, если состояния $|\psi_i\rangle$ не образуют ортонормированного набора, то можно доказать, что *не существует квантового измерения, различающего эти состояния*. Идея заключается в том, что Боб будет делать измерение, описываемое операторами M_j , дающими результаты j . В зависимости от результата измерения Боб пытается угадать, какому индексу i соответствовало исходное состояние. Для этого он использует некоторое правило (функцию $i = f(j)$). Причина, по которой Боб не может различить неортогональные состояния $|\psi_1\rangle$ и $|\psi_2\rangle$, состоит в следующем: $|\psi_2\rangle$ раскладывается в сумму (ненулевой) компоненты, параллельной вектору $|\psi_1\rangle$, и компоненты, ортогональной вектору $|\psi_1\rangle$. Пусть j — такой результат измерения, для которого $f(j) = 1$, т. е. Боб определяет, что сначала система была в состоянии $|\psi_1\rangle$, если он получает в качестве результата измерения j . Но поскольку у вектора $|\psi_2\rangle$ есть составляющая, параллельная вектору $|\psi_1\rangle$, существует ненулевая вероятность того, что результат j был получен и в том случае, когда исходным было состояние $|\psi_2\rangle$. Следовательно, Боб иногда будет ошибаться при определении исходного состояния. Более строго это рассуждение проведено на вставке 2.3.

2.2.5 Проективные измерения

Рассмотрим важный случай постулата 3. Имеется в виду специальный класс измерений, известный как *проективные измерения*. Во многих применениях

Вставка 2.3. Доказательство неразличимости неортогональных состояний

Докажем от противного, что никакое измерение не позволяет различить неортогональные состояния $|\psi_1\rangle$ и $|\psi_2\rangle$. Предположим обратное, т. е. будем считать, что измерение, различающее эти два состояния, существует. Если приготовлено состояние $|\psi_1\rangle$ ($|\psi_2\rangle$), то вероятность получить при измерении такой результат j , что $f(j) = 1$ ($f(j) = 2$), равна единице. Введем оператор $E_i \equiv \sum_{j:f(j)=i} M_j^\dagger M_j$, тогда можно записать, что

$$\langle\psi_1|E_1|\psi_1\rangle = 1, \quad \langle\psi_2|E_2|\psi_2\rangle = 1. \quad (2.99)$$

Поскольку $\sum_i E_i = I$, то $\sum_i \langle\psi_1|E_i|\psi_1\rangle = 1$, а так как $\langle\psi_1|E_1|\psi_1\rangle = 1$, должно выполняться равенство $\langle\psi_1|E_2|\psi_1\rangle = 0$, т. е. $\sqrt{E_2}|\psi_1\rangle = 0$. Предположим, что мы разложили вектор $|\psi_2\rangle$ на две составляющие: $|\psi_2\rangle = \alpha|\psi_1\rangle + \beta|\varphi\rangle$, где вектор $|\varphi\rangle$ ортогонален вектору $|\psi_1\rangle$ и равен по модулю единице, $|\alpha|^2 + |\beta|^2 = 1$, $|\beta| < 1$, поскольку векторы $|\psi_1\rangle$ и $|\psi_2\rangle$ не ортогональны. Тогда $\sqrt{E_2}|\psi_2\rangle = \beta\sqrt{E_2}|\varphi\rangle$, что противоречит равенству (2.99), поскольку

$$\langle\psi_2|E_2|\psi_2\rangle = |\beta|^2 \langle\varphi|E_2|\varphi\rangle \leq |\beta|^2 < 1, \quad (2.100)$$

где предпоследнее неравенство следует из того, что

$$\langle\varphi|E_2|\varphi\rangle \leq \sum_i \langle\varphi|E_i|\varphi\rangle = \langle\varphi|\varphi\rangle = 1. \quad (2.101)$$

квантовых вычислений и обработки квантовой информации в первую очередь имеют дело с проективными измерениями. Такие измерения фактически эквивалентны измерениям общего вида, описанным в постулате 3, если добавить к ним возможность выполнения унитарных преобразований, описываемых постулатом 2. Это может показаться удивительным, так как описание проективных измерений на первый взгляд совсем непохоже на описание общих измерений. Отмеченная эквивалентность будет объяснена ниже (см. подразд. 2.2.8).

Проективные измерения. Проективное измерение описывается наблюдаемой M , т. е. эрмитовым оператором, действующим в пространстве состояний изучаемой системы. Наблюдаемая может быть представлена в виде спектрального разложения:

$$M = \sum_m m P_m, \quad (2.102)$$

где P_m — проектор на собственное подпространство, соответствующее оператору M , с собственным числом m . Возможные результаты измерения соответствуют собственным числам m наблюдаемой. При измерении над состоянием $|\psi\rangle$ вероятность получения результата m задается выражением

$$p(m) = \langle\psi|P_m|\psi\rangle. \quad (2.103)$$

В предположении того, что результат измерения равен m , состояние квантовой системы непосредственно после измерения определяется вектором

$$\frac{P_m |\psi\rangle}{\sqrt{p(m)}}. \quad (2.104)$$

Проективные измерения можно представлять себе как частный случай измерений, описываемых в постулате 3. Предположим, что оператор измерения из постулата 3 не только удовлетворяет условию полноты $\sum_m M_m^\dagger M_m = I$, но и обладает тем свойством, что все операторы M_m являются ортогональными проекторами, т. е. M_m — эрмитовы операторы, $M_m M_{m'} = \delta_{mm'} M_m$. При этих дополнительных ограничениях постулат 3 будет определять только проективные операторы, введенные выше.

Вставка 2.4. Принцип неопределенности Гейзенберга

Возможно, наиболее известным результатом из квантовой механики является *принцип неопределенности Гейзенberга*. Пусть A и B — два эрмитовых оператора, $|\psi\rangle$ — квантовое состояние. Предположим, $\langle\psi|AB|\psi\rangle = x + iy$, где x и y — действительные числа. Заметим, что $\langle\psi|[A, B]|\psi\rangle = 2iy$, $\langle\psi|\{A, B\}|\psi\rangle = 2x$. Из этого следует, что

$$|\langle\psi|[A, B]|\psi\rangle|^2 + |\langle\psi|\{A, B\}|\psi\rangle|^2 = 4|\langle\psi|AB|\psi\rangle|^2. \quad (2.105)$$

Согласно неравенству Коши–Шварца, имеем соотношение

$$|\langle\psi|AB|\psi\rangle|^2 \leq \langle\psi|A^2|\psi\rangle\langle\psi|B^2|\psi\rangle, \quad (2.106)$$

которое вместе с формулой (2.105) после отбрасывания неотрицательных слагаемых дает неравенство

$$|\langle\psi|[A, B]|\psi\rangle|^2 \leq 4\langle\psi|A^2|\psi\rangle\langle\psi|B^2|\psi\rangle. \quad (2.107)$$

Пусть C и D — две наблюдаемые. Сделав в последнем уравнении замены $A = C - \langle C \rangle$ и $B = D - \langle D \rangle$, получим принцип неопределенности Гейзенберга в наиболее распространенной форме:

$$\Delta(C)\Delta(D) \geq \frac{|\langle\psi|[C, D]|\psi\rangle|}{2}. \quad (2.108)$$

Следует проявлять осторожность и не повторять стандартного заблуждения относительно принципа неопределенности (о том, что измерение значения наблюдаемой C с «точностью» $\Delta(C)$ приводит к «возмущению» значения D на некоторую величину $\Delta(D)$ таким образом, что выполняется неравенство, подобное (2.108)). Хотя измерение в квантовой механике действительно приводит к возмущению измеряемой системы, следует подчеркнуть, что содержание принципа неопределенности заключается *не* в этом.

Правильная интерпретация принципа неопределенности такова. Если мы приводим большое количество квантовых систем в идентичные состояния ($|\psi\rangle$), а затем выполняем измерения значений наблюдаемой C над некоторыми из этих систем и значений наблюдаемой D над остальными, то произведение среднеквадратичного отклонения $\Delta(C)$ величины C на среднеквадратичное отклонение $\Delta(D)$ величины D будет удовлетворять неравенству (2.108). В качестве иллюстрации принципа неопределенности рассмотрим измерение наблюдаемых X и Y над квантовым состоянием $|0\rangle$. Было показано, что $[X, Y] = 2iZ$ (см. уравнение (2.70)), поэтому в соответствии с принципом неопределенности получим

$$\Delta(X)\Delta(Y) \geq \langle 0|Z|0 \rangle = 1. \quad (2.109)$$

Из этого неравенства следует, что обе величины $\Delta(X)$ и $\Delta(Y)$ должны быть одновременно строго больше нуля (что легко проверяется прямым вычислением).

Проективные измерения обладают рядом замечательных свойств. В частности, очень легко вычислить среднее значение таких измерений. По определению измерения, среднее значение (или математическое ожидание, см. элементарные определения и результаты из теории вероятностей в Приложении 1) задается выражением

$$E(M) = \sum_m mp(m) \quad (2.110)$$

$$= \sum_m m\langle\psi|P_m|\psi\rangle \quad (2.111)$$

$$= \left\langle \psi \left| \left(\sum_m mP_m \right) \right| \psi \right\rangle \quad (2.112)$$

$$= \langle\psi|M|\psi\rangle. \quad (2.113)$$

Это очень полезная формула, которая упрощает многие вычисления. Среднее значение наблюдаемой M часто записывают в виде $\langle M \rangle = \langle\psi|M|\psi\rangle$. Из этой формулы для среднего значения получают выражение для среднеквадратичного отклонения величины, связанной с наблюдаемой M :

$$[\Delta(M)]^2 = \langle (M - \langle M \rangle)^2 \rangle \quad (2.114)$$

$$= \langle M^2 \rangle - \langle M \rangle^2. \quad (2.115)$$

Среднеквадратичное отклонение — это мера типичного разброса получаемых в эксперименте значений наблюдаемой M . В частности, если выполняется большое количество экспериментов, в которых заранее подготавливается состоя-

ние $|\psi\rangle$ и измеряется значение наблюдаемой M , то дисперсия $\Delta(M)$ получаемых значений определяется формулой $\Delta(M) = \langle M^2 \rangle - \langle M \rangle^2$. Формулировка в терминах наблюдаемых приводит элегантным образом к результату, известному под названием *принципа неопределенности Гейзенберга* (см. вставку 2.4).

Упражнение 2.58. Предположим, мы приготовили квантовую систему в собственном для некоторой наблюдаемой M состоянии $|\psi\rangle$ (соответствующее собственное значение равно m). Чему будут равны среднее измеренное значение наблюдаемой M и среднеквадратичное отклонение?

Следует упомянуть два широко используемых обозначения. Вместо того чтобы описывать проективные измерения с помощью наблюдаемых, часто просто выписывают полное множество ортогональных проекторов P_m , удовлетворяющих соотношениям $\sum_m P_m = I$ и $P_m P_{m'} = \delta_{mm'} P_m$. Наблюдаемая, подразумеваемая в этих выражениях, имеет вид $M = \sum_m m P_m$. Другое широко используемое выражение — «измерение в базисе $|m\rangle$ », где $|m\rangle$ — ортонормированный базис, и оно означает просто выполнение проективных измерений с проекторами $P_m = |m\rangle\langle m|$.

Рассмотрим теперь пример проективных измерений на одиночном кубите. Сначала обсудим измерение наблюдаемой Z с собственными числами $+1$ и -1 и соответствующими им собственными векторами $|0\rangle$ и $|1\rangle$. Например, измерение Z для состояния $|\psi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ дает результат $+1$ с вероятностью $\langle\psi|0\rangle\langle 0|\psi\rangle = 1/2$; аналогично доказывается, что результат -1 получается также с вероятностью $1/2$. Рассмотрим более общий случай. Пусть \vec{v} — единичный вектор в трехмерном действительном пространстве. Тогда можно определить наблюдаемую

$$\vec{v} \cdot \vec{\sigma} \equiv v_1 \sigma_1 + v_2 \sigma_2 + v_3 \sigma_3. \quad (2.116)$$

Измерение этой наблюдаемой иногда называют «измерением компоненты спина вдоль оси \vec{v} » (для этого имеются исторические причины). Следующие два первых упражнения позволяют лучше узнать некоторые простые, но важные свойства таких измерений.

Упражнение 2.59. Пусть кубит находится в состоянии $|0\rangle$ и выполняется измерение наблюдаемой X . Чему равно среднее значение и среднеквадратичное отклонение X ?

Упражнение 2.60. Покажите, что собственные значения оператора $\vec{v} \cdot \vec{\sigma}$ равны ± 1 , а проекторы на соответствующие собственные пространства определяются выражениями $P_{\pm} = (I \pm \vec{v} \cdot \vec{\sigma})/2$.

Упражнение 2.61. Вычислите вероятность получения результата $+1$ при измерении $\vec{v} \cdot \vec{\sigma}$, полагая, что перед измерением система находилась в состоянии $|0\rangle$. В каком состоянии будет находиться система после измерения, если известно, что было получено значение $+1$?

2.2.6 POVM-измерения

Постулат о квантовых измерениях (постулат 3) содержит два ключевых момента. Во-первых, он определяет правило, описывающее статистику измерений,

т. е. вероятности возможных результатов измерений. Во-вторых, он дает правило, описывающее состояние системы после измерения. Однако в некоторых случаях состояние системы после измерения не представляет большого интереса, а главное, что интересует исследователя, — возможные результаты измерения. Такая ситуация, например, имеет место, когда измерение над системой производится только один раз — по окончании эксперимента. В таких ситуациях применяется математический метод, называемый *POVM-формализм*, который особенно хорошо приспособлен для анализа результатов измерений. («POVM» является сокращением словосочетания «Positive Operator-Valued Measure», — технического термина, происхождение которого не представляет для нас интереса.) Этот формализм есть просто следствие из общего описания измерений, данного в постулате 3, но теория POVM-измерений столь элегантна и широко используема, что заслуживает отдельного обсуждения.

Пусть измерение, описываемое операторами измерений M_m , выполняется над квантовой системой, находящейся в состоянии $|\psi\rangle$. Тогда вероятность результата m задается формулой $p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$. Введем определение

$$E_m \equiv M_m^\dagger M_m. \quad (2.117)$$

Из постулата 3 и элементарной линейной алгебры следует, что E_m — неотрицательно определенный оператор и $\sum_m E_m = I$, а $p(m) = \langle\psi|E_m|\psi\rangle$. Таким образом, набор операторов E_m достаточен для определения вероятностей различных исходов измерения. Операторы E_m — это *POVM-элементы*, связанные с измерением, а полный набор $\{E_m\}$ называют *POVM*.

В качестве примера POVM-измерений рассмотрим проективное измерение, описываемое операторами измерений P_m , которые являются проекторами и обладают свойствами $P_m P_{m'} = \delta_{mm'} P_m$ и $\sum_m P_m = I$. В таком (и только в таком) случае все POVM-элементы совпадают с самими операторами измерений, поскольку $E_m \equiv P_m^\dagger P_m = P_m$.

Упражнение 2.62. Покажите, что любое измерение, в котором операторы измерения и POVM-элементы совпадают, является проективным.

Выше мы отмечали, что POVM-операторы являются неотрицательно определенными и удовлетворяют условию $\sum_m E_m = I$. Пусть теперь $\{E_m\}$ — некоторый произвольный набор неотрицательно определенных операторов, для которого $\sum_m E_m = I$. Покажем, что существует набор операторов измерений M_m , определяющий измерение, описываемое POVM-операторами $\{E_m\}$. Положив $M_m \equiv \sqrt{E_m}$, получим $\sum_m M_m^\dagger M_m = \sum_m E_m = I$, а значит, множество $\{M_m\}$ описывает измерение, задаваемое POVM-операторами $\{E_m\}$. Поэтому удобно определить набор POVM-операторов как такое множество операторов $\{E_m\}$, когда все операторы E_m являются неотрицательно определенными и выполняется условие полноты: $\sum_m E_m = I$ (это означает, что сумма вероятностей всех результатов равна единице). Напомним, что если задан набор POVM-операторов $\{E_m\}$, то вероятность результата m задается выражением $p(m) = \langle\psi|E_m|\psi\rangle$.

Мы рассмотрели проективные измерения как пример использования POVM-операторов, однако это не очень интересно, поскольку мы не узнали ниче-

го нового. Ниже приводится более сложный пример использования POVM-формализма. Пусть Алиса выдает Бобу кубит, находящийся в одном из двух состояний: $|\psi_1\rangle = |0\rangle$ или $|\psi_2\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. Как объяснялось в подразд. 2.2.4, Боб не может надежно определить, выдан ему кубит в состоянии $|\psi_1\rangle$ или $|\psi_2\rangle$. Тем не менее он может выполнить измерение, которое различает состояния в некоторых случаях и *никогда* не выдает неправильного ответа. Рассмотрим набор из трех POVM-элементов:

$$E_1 \equiv \frac{\sqrt{2}}{1+\sqrt{2}} |1\rangle\langle 1|, \quad (2.118)$$

$$E_2 \equiv \frac{\sqrt{2}}{1+\sqrt{2}} \frac{(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)}{2}, \quad (2.119)$$

$$E_3 \equiv I - E_1 - E_2. \quad (2.120)$$

Можно непосредственно проверить, что все три оператора являются неотрицательно определенными и выполняется условие полноты $\sum_m E_m = I$, поэтому они образуют правильный POVM-набор.

Пусть Боб получает состояние $|\psi_1\rangle = |0\rangle$. Он выполняет измерение, описываемое POVM-набором $\{E_1, E_2, E_3\}$. Результат E_1 он получит с нулевой вероятностью, поскольку оператор E_1 выбран так, что $\langle\psi_1|E_1|\psi_1\rangle = 0$. Таким образом, если измерение даст результат E_1 , то Боб может сделать точное заключение, что ему был выдан кубит в состоянии $|\psi_2\rangle$. Аналогичное рассмотрение показывает, что если в результате измерения получен ответ E_2 , то вначале кубит находился в состоянии $|\psi_1\rangle$. Однако иногда в результате измерения Боб будет получать ответ E_3 , и тогда он не сможет сделать никакого вывода об исходном состоянии кубита. Принципиальный момент состоит в том, что Боб *никогда* не сделает неправильного вывода об исходном состоянии своего кубита. За такую безошибочность приходится платить тем, что иногда Боб не получает никакой информации об исходном состоянии кубита.

Этот простой пример демонстрирует полезность POVM-формализма в качестве простого и удобного способа работы с квантовыми измерениями в тех случаях, когда важна только статистика измерений. Далее мы будем часто интересоваться только статистикой, поэтому будем использовать POVM-формализм, а не более общий, описанный в постулате 3.

Упражнение 2.63. Пусть некоторое измерение описывается операторами измерений M_m . Покажите, что существуют такие унитарные операторы U_m , что $M_m = U_m \sqrt{E_m}$, где E_m — POVM-операторы, связанные с измерением.

Упражнение 2.64. Пусть Боб получает квантовое состояние, выбираемое из набора $|\psi_1\rangle, \dots, |\psi_m\rangle$ линейно-независимых состояний. Постройте такой POVM-набор $\{E_1, E_2, \dots, E_{m+1}\}$, при котором в случае, если результат измерения равен E_m ($1 \leq i \leq m$), Бобу достоверно известно, что ему было выдано состояние $|\psi_i\rangle$. (POVM-набор должен удовлетворять условию $\langle\psi_i|E_i|\psi_i\rangle > 0$ при любом i .)

Вставка 2.5. Измерения проективные, общего вида, и POVM

В большинстве вводных текстов по квантовой механике описываются только проективные измерения, вследствие чего общее описание измерений, данное в постулате 3, равно как и формализм POVM-измерений, описанный в подразд. 2.2.6, остаются малоизвестными. Причина, по которой многие физики не изучают формализм измерений общего вида, состоит в том, что над большинством физических систем можно проводить только весьма грубые измерения. В теории квантовых вычислений и в обработке квантовой информации мы стремимся к возможно большему разнообразию выполняемых измерений, так что более общее описание измерений оказывается полезным.

Конечно, если учесть другие аксиомы квантовой механики, то проективные измерения, дополненные унитарными операциями эволюции, оказываются полностью эквивалентными измерениям общего вида, как показано в подразд. 2.2.8. Поэтому физик, имеющий опыт использования проективных измерений, может задаться вопросом: почему мы начали с введения общего формализма (постулата 3)? Существует несколько причин для этого. Во-первых, в математическом отношении операторы измерений общего вида в некотором смысле проще устроены, чем проекторы, поскольку на них налагается меньше ограничений: например, нет ограничения, аналогичного условию $P_i P_j = \delta_{ij} P_i$ для проекторов. Эта более простая структура приводит также к появлению у операторов измерений общего вида многих полезных свойств, которых нет у проекторов. Во-вторых, оказывается, что в теории квантовых вычислений и в обработке квантовой информации существуют важные задачи (такие как оптимальный способ различения квантовых состояний), для решения которых используются операторы измерения общего вида, а не только проекторы.

В-третьих, проективные операторы обладают особым свойством, называемым *воспроизведимостью*. Проективные измерения повторяемы в том смысле, что если проективное измерение выполняется один раз, и при этом получается результат m , то после повторного измерения над получившимся состоянием вновь получается ответ m , а состояние не меняется. Проверим этот факт. Пусть начальное состояние задавалось вектором $|\psi\rangle$. После первого измерения система будет находиться в состоянии $|\psi_m\rangle = (P_m|\psi\rangle) / \sqrt{\langle\psi|P_m|\psi\rangle}$. Действие оператора P_m на состояние $|\psi_m\rangle$ не изменяет последнее, поэтому $\langle\psi_m|P_m|\psi_m\rangle = 1$, а, следовательно, каждое последующее измерение также даст ответ m и состояние при этом не изменится.

Воспроизводимость проективных измерений позволяет легко понять тот факт, что многие важные измерения в квантовой механике не сводятся к операторам проектирования. Например, если мы находим положение фотона с помощью посеребренного экрана, то при этом уничтожается фотон. В таком случае очевидно, что повторное измерение положения фотона невозможно. Существует также много других квантовых измерений,

которые не воспроизводимы в том смысле, в каком воспроизводимы проективные измерения. Для таких измерений следует использовать постулат 3. Где в этой картине находится место для POVM-измерений? Лучше всего рассматривать их как специальный случай формализма операторов измерений общего вида, который дает простейший способ изучения статистики измерений общего вида (когда нет необходимости знать состояние системы после измерения). POVM-операторы представляют собой удобный математический «трюк», позволяющий в некоторых случаях получить дополнительное представление о квантовых измерениях.

2.2.7 Фаза

«Фаза» — это часто используемый в квантовой механике термин, имеющий несколько конкретных значений в зависимости от контекста. Сейчас подходящий момент описать некоторые из них. Рассмотрим, например, состояние $e^{i\theta}|\psi\rangle$, где $|\psi\rangle$ — вектор состояния, θ — действительное число. Будем говорить, что состояние $e^{i\theta}|\psi\rangle$ совпадает с состоянием $|\psi\rangle$ с точностью до общего фазового множителя $e^{i\theta}$. Интересно отметить, что *статистика измерений*, предсказываемая для этих двух состояний, одинаковая. Чтобы доказать это, предположим, что M_m — оператор измерения, отвечающий некоторому квантовому измерению, и заметим, что вероятности результата m для первого и второго состояний равны соответственно $\langle\psi|M_m^\dagger M_m|\psi\rangle$ и $\langle\psi|e^{-i\theta}M_m^\dagger M_m e^{i\theta}|\psi\rangle = \langle\psi|M_m^\dagger M_m|\psi\rangle$. Таким образом, если речь идет об измерении физических величин, два указанных состояния следует считать одинаковыми. По этой причине можно игнорировать не влияющие на наблюдаемые свойства физической системы общие фазовые множители.

Существует также другой вид фазы, называемый *относительной фазой*. Рассмотрим состояния

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad \text{и} \quad \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \quad (2.121)$$

В первом из них амплитуда слагаемого $|1\rangle$ равна $1/\sqrt{2}$, во втором состоянии амплитуда слагаемого $|1\rangle$ равна $-1/\sqrt{2}$. В обоих случаях *абсолютная величина* амплитуды одна и та же, но знаки разные. В общем случае можно сказать, что две амплитуды (a и b) *различаются относительными фазами*, если существует такое действительное число θ , что $a = e^{i\theta}b$, или два состояния *различаются относительными фазами* в некотором базисе, если все их амплитуды в этом базисе получаются одна из другой умножением на фазовые множители вида $e^{i\theta}$. Например, два описанных выше состояния совпадают с точностью до сдвига фазы, поскольку амплитуды слагаемых $|0\rangle$ одинаковы (относительный фазовый множитель равен 1), а амплитуды слагаемых $|1\rangle$ различаются фазовым множителем, равным -1 . Разница между относительными фазами и общими фазовыми множителями заключается в том, что в первом случае фазовые множители могут быть различными для разных амплитуд. Поэтому

относительные фазы зависят от выбора базиса в отличие от общих фаз. Как следствие состояния, различающиеся только относительными фазами в некотором базисе, приводят к физически наблюдаемым различиям в статистике измерений, т. е. эти состояния нельзя рассматривать как физически эквивалентные, подобно тому, как мы поступали с состояниями, различающимися только общими фазовыми множителями.

Упражнение 2.65. Перепишите состояния $(|0\rangle + |1\rangle)/\sqrt{2}$ и $(|0\rangle - |1\rangle)/\sqrt{2}$ в базисе, в котором они не совпадают с точностью до относительного сдвига фазы.

2.2.8 Составные системы

Перейдем к изучению составных систем, образуемых из двух (или большего числа) отдельных физических систем. Как описывать состояния составной системы? Приводимый ниже постулат показывает, каким образом строится пространство состояний составной системы из пространств состояний входящих в нее систем.

Постулат 4. Пространство состояний составной системы представляет собой тензорное произведение пространств состояний входящих в нее систем. Более того, если берутся состояния, пронумерованные от 1 до n , и система с номером i находится в состоянии $|\psi_i\rangle$, то состояние составной системы описывается вектором $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \dots \otimes |\psi_n\rangle$.

Почему для описания состояния составной системы используется именно тензорное произведение? Можно рассматривать этот факт просто как основной постулат. В конце концов мы могли бы ожидать, что в квантовой механике существует *некоторый канонический способ* описания составных систем. Имеется ли какой-нибудь другой способ прийти к этому постулату? Приведем используемую время от времени эвристическую процедуру. Физики иногда говорят о *принципе суперпозиции в квантовой механике*, согласно которому, если $|x\rangle$ и $|y\rangle$ — два состояния квантовомеханической системы, то последняя может также находиться в любом состоянии вида $\alpha|x\rangle + \beta|y\rangle$, где $|\alpha|^2 + |\beta|^2 = 1$; такое состояние называется суперпозицией состояний $|x\rangle$ и $|y\rangle$. Для составной системы естественно было бы ожидать, что если $|A\rangle$ — некоторое состояние системы A и $|B\rangle$ — некоторое состояние системы B , то должно существовать соответствующее состояние составной системы AB , которое будем обозначать как $|A\rangle|B\rangle$. Применяя принцип суперпозиции для разнообразных состояний такого вида, получим приведенную выше формулировку постулата 4. Данное рассуждение не является доказательством, поскольку мы не объявляем принцип суперпозиции фундаментальным фактом в нашем описании квантовой механики, однако оно показывает разнообразие способов формулировки одних и тех же идей в квантовой механике.

В литературе встречается множество различных обозначений для составных систем. Это обилие отчасти объясняется тем, что разные обозначения лучше приспособлены для различных приложений, и нам тоже будет удобно при необходимости вводить специальные обозначения. В данный момент достаточ-

но указать полезные обозначения в виде нижних индексов, которые отмечают состояния и операторы, действующие на разные системы (в тех случаях, когда эти системы трудно различить по контексту). Например, в системе из трех кубитов через X_2 удобно обозначать оператор Паули σ_x , действующий на второй кубит.

Упражнение 2.66. Покажите, что среднее значение наблюдаемой $X_1 Z_2$ для системы из двух кубитов, измеренное для состояния $(|00\rangle + |11\rangle)/\sqrt{2}$, равно 0.

В подразд. 2.2.5 мы сделали утверждение, что проективных измерений вместе с унитарными преобразованиями достаточно для того, чтобы выполнить любое измерение общего вида. Доказательство этого утверждения требует использования составных квантовых систем и является красивой иллюстрацией применения постулата 4. Предположим, имеется квантовая система с пространством состояний Q и надо выполнить над ней измерение, описываемое операторами измерений M_m . Для этого введем *вспомогательную систему* с пространством состояний M , в котором выделен ортонормированный базис $|m\rangle$, находящийся во взаимнооднозначном соответствии с возможными результатами измерения, которое необходимо выполнить. Эту вспомогательную систему можно считать просто математической конструкцией, появляющейся в нашем построении, а можно рассматривать ее с физической точки зрения как включенную в опыт дополнительную систему, пространство состояний которой удовлетворяет требуемым свойствам.

Полагая, что $|0\rangle$ — некоторое фиксированное состояние системы M , а $|\psi\rangle$ — произвольное состояние системы Q , определим оператор U следующим образом:

$$U|\psi\rangle|0\rangle \equiv \sum_m M_m |\psi\rangle|m\rangle. \quad (2.122)$$

Используя ортонормированность базиса $|m\rangle$ и условие полноты $\sum_m M_m^\dagger M_m = I$, убедимся, что оператор U сохраняет скалярное произведение состояний вида $|\psi\rangle|0\rangle$:

$$\langle \varphi | \langle 0 | U^\dagger U | \psi \rangle | 0 \rangle = \sum_{m,m'} \langle \varphi | M_m^\dagger M_{m'} | \psi \rangle \langle m | m' \rangle \quad (2.123)$$

$$= \sum_m \langle \varphi | M_m^\dagger M_m | \psi \rangle \quad (2.124)$$

$$= \langle \varphi | \psi \rangle. \quad (2.125)$$

Из упражнения 2.67 следует, что оператор U может быть продолжен до унитарного оператора на пространстве $Q \otimes M$, который мы также обозначим U .

Упражнение 2.67. Пусть V — гильбертово пространство, W — его подпространство, $U: W \rightarrow V$ — линейный оператор, сохраняющий скалярное произведение, т. е. для любых $|w_1\rangle$ и $|w_2\rangle$ из пространства W имеем

$$\langle w_1 | U^\dagger U | w_2 \rangle = \langle w_1 | w_2 \rangle. \quad (2.126)$$

Докажите, что существует унитарный оператор $U': V \rightarrow V$, который *продолжает* оператор U . Другими словами, $U'|w\rangle = U|w\rangle$ для всех $|w\rangle$, лежащих

в подпространстве W , но при этом оператор U' определен на всем пространстве V . Обычно мы будем опускать штрих и использовать обозначение U для этого продолжения.

Предположим далее, что мы выполняем проективное измерение над двумя системами, описываемое проекторами $P_m \equiv I_Q \otimes |m\rangle\langle m|$. Результат m будет получен с вероятностью

$$p(m) = \langle \psi | \langle 0 | U^\dagger P_m U | \psi \rangle | 0 \rangle \quad (2.127)$$

$$= \sum_{m', m''} \langle \psi | M_m^\dagger \langle m' | (I_Q \otimes |m\rangle\langle m|) M_m | \psi \rangle | m'' \rangle \quad (2.128)$$

$$= \langle \psi | M_m^\dagger M_m | \psi \rangle, \quad (2.129)$$

что соответствует постулату 3. Общее состояние системы QM после измерения в предположении, что получен результат m , задается выражением

$$\frac{P_m U | \psi \rangle | 0 \rangle}{\sqrt{\langle \psi | U^\dagger P_m U | \psi \rangle}} = \frac{M_m | \psi \rangle | m \rangle}{\sqrt{\langle \psi | M_m^\dagger M_m | \psi \rangle}}. \quad (2.130)$$

Ясно, что состояние системы M после измерения описывается вектором $|m\rangle$, а состояние системы Q — вектором

$$\frac{M_m | \psi \rangle}{\sqrt{\langle \psi | M_m^\dagger M_m | \psi \rangle}}, \quad (2.131)$$

как это предписывается постулатом 3. Итак, используя унитарные преобразования, проективные измерения и возможность подключения вспомогательных систем, можно выполнить любое измерение описанного в постулате 3 вида.

Постулат 4 также позволяет определить одну из наиболее интересных и интригующих идей, связанных с составными квантовыми системами — идею *запутанности*. Рассмотрим состояние системы двух кубитов

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \quad (2.132)$$

Это состояние обладает тем замечательным свойством, что не существует таких двух однокубитовых состояний $|a\rangle$ и $|b\rangle$, что $|\psi\rangle = |a\rangle|b\rangle$. Убедитесь в этом самостоятельно.

Упражнение 2.68. Докажите, что $|\psi\rangle \neq |a\rangle|b\rangle$ для любых однокубитовых состояний $|a\rangle$ и $|b\rangle$.

Итак, состояние составной системы, не представимое в виде произведения состояний входящих в эту систему компонент, является *запутанным*. По причинам, которые до конца не ясны, запутанные состояния играют ключевую роль в квантовых вычислениях и обработке квантовой информации. Эти состояния будут многократно появляться в других главах. Как было показано, запутанность играет решающую роль в квантовой телепортации (см. подразд. 1.2.7). Ниже мы приведем два примера странных эффектов, обязанных

своим существованием запутанным квантовым состояниям: сверхплотное кодирование (разд. 2.3) и нарушение неравенства Белла (разд. 2.6).

2.2.9 Квантовая механика: общий взгляд

Мы рассмотрели все фундаментальные постулаты квантовой механики. Значительную часть дальнейшего изложения будет занимать получение из них следствий. Проанализируем теперь все постулаты вместе, чтобы понять роль каждого из них в общей картине.

Постулат 1 задает место действия квантовой механики, указывая, каким именно образом должно описываться состояние изолированной квантовомеханической системы. Постулат 2 говорит о том, что динамика *замкнутой* квантовомеханической системы описывается уравнением Шрёдингера, т. е. унитарной эволюцией. Постулат 3 показывает, как можно извлечь информацию из квантовой системы (в нем содержится «рецепт» для описания измерений). Постулат 4 предписывает, как должны комбинироваться друг с другом пространства состояний квантовых систем при конструировании из них составной системы.

Странным в квантовой механике (по крайней мере с классической точки зрения) является то, что мы не можем наблюдать непосредственно вектор состояния. Это похоже на игру в шахматы по правилам, согласно которым вы никогда не знаете точно, на какой клетке стоит та или иная фигура, известен лишь ряд на доске, в котором она находится. Классическая физика — и наша интуиция — говорят нам что фундаментальные свойства объекта (энергия, координаты, скорость и т.п.) доступны для наблюдения. В квантовой механике эти величины уже не являются фундаментальными, а вместо них появляется вектор состояния, который непосредственно наблюдать нельзя. Все выглядит так, как будто в квантовой механике существует *скрытый мир*, с которым мы можем взаимодействовать лишь косвенным и весьма несовершенным способом. Более того, классическая система не меняет своего состояния только из-за того, что за ней наблюдают. Представьте себе, как трудно было бы играть в теннис, если бы каждый раз, когда вы посмотрите на мяч, он менял свое положение! Однако в соответствии с постулатом 3, наблюдение в квантовой механике воздействует на систему, отчего она обычно меняет свое состояние.

Какие выводы можно сделать из этих странных свойств квантовой механики? Можно ли переформулировать квантовую механику в математически эквивалентном виде так, чтобы ее структура оказалась похожей на структуру классической физики? В разд. 2.6 мы докажем *неравенство Белла* — удивительный результат, который показывает, что любая попытка такой переформулировки обречена на неудачу. Противоречащие интуиции положения квантовой механики ставят нас в тупик. Однако не следует огорчаться по этому поводу. Можно развить такие приемы рассуждений, которые делают квантовую механику интуитивно понятной. Более того, скрытую природу вектора состояния можно использовать для решения таких задач обработки информации, которые недоступны в рамках классической механики. Без этого противоречащего интуиции поведения квантовые вычисления и квантовая обработка информации были бы гораздо менее интересными.

Мы также можем задаться следующим вопросом: «Если квантовая механика так отличается от классической физики, почему привычный нам мир выглядит настолько классическим?» Почему мы не видим проявлений скрытой природы вектора состояний в обычной жизни? Оказывается, наблюдаемый нами классический мир может быть получен из квантовой механики как приближенное описание, верное на тех масштабах времени, длины и массы, которые нам привычны в повседневной жизни. Объяснение того, как квантовая механика порождает классические законы физики, выходит за пределы нашей книги, однако читатель, которого интересует данная проблема, может ознакомиться с ее обсуждением, обратившись к разд. «История и дополнительная литература» в гл. 8.

2.3 Сверхплотное кодирование

Сверхплотное кодирование — это простое и вместе с тем удивительное приложение элементарной квантовой механики. Оно сочетает в себе конкретным и нетривиальным образом все фундаментальные идеи элементарной квантовой механики, описанные в предыдущем разделе, и поэтому является идеальным примером задачи по обработке информации, выполняемой с использованием квантовой механики.

В сверхплотном кодировании задействованы два участника, которых традиционно называют «Алиса» и «Боб». Они находятся на большом расстоянии друг от друга. Задача состоит в передаче некоторой классической информации от Алисы к Бобу. Пусть у Алисы имеются два классических бита, которые она хочет передать Бобу, но при этом она может послать ему только один кубит. Имеет ли такая задача решение?

Оказывается, это можно сделать с помощью сверхплотного кодирования. Предположим, между Алисой и Бобом разделена пара кубитов в запутанном состоянии:

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \quad (2.133)$$

Вначале в распоряжении Алисы находится первый кубит, а Боба — второй (рис. 2.3). Обратите внимание на то, что $|\psi\rangle$ — фиксированное состояние; Алиса не должна посылать Бобу какие-либо кубиты, чтобы он приготовил у себя такое состояние. Вместо этого запутанное состояние может создать заранее, например какое-нибудь третье лицо, которое отправит один из кубитов Алисе, а второй — Бобу.

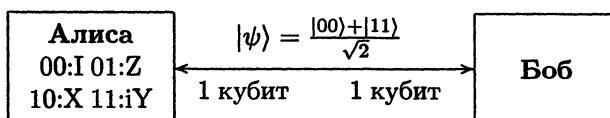


Рис. 2.3. Начальное состояние для процедуры сверхплотного кодирования Алиса и Боб имеют в своем распоряжении по половине двух кубитов в запутанном состоянии. С помощью сверхплотного кодирования Алиса может передать два классических бита Бобу, послав ему всего один кубит, но используя при этом предварительно подготовленное запутанное состояние, которое вначале частично принадлежит ей, а частично — Бобу

Покажем, что Алиса может передать Бобу два классических бита, переслав только один кубит (который она получила в начале процедуры). Если она хочет послать битовую строку 00, ей не надо выполнять никаких преобразований над своим кубитом. Если она хочет послать строку 01, ей следует применить к своему кубиту оператор переворота фазы Z . Если же она хочет отправить строку 10, она должна использовать элемент NOT (оператор X). При передаче строки 11 ей необходимо применить к своему кубиту оператор iY . Легко определить четыре получающихся состояния:

$$00 : |\psi\rangle \rightarrow \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \quad (2.134)$$

$$01 : |\psi\rangle \rightarrow \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \quad (2.135)$$

$$10 : |\psi\rangle \rightarrow \frac{|10\rangle + |01\rangle}{\sqrt{2}}, \quad (2.136)$$

$$11 : |\psi\rangle \rightarrow \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \quad (2.137)$$

Как было отмечено в подразд. 1.3.6, эти четыре состояния называют состояниями или *базисом Белла*, *состояниями Белла* либо *ЭЛР-парами* — в честь первооткрывателей, обративших внимание на новизну идеи запутанности. Обратите внимание на то, что состояния Белла образуют ортонормированный базис, поэтому их можно различить подходящим измерением. Если Алиса посыпает свой кубит Бобу, то у того в распоряжении оказываются оба кубита. Проведя измерение в базисе Белла, Боб может определить, какую из четырех возможных двухбитовых строк послала ему Алиса.

Таким образом, Алиса, передавая только 1 кубит, может сообщить два бита информации Бобу. Конечно, в протоколе используются 2 кубита, но Алиса никогда не будет воздействовать на второй кубит. Если бы Алиса передавала один классический бит, задача была бы неразрешимой (это будет показано в гл. 12). Укажем также, что описанный выше протокол сверхплотного кодирования был частично проверен в эксперименте (см. ссылки на экспериментальную проверку в разд. «История и дополнительная литература»). В других главах будет приведено много примеров использования квантовой механики для обработки информации, часть из которых будет выглядеть более эффектно, чем сверхплотное кодирование. Тем не менее ключевая идея видна в этом красивом примере: информация имеет физическую природу и удивительные физические теории (например, квантовая механика) могут приводить к удивительным возможностям в обработке информации.

Упражнение 2.69. Проверьте, что состояния (2.134)–(2.137) образуют ортонормированный базис в пространстве состояний двух кубитов.

Упражнение 2.70. Пусть E — произвольный неотрицательно определенный оператор, действующий на кубит Алисы. Покажите, что $\langle\psi|E\otimes I|\psi\rangle$ принимает одинаковое значение для любого $|\psi\rangle$ из четырех состояний Белла. Предположим, что некий недоброжелатель («Ева») перехватывает кубит Алисы на пути

к Бобу. Может ли Ева определить, какую из четырех возможных последовательностей битов (00, 01, 10 или 11) пыталась отправить Алиса? Если да, то как, а если нет, то почему?

2.4 Оператор плотности

Мы сформулировали законы квантовой механики с помощью языка векторов состояний. Существует альтернативная формулировка, в которой используется понятие *оператора*, или *матрицы, плотности*. Эта формулировка математически эквивалентна подходу, опериющему понятием векторов состояний, однако предоставляет в наше распоряжение более удобный язык для описания некоторых часто встречающихся в квантовой механике сценариев. В следующих трех подразделах будут изложены законы квантовой механики с использованием операторов плотности. В подразд. 2.4.1 с использованием понятия ансамбля квантовых состояний вводится оператор плотности. В подразд. 2.4.2 обсуждаются некоторые общие свойства оператора плотности. Наконец, в подразд. 2.4.3 рассматриваются применения, в которых оператор плотности выступает особенно ярко — как средство для описания *индивидуальных подсистем*, входящих в составную квантовую систему.

2.4.1 Ансамбли квантовых состояний

С помощью операторов плотности удобно описывать квантовые системы, состояния которых известны не полностью. Предположим, что квантовая система находится в одном из состояний набора $|\psi_i\rangle$, причем вероятность состояния $|\psi_i\rangle$ равна p_i . Будем называть $\{p_i, |\psi_i\rangle\}$ *ансамблем чистых состояний*. Оператор плотности системы определяется выражением

$$\rho \equiv \sum_i p_i |\psi_i\rangle \langle \psi_i|. \quad (2.138)$$

Этот оператор также называют *матрицей плотности*; мы будем использовать и тот и другой термин. Оказывается, все постулаты квантовой механики можно переформулировать в терминах операторов плотности. Цель данного и следующего за ним подразделов — объяснить, как это сделать и когда такая переформулировка полезна. Использовать язык операторов плотности или векторов состояний — дело вкуса, поскольку оба метода дают одинаковые результаты; тем не менее для решения некоторых конкретных задач один из этих методов оказывается гораздо удобнее другого.

Пусть, например, эволюция замкнутой квантовой системы описывается унитарным оператором U . Если система сначала находилась в состоянии $|\psi_i\rangle$ с вероятностью p_i , то в результате эволюции она окажется в состоянии $U|\psi_i\rangle$ с вероятностью p_i . Таким образом, эволюция оператора плотности описывается уравнением

$$\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i| \xrightarrow{U} \sum_i p_i U |\psi_i\rangle \langle \psi_i| U^\dagger = U \rho U^\dagger. \quad (2.139)$$

Измерения также можно легко описать на языке операторов плотности. Предположим, мы выполняем измерение, описываемое операторами M_m . Если начальное состояние задавалось вектором $|\psi_i\rangle$, то вероятность получения результата m определяется выражением

$$p(m|i) = \langle\psi_i|M_m^\dagger M_m|\psi_i\rangle = \text{tr}(M_m^\dagger M_m|\psi_i\rangle\langle\psi_i|) \quad (2.140)$$

(последнее равенство является следствием уравнения (2.61)). Из формулы полной вероятности (см. Приложение 1, где объясняется эта формула, а также другие элементарные понятия теории вероятностей) следует, что вероятность получения результата m задается выражением

$$p(m) = \sum_i p(m|i)p_i \quad (2.141)$$

$$= \sum_i p_i \text{tr}(M_m^\dagger M_m|\psi_i\rangle\langle\psi_i|) \quad (2.142)$$

$$= \text{tr}(M_m^\dagger M_m \rho). \quad (2.143)$$

Как будет выглядеть оператор плотности системы после получения результата m в процессе измерения? Если начальное состояние задавалось вектором $|\psi_i\rangle$, то состояние после получения результата m будет иметь вид

$$|\psi_i^m\rangle = \frac{M_m|\psi_i\rangle}{\sqrt{\langle\psi_i|M_m^\dagger M_m|\psi_i\rangle}}. \quad (2.144)$$

Таким образом, после измерения, в результате которого был получен ответ m , имеем ансамбль состояний $|\psi_i^m\rangle$ с соответствующими вероятностями $p(i|m)$. Соответствующий этому ансамблю оператор плотности ρ_m задается выражением

$$\rho_m = \sum_i p(i|m)|\psi_i^m\rangle\langle\psi_i^m| = \sum_i p(i|m) \frac{M_m|\psi_i\rangle\langle\psi_i|M_m^\dagger}{\langle\psi_i|M_m^\dagger M_m|\psi_i\rangle}. \quad (2.145)$$

Из элементарной теории вероятностей следует, что $p(i|m) = p(m,i)/p(m) = p(m|i)p_i/p(m)$. Используя равенства (2.143) и (2.140), получим

$$\rho_m = \sum_i p_i \frac{M_m|\psi_i\rangle\langle\psi_i|M_m^\dagger}{\text{tr}(M_m^\dagger M_m \rho)} \quad (2.146)$$

$$= \frac{M_m \rho M_m^\dagger}{\text{tr}(M_m^\dagger M_m \rho)}. \quad (2.147)$$

Мы показали, что основные постулаты квантовой механики, относящиеся к унитарной эволюции и измерениям, могут быть переформулированы на языке операторов плотности. В следующем подразделе мы завершим это переформулирование, приведя описание операторов плотности, вообще не использующее понятие вектора состояния.

Перед этим полезно ввести некоторые термины и сообщить несколько фактов, относящихся к операторам плотности. Начнем с терминов. Про квантовую систему, описываемую вектором $|\psi\rangle$, говорят, что она находится в *чистом состоянии*. В таком случае оператор плотности представляется выражением $\rho = |\psi\rangle\langle\psi|$. В противном случае говорят, что ρ описывает *смешанное состояние*, которое также называют *смесью* разных чистых состояний в ансамбле, описываемом оператором ρ . В упражнениях читателю будет предложено доказать простой критерий того, что состояние является чистым: такое состояние должно удовлетворять условию $\text{tr}(\rho^2) = 1$, в то время как для смешанного состояния $\text{tr}(\rho^2) < 1$. Хотим предупредить относительно обозначений: иногда, используя термин «смешанные состояния», имеют в виду оба случая — и чистые, и смешанные состояния. Делается это обычно для того, чтобы подчеркнуть, что не обязательно *предполагается*, что состояние является чистым. Кроме того, термин «чистое состояние» часто используется для обозначения вектора состояния $|\psi\rangle$, чтобы отличить его от оператора плотности ρ .

Наконец, представим себе квантовую систему, приготовленную в состоянии ρ_i с вероятностью p_i . Нетрудно убедиться, что систему можно описать матрицей плотности $\sum_i p_i \rho_i$. Докажем этот факт. Предположим, ρ_i возникает из ансамбля $\{p_{ij}, |\psi_{ij}\rangle\}$ (отметим, что индекс фиксирован) чистых состояний, поэтому вероятность пребывания системы в состоянии $|\psi_{ij}\rangle$ равна $p_i p_{ij}$. Матрица плотности для нашей системы имеет вид

$$\rho = \sum_{i,j} p_i p_{ij} |\psi_{ij}\rangle\langle\psi_{ij}| \quad (2.148)$$

$$= \sum_i p_i \rho_i, \quad (2.149)$$

поскольку по определению $\rho_i = \sum_j p_{ij} |\psi_{ij}\rangle\langle\psi_{ij}|$. Будем называть ρ *смесью* состояний ρ_i с вероятностями p_i . Это понятие смеси многократно появляется в анализе таких проблем, как квантовый шум, где шум ограничивает степень нашей осведомленности о квантовом состоянии. Приведем простой пример, возникающий на основе описанного выше сценария измерений. Представьте себе, что по некоторой причине был утерян результат m , полученный при измерении. Квантовая система находится в состоянии ρ_m с вероятностью $p(m)$, но мы уже не знаем настоящего значения m . Состояние такой квантовой системы будет описываться оператором плотности

$$\rho = \sum_m p(m) \rho_m \quad (2.150)$$

$$= \sum_m \text{tr}(M_m^\dagger M_m \rho) \frac{M_m \rho M_m^\dagger}{\text{tr}(M_m^\dagger M_m \rho)} \quad (2.151)$$

$$= \sum_m M_m \rho M_m^\dagger. \quad (2.152)$$

Как можно видеть, окончательная формула, которую можно использовать для дальнейшего анализа рассматриваемой системы, компактна и удобна.

2.4.2 Общие свойства операторов плотности

Оператор плотности вводился как средство для описания ансамблей квантовых состояний. В этом подразделе мы продвинемся дальше и рассмотрим определение операторов, которое не связано с представлением об ансамбле состояний. Это позволит завершить описание квантовой механики, которое не опирается на понятие вектора состояния. Кроме того, появится возможность рассмотреть другие элементарные свойства операторов плотности.

Класс операторов, являющихся операторами плотности, описывается следующей полезной теоремой.

Теорема 2.5 (свойства и признаки операторов плотности). Оператор ρ является оператором плотности, связанным с некоторым ансамблем $\{p_i, |\psi_i\rangle\}$, тогда и только тогда, когда выполняются следующие условия:

1. (условие единичности следа) след оператора ρ равен единице,
2. (условие неотрицательности) ρ — неотрицательно определенный оператор.

Доказательство. Пусть $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ — оператор плотности. Тогда

$$\text{tr}(\rho) = \sum_i p_i \text{tr}(|\psi_i\rangle\langle\psi_i|) = \sum_i p_i = 1, \quad (2.153)$$

поэтому условие единичности следа выполнено. Предположим, $|\varphi\rangle$ — произвольный вектор в пространстве состояний. В этом случае имеем

$$\langle\varphi|\rho|\varphi\rangle = \sum_i p_i \langle\varphi|\psi_i\rangle\langle\psi_i|\varphi\rangle \quad (2.154)$$

$$= \sum_i p_i |\langle\varphi|\psi_i\rangle|^2 \quad (2.155)$$

$$\geq 0, \quad (2.156)$$

и условие неотрицательности также доказано.

Теперь докажем обратное утверждение. Пусть ρ — произвольный неотрицательный оператор с единичным следом. Поскольку ρ — неотрицательно определенный оператор, для него имеется спектральное разложение

$$\rho = \sum_j \lambda_j |j\rangle\langle j|, \quad (2.157)$$

где векторы $|j\rangle$ ортогональны, а числа λ_j — действительные неотрицательные и являются собственными числами оператора ρ . Из условия единичности следа можно заключить, что $\sum_j \lambda_j = 1$. Следовательно, система, находящаяся с вероятностью λ_j в состоянии $|j\rangle$, будет описываться оператором плотности ρ . Поэтому набор $\{\lambda_j, |j\rangle\}$ — это ансамбль состояний, которому соответствует оператор ρ . ■

Эта теорема дает описание операторов плотности самих по себе: можно определить оператор плотности как неотрицательно определенный оператор ρ , след которого равен единице. После этого можно переформулировать постулаты квантовой механики на языке операторов плотности. Для упрощения ссылок приведем все переформулированные постулаты вместе.

Постулат 1. С каждой изолированной физической системой связано комплексное векторное пространство со скалярным произведением (т. е. гильберто-во пространство), которое называют *пространством состояний* системы. Система полностью описывается своим *оператором плотности* ρ , который представляет собой неотрицательно определенный оператор с единичным следом, действующий в пространстве состояний системы. Если квантовая система находится в состоянии ρ_i с вероятностью p_i , то оператор плотности равен $\sum_i p_i \rho_i$.

Постулат 2. Эволюция замкнутой квантовой системы описывается *унитарным преобразованием*, а именно: состояние ρ системы в момент времени t_1 связано с состоянием ρ' в момент t_2 унитарным оператором U , который зависит только от времен t_1 и t_2 :

$$\rho' = U \rho U^\dagger. \quad (2.158)$$

Постулат 3. Квантовые измерения описываются набором $\{M_m\}$ *операторов измерения*. Это операторы, действующие в пространстве состояний системы, над которой производится измерение. Индекс соответствует результату, который может быть получен при измерении. Если непосредственно перед измерением квантовая система находится в состоянии ρ , то вероятность получения результата m равна

$$p(m) = \text{tr}(M_m^\dagger M_m \rho), \quad (2.159)$$

а состояние системы сразу после измерения будет задаваться оператором

$$\frac{M_m \rho M_m^\dagger}{\text{tr}(M_m^\dagger M_m \rho)}. \quad (2.160)$$

Набор операторов измерений удовлетворяет *условию полноты*:

$$\sum_m M_m^\dagger M_m = I. \quad (2.161)$$

Постулат 4. Пространство состояний составной физической системы представляет собой тензорное произведение пространств состояний входящих в нее систем. Кроме того, если исходные системы пронумерованы от 1 до n и система с номером i находится в состоянии ρ_i , то общее состояние составной системы описывается оператором $\rho_1 \otimes \rho_2 \otimes \dots \otimes \rho_n$.

Приведенные выше постулаты квантовой механики, переформулированные в терминах операторов плотности, конечно, математически эквивалентны постулатам, сформулированным в терминах векторов состояний. Тем не менее описание через операторы плотности исключительно полезно в двух приложениях: для описания квантовых систем, состояния которых точно не известны, а

также для описания подсистем составных квантовых систем (об этом речь пойдет в следующем подразделе). В оставшейся части данного раздела мы более подробно ознакомимся со свойствами матриц плотности.

Упражнение 2.71 (критерий чистого состояния). Пусть ρ — оператор плотности. Покажите, что $\text{tr}(\rho^2) \leq 1$, причем равенство достигается тогда и только тогда, когда матрица ρ описывает чистое состояние.

Легко сделать следующую (распространенную) ошибку: решить, что собственные числа и собственные векторы матрицы плотности имеют особое значение для ансамбля квантовых состояний, представляемых данной матрицей плотности. Например, можно было бы предположить, что квантовая система, описываемая матрицей плотности

$$\rho = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|, \quad (2.162)$$

находится с вероятностью $3/4$ в состоянии $|0\rangle$ и с вероятностью $1/4$ в состоянии $|1\rangle$. В действительности, все может оказаться по-другому. Пусть

$$|a\rangle \equiv \sqrt{\frac{3}{4}}|0\rangle + \sqrt{\frac{1}{4}}|1\rangle, \quad (2.163)$$

$$|b\rangle \equiv \sqrt{\frac{3}{4}}|0\rangle - \sqrt{\frac{1}{4}}|1\rangle \quad (2.164)$$

и квантовую систему приготавливают с вероятностью $1/2$ в состоянии $|a\rangle$ и с вероятностью $1/2$ в состоянии $|b\rangle$. Тогда легко проверить, что соответствующая матрица плотности описывается выражением

$$\rho = \frac{1}{2}|a\rangle\langle a| + \frac{1}{2}|b\rangle\langle b| = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|. \quad (2.165)$$

Таким образом, эти два *разных* ансамбля квантовых состояний порождают *одинаковые* матрицы плотности. Вообще говоря, собственные векторы и собственные числа матрицы плотности просто указывают на *один* из возможных ансамблей, которому соответствует некоторая конкретная матрица плотности, и нет никаких причин считать, что этот ансамбль чем-то выделен по сравнению с остальными.

Отсюда возникает естественный вопрос — как устроен класс ансамблей, порождающих данную матрицу плотности? Приведенное ниже решение этой задачи очень часто используется в квантовых вычислениях и обработке квантовой информации, особенно при рассмотрении квантового шума и исправления ошибок в квантовых вычислениях (гл. 8 и 10). Для этой цели удобно использовать векторы $|\tilde{\psi}_i\rangle$, которые могут быть не нормированы на единицу. Будем говорить, что набор векторов $|\tilde{\psi}_i\rangle$ порождает оператор $\rho \equiv \sum_i |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|$, а следовательно, связь с обычным описанием операторов плотности будет задаваться равенством $|\tilde{\psi}_i\rangle = \sqrt{p_i}|\psi_i\rangle$. Возникает вопрос: когда два набора векторов ($|\tilde{\psi}_i\rangle$ и $|\tilde{\varphi}_i\rangle$) определяют один и тот же оператор ρ ? Ответ на этот вопрос поз-

волит решить задачу о том, какие ансамбли формируют заданную матрицу плотности.

Теорема 2.6 (унитарная свобода в представлении матрицы плотности). Наборы $|\tilde{\psi}_i\rangle$ и $|\tilde{\varphi}_i\rangle$ порождают одну и ту же матрицу плотности тогда и только тогда, когда

$$|\tilde{\psi}_i\rangle = \sum_j u_{ij} |\tilde{\varphi}_j\rangle, \quad (2.166)$$

где комплексные числа u_{ij} задают унитарную матрицу. Тот набор из векторов $|\tilde{\psi}_i\rangle$ и $|\tilde{\varphi}_i\rangle$, который содержит меньше элементов, следует дополнить нулевыми векторами так, чтобы в обоих наборах векторов стало поровну.

Отметим такое следствие этой теоремы: $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| = \sum_j q_j |\varphi_j\rangle\langle\varphi_j|$ для нормированных состояний $|\psi_i\rangle$ и $|\varphi_j\rangle$ с соответствующими вероятностями p_i и q_j тогда и только тогда, когда выполняется равенство

$$\sqrt{p_i} |\psi_i\rangle = \sum_j u_{ij} \sqrt{q_j} |\varphi_j\rangle \quad (2.167)$$

с некоторой унитарной матрицей u_{ij} ; в этом случае можно расширить меньший из ансамблей состояниями, встречающимися с нулевой вероятностью, чтобы количество векторов в ансамблях стало одинаковым. Таким образом, теорема 2.6 описывает свободу в выборе ансамблей $\{p_i, |\psi_i\rangle\}$, порождающих матрицу плотности ρ . Легко проверить, что наш предыдущий пример матрицы плотности с двумя разными разложениями (см. уравнение (2.162)) возникает как частный случай этого общего утверждения. Переходим к доказательству теоремы.

Доказательство.

Пусть $|\tilde{\psi}_i\rangle = \sum_j u_{ij} |\tilde{\varphi}_j\rangle$, где u_{ij} — элементы некоторой унитарной матрицы. Тогда имеем

$$\sum_i |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i| = \sum_{i,j,k} u_{ij} u_{ik}^* |\tilde{\varphi}_j\rangle\langle\tilde{\varphi}_k| \quad (2.168)$$

$$= \sum_{j,k} \left(\sum_i u_{ki}^* u_{ij} \right) |\tilde{\varphi}_j\rangle\langle\tilde{\varphi}_k| \quad (2.169)$$

$$= \sum_{j,k} \delta_{kj} |\tilde{\varphi}_j\rangle\langle\tilde{\varphi}_k| \quad (2.170)$$

$$= \sum_j |\tilde{\varphi}_j\rangle\langle\tilde{\varphi}_j|, \quad (2.171)$$

откуда следует, что наборы $|\tilde{\psi}_i\rangle$ и $|\tilde{\varphi}_j\rangle$ задают один и тот же оператор плотности.

Докажем теперь обратное утверждение. Предположим, что

$$A = \sum_i |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i| = \sum_j |\tilde{\varphi}_j\rangle\langle\tilde{\varphi}_j|. \quad (2.172)$$

Пусть $A = \sum_k \lambda_k |k\rangle\langle k|$ — такое разложение оператора A , что состояния $|k\rangle$ ортонормированы, а все числа λ_k строго положительны. Наша идея заключается в том, чтобы связать состояния $|\tilde{\psi}_i\rangle$ с состояниями $|\tilde{k}\rangle \equiv \sqrt{\lambda_k} |k\rangle$, а также аналогичным образом связать состояния $|\tilde{\varphi}_j\rangle$ и $|\tilde{k}\rangle$. Скомбинировав эти соотношения, получим нужный результат. Пусть $|\psi\rangle$ — произвольный нормированный вектор, ортогональный пространству, порождаемому набором $|\tilde{k}\rangle$: $\langle\psi|\tilde{k}\rangle\langle\tilde{k}|\psi\rangle = 0$ для всех k . Тогда нетрудно заметить, что

$$0 = \langle\psi|A|\psi\rangle = \sum_i \langle\psi_i|\tilde{\psi}\rangle\langle\tilde{\psi}|\psi_i\rangle = \sum_i |\langle\psi|\tilde{\psi}_i\rangle|^2. \quad (2.173)$$

Следовательно, $\langle\psi|\tilde{\psi}_i\rangle = 0$ для всех i и всех нормированных векторов $|\psi\rangle$, ортогональных к пространству, порождаемому набором $|\tilde{k}\rangle$. Поэтому любой вектор $|\tilde{\psi}_i\rangle$ может быть представлен в виде линейной комбинации векторов $|\tilde{k}\rangle$: $|\tilde{\psi}_i\rangle = \sum_k c_{ik} |\tilde{k}\rangle$. Поскольку $A = \sum_k |\tilde{k}\rangle\langle\tilde{k}| = \sum_i |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|$, можно заключить, что

$$\sum_k |\tilde{k}\rangle\langle\tilde{k}| = \sum_{k,l} \left(\sum_i c_{ik} c_{il}^* \right) |\tilde{k}\rangle\langle\tilde{l}|. \quad (2.174)$$

Легко видеть, что операторы $|\tilde{k}\rangle\langle\tilde{l}|$ линейно независимы, поэтому $\sum_i c_{ik} c_{il}^* = \delta_{kl}$. Отсюда следует, что можно добавить дополнительные столбцы к матрице c_{ik} , чтобы получить такую унитарную матрицу v , что $|\tilde{\psi}_i\rangle = \sum_k v_{ik} |\tilde{k}\rangle$ (в последнем равенстве добавлены нулевые векторы к набору $|\tilde{k}\rangle$). Аналогично можно найти такую унитарную матрицу w , что $|\tilde{\varphi}_j\rangle = \sum_k w_{jk} |\tilde{k}\rangle$. Таким образом, $|\tilde{\psi}_i\rangle = \sum_j u_{ij} |\tilde{\varphi}_j\rangle$, где $u = vw^\dagger$ — унитарная матрица. ■

Упражнение 2.72 (сфера Блоха для смешанных состояний). Понятие сферы Блоха для чистых состояний одиночного кубита было введено в разд. 1.2. Оно допускает приводимое ниже важное обобщение на смешанные состояния.

1. Покажите, что произвольная матрица плотности для смешанного состояния кубита может быть записана в виде

$$\rho = \frac{I + \vec{r} \cdot \vec{\sigma}}{2}, \quad (2.175)$$

где \vec{r} — такой трехмерный действительный вектор, что $\|\vec{r}\| \leq 1$. Этот вектор называют *вектором Блоха* для состояния ρ .

2. Чему равен вектор Блоха для состояния $\rho = I/2$?
3. Покажите, что состояние ρ является чистым тогда и только тогда, когда $\|\vec{r}\| = 1$.
4. Покажите, что для чистого состояния приведенное в данном упражнении описание через вектор Блоха совпадает с тем, которое приводилось в разд. 1.2.

Упражнение 2.73. Пусть ρ — оператор плотности. *Минимальный ансамбль*, порождающий ρ , — это такой ансамбль $\{p_i, |\psi_i\rangle\}$, число элементов в котором равно рангу оператора ρ . Рассмотрим любое чистое состояние $|\psi\rangle$ из носителя оператора ρ . (*Носителем* эрмитова оператора A называется векторное пространство, порожденное собственными векторами оператора A , соответствующими ненулевым собственным числам.) Покажите, что состояние $|\psi\rangle$ входит в некоторый минимальный ансамбль, определяющий ρ , причем вероятность состояния $|\psi\rangle$ в любом содержащем его минимальном ансамбле, порождающем ρ , задается формулой

$$p_i = \frac{1}{\langle \psi_i | \rho^{-1} | \psi \rangle}, \quad (2.176)$$

где ρ^{-1} — оператор, обратный оператору ρ ; при этом ρ рассматривается как оператор, действующий только на своем носителе. (Такое определение корректно и в том случае, когда у самого оператора ρ нет обратного.)

2.4.3 Редуцированный оператор плотности

Возможно, наиболее содержательное применение оператора плотности — использование его как средства для описания *подсистем* составных квантовых систем. Такое описание выполняется с помощью *редуцированного оператора плотности*, который и рассматривается в данном подразделе. Этот оператор настолько полезен, что практически всегда встречается в анализе составных квантовых систем.

Предположим, мы взяли две квантовые системы (A и B) и состояние составной системы описывается оператором плотности ρ^{AB} . Редуцированный оператор плотности для системы A определяется соотношением

$$\rho^A \equiv \text{tr}_B(\rho^{AB}), \quad (2.177)$$

где tr_B — отображение операторов, называемое *частичным следом* по системе B . Частичный след определяется следующим образом:

$$\text{tr}_B(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) \equiv |a_1\rangle\langle a_2| \text{tr}(|b_1\rangle\langle b_2|), \quad (2.178)$$

где $|a_1\rangle$ и $|a_2\rangle$ — два произвольных вектора состояния системы A , $|b_1\rangle$ и $|b_2\rangle$ — два произвольных вектора состояния системы B . Операция взятия следа в правой части — обычное взятие следа в системе B ($\text{tr}(|b_1\rangle\langle b_2|) = \langle b_2|b_1\rangle$). Мы определили частичный след только для специального подкласса операторов, действующих на пространстве состояний системы AB ; для завершения описания следует, чтобы в дополнение к уравнению (2.178) частичный след был линеен по аргументу.

Не очевидно, что редуцированный оператор плотности для системы A в каком-либо смысле задает описание состояния системы A . Физическое обоснование таково: редуцированный оператор плотности дает правильную статистику для измерений, выполняемых над системой A . Это объясняется более подробно во вставке 2.6. В качестве примера приведем несколько простых

Вставка 2.6. Почему должен оставаться частичный след?

Почему для описания части, входящей в некую квантовую систему, используется именно частичный след? Причина такова. Оператор частичного следа является единственным оператором, приводящим к правильному описанию наблюдаемых величин для подсистемы составной системы. Укажем точную формулировку этого утверждения.

Пусть M — наблюдаемая, относящаяся к системе A ; имеется измерительное устройство, с помощью которого можно измерить величину M . Обозначим через \tilde{M} соответствующую наблюдаемую для того же измерения, выполненного над составной системой AB . Сейчас мы хотим доказать, что \tilde{M} обязательно совпадает с $M \otimes I_B$. Обратите внимание, что если система AB приготовлена в состоянии $|m\rangle|\psi\rangle$, где $|m\rangle$ — собственное состояние оператора M с собственным числом m , а $|\psi\rangle$ — произвольное состояние системы B , то измерительное устройство должно с единичной вероятностью выдать после измерения результат m . Таким образом, если P_m — проектор на собственное подпространство оператора M , соответствующее собственному значению m , то соответствующий проектор для оператора \tilde{M} равен $P_m \otimes I_B$. Следовательно, имеем

$$\tilde{M} = \sum_m m P_m \otimes I_B = M \otimes I_B. \quad (2.179)$$

На следующем шаге необходимо показать, что процедура взятия частичного следа дает правильную статистику измерений при наблюдении за частью системы. Предположим, выполняется измерение над системой A , описываемое наблюдаемой M . Согласно требованию физической непротиворечивости, усредненный результат измерения не должен зависеть от способа образования смеси ρ^A в системе A . Вычисляя его с помощью матриц ρ^A и через ρ^{AB} , получим следующее равенство:

$$\text{tr}(M\rho^A) = \text{tr}(\tilde{M}\rho^{AB}) = \text{tr}((M \otimes I_B)\rho^{AB}). \quad (2.180)$$

Это уравнение, конечно, выполняется, если принять $\rho^A \equiv \text{tr}_B(\rho^{AB})$. Действительно, частичный след оказывается единственной функцией, обладающей таким свойством. Чтобы убедиться в единственности, обозначим через $f(\cdot)$ произвольное отображение множества операторов плотности системы AB во множество операторов плотности системы A , обладающее свойством для всех наблюдаемых M . Пусть M_i — ортонормированный базис в пространстве эрмитовых операторов со скалярным произведением Гильберта–Шмидта ($X, Y \equiv \text{tr}(XY)$ (сравните с упражнением 2.39)). Тогда разложение оператора $f(\rho^{AB})$ по этому базису дает

$$\text{tr}(M f(\rho^{AB})) = \text{tr}((M \otimes I_B)\rho^{AB}) \quad (2.181)$$

$$f(\rho^{AB}) = \sum_i M_i \operatorname{tr}(M_i f(\rho^{AB})) \quad (2.182)$$

$$= \sum_i M_i \operatorname{tr}((M_i \otimes I_B) \rho^{AB}). \quad (2.183)$$

Поэтому очевидно, что функция f однозначно определяется уравнением (2.180).

вычислений, в которых используются редуцированные операторы плотности. Представьте себе, что квантовая система находится в состоянии, описываемом тензорным произведением $\rho^{AB} = \rho \otimes \sigma$, где ρ и σ — операторы плотности для систем A и B соответственно. Тогда

$$\rho^A = \operatorname{tr}_B(\rho \otimes \sigma) = \rho \operatorname{tr} \sigma = \rho, \quad (2.184)$$

что и следовало ожидать в соответствии с интуитивными представлениями. Аналогично в этом состоянии $\rho^B = \sigma$. Менее тривиальным примером служит состояние Белла $(|00\rangle + |11\rangle)/\sqrt{2}$. Его оператор плотности равен

$$\rho = \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}} \right) \left(\frac{\langle 00| + \langle 11|}{\sqrt{2}} \right) \quad (2.185)$$

$$= \frac{|00\rangle\langle 00| + |11\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 11|}{2}. \quad (2.186)$$

Взяв след по второму кубиту, найдем редуцированный оператор плотности для первого кубита:

$$\rho^1 = \operatorname{tr}_2 \rho \quad (2.187)$$

$$= \frac{\operatorname{tr}_2(|00\rangle\langle 00|) + \operatorname{tr}_2(|11\rangle\langle 00|) + \operatorname{tr}_2(|00\rangle\langle 11|) + \operatorname{tr}_2(|11\rangle\langle 11|)}{2} \quad (2.188)$$

$$= \frac{|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 1|}{2} \quad (2.189)$$

$$= \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} \quad (2.190)$$

$$= \frac{I}{2}. \quad (2.191)$$

Обратите внимание, что это состояние является *смешанным*, поскольку $\operatorname{tr}((I/2)^2) = 1/2 < 1$. Это поистине замечательный результат. Состояние системы, содержащей оба кубита, является чистым, т. е. известно *точно*; тем не менее первый кубит находится в смешанном состоянии, т. е. в состоянии, о котором наши знания неполны. Это странное свойство — существование такого состояния всей системы, которое нам известно точно, при том что ее составная

часть находится в смешанном состоянии, — отличительный признак квантового запутывания.

Упражнение 2.74. Пусть система, состоящая из систем A и B , находится в состоянии $|a\rangle|b\rangle$, где $|a\rangle$ и $|b\rangle$ — чистые состояния соответственно систем A и B . Покажите, что редуцированный оператор плотности системы A соответствует чистому состоянию.

Упражнение 2.75. Найдите редуцированные операторы плотности для каждого кубита в каждом из четырех состояний Белла.

Квантовая телепортация и редуцированный оператор плотности

Полезным приложением редуцированного оператора плотности является анализ квантовой телепортации. Напомним сказанное в подразд. 1.3.7. Квантовой телепортацией называют процедуру передачи квантовой информации по классическому каналу от Алисы к Бобу при условии, что они заранее разделили между собой кубиты ЭПР-пары.

На первый взгляд кажется, что телепортацию можно использовать для передачи сообщения со скоростью, превышающей скорость света, что является главным «табу» теории относительности. В подразд. 1.3.7 мы предположили, что запрет на передачу сообщения со скоростью, большей скорости света, в данном методе возникает из-за необходимости передать Бобу результат измерения Алисы. Редуцированный оператор плотности позволяет строго обосновать эту идею.

Напомним, что непосредственно перед тем, как Алиса выполнит свое измерение, квантовое состояние трех кубитов задается следующим вектором (уравнение (1.32)):

$$\begin{aligned} |\psi_2\rangle = \frac{1}{2} [& |00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) \\ & + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)]. \end{aligned} \quad (2.192)$$

Состояние системы сразу после измерения, проведенного в вычислительном базисе Алисы, можно записать как

$$|00\rangle[\alpha|0\rangle + \beta|1\rangle] \quad \text{с вероятностью } \frac{1}{4}, \quad (2.193)$$

$$|01\rangle[\alpha|1\rangle + \beta|0\rangle] \quad \text{с вероятностью } \frac{1}{4}, \quad (2.194)$$

$$|10\rangle[\alpha|0\rangle - \beta|1\rangle] \quad \text{с вероятностью } \frac{1}{4}, \quad (2.195)$$

$$|11\rangle[\alpha|1\rangle - \beta|0\rangle] \quad \text{с вероятностью } \frac{1}{4}. \quad (2.196)$$

Таким образом, оператор плотности имеет вид

$$\begin{aligned} \rho = \frac{1}{4} [& |00\rangle\langle 00|(\alpha|0\rangle + \beta|1\rangle)(\alpha^*\langle 0| + \beta^*\langle 1|) + |01\rangle\langle 01|(\alpha|1\rangle + \beta|0\rangle)(\alpha^*\langle 1| + \beta^*\langle 0|) \\ & + |10\rangle\langle 10|(\alpha|0\rangle - \beta|1\rangle)(\alpha^*\langle 0| - \beta^*\langle 1|) + |11\rangle\langle 11|(\alpha|1\rangle - \beta|0\rangle)(\alpha^*\langle 1| - \beta^*\langle 0|)]. \end{aligned} \quad (2.197)$$

Взяв след от системы Алисы, можно видеть, что редуцированный оператор плотности системы Боба выглядит как

$$\rho^B = \frac{1}{4} [(\alpha|0\rangle + \beta|1\rangle)(\alpha^*\langle 0| + \beta^*\langle 1|) + (\alpha|1\rangle + \beta|0\rangle)(\alpha^*\langle 1| + \beta^*\langle 0|)] \\ + (\alpha|0\rangle - \beta|1\rangle)(\alpha^*\langle 0| - \beta^*\langle 1|) + (\alpha|1\rangle - \beta|0\rangle)(\alpha^*\langle 1| - \beta^*\langle 0|)] \quad (2.198)$$

$$= \frac{2(|\alpha|^2 + |\beta|^2)|0\rangle\langle 0| + 2(|\alpha|^2 + |\beta|^2)|1\rangle\langle 1|}{4} \quad (2.199)$$

$$= \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} \quad (2.200)$$

$$= \frac{I}{2}; \quad (2.201)$$

в последнем равенстве использовано условие полноты. Таким образом, состояние системы Боба *после* того, как Алиса провела свое измерение, но *до* того, как Боб узнал его результат, задается матрицей $I/2$. Это состояние не зависит от переданного при телепортации состояния $|\psi\rangle$, поэтому любое измерение, сделанное Бобом до того, как он узнает результат измерения Алисы, не будет содержать никакой информации относительно состояния $|\psi\rangle$, а это как раз и означает, что Алисе не удастся использовать телепортацию для передачи информации Бобу со скоростью, превышающей скорость света.

2.5 Разложение Шмидта и расширение до чистого состояния

Операторы плотности и операция взятия частичного следа — только первые инструменты, полезные при изучении составных квантовых систем, являющихся ключевым понятием в теории квантовых вычислений и в обработке квантовой информации. Двумя другими широко применяемыми инструментами являются *разложение Шмидта* и *расширение до чистого состояния*. В данном разделе мы введем эти понятия и попытаемся объяснить их важность.

Теорема 2.7 (разложение Шмидта). Пусть $|\psi\rangle$ — чистое состояние составной системы AB . Тогда существуют такие ортонормированные состояния $|i_A\rangle$ системы A и ортонормированные состояния $|i_B\rangle$ системы B , что

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle|i_B\rangle, \quad (2.202)$$

где λ_i — неотрицательные действительные числа, удовлетворяющие условию $\sum_i \lambda_i^2 = 1$; их называют *коэффициентами Шмидта*.

Это утверждение очень полезно. Чтобы осознать его важность, рассмотрим такое его следствие. Пусть $|\psi\rangle$ — чистое состояние составной системы AB . Тогда, согласно теореме 2.7, состояния систем A и B задаются соответственно матрицами $\rho^A = \sum_i \lambda_i^2 |i_A\rangle\langle i_A|$ и $\rho^B = \sum_i \lambda_i^2 |i_B\rangle\langle i_B|$, поэтому собственные числа матриц ρ^A и ρ^B одинаковы и равны λ_i^2 . Многие важные характеристики квантовых систем выражаются через собственные числа редуцированных операторов плотности соответствующих систем, поэтому в чистом

состоянии составной системы такие характеристики одинаковы для обеих подсистем. Например, рассмотрим состояние двух кубитов, задаваемое вектором $(|00\rangle + |01\rangle + |11\rangle)/\sqrt{3}$. Оно не обладает никакой очевидной симметрией, но если вычислить $\text{tr}((\rho^A)^2)$ и $\text{tr}((\rho^B)^2)$, то результат в обоих случаях будет равен $7/9$. Это не что иное как следствие теоремы о разложении Шмидта.

Доказательство.

Приведем доказательство для случая, когда размерности пространств состояний систем A и B равны. Общий случай предлагается доказать в упр. 2.76. Пусть $|j\rangle$ и $|k\rangle$ — фиксированные ортонормированные базисы соответственно систем A и B . Тогда вектор $|\psi\rangle$ может быть переписан в виде

$$|\psi\rangle = \sum_{j,k} a_{jk} |j\rangle |k\rangle, \quad (2.203)$$

где a — матрица с комплексными коэффициентами a_{jk} . Мы можем воспользоваться разложением по сингулярным числам: $a = u d v$, где d — диагональная матрица с неотрицательными элементами, u и v — унитарные матрицы. Таким образом, имеем

$$|\psi\rangle = \sum_{i,j,k} u_{ji} d_{ii} v_{ik} |j\rangle |k\rangle. \quad (2.204)$$

Введем обозначения $|i_A\rangle \equiv \sum_j u_{ji} |j\rangle$, $|i_B\rangle \equiv \sum_k v_{ik} |k\rangle$, $\lambda_i \equiv d_{ii}$. Тогда получим равенство

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle. \quad (2.205)$$

Легко проверить, что векторы $|i_A\rangle$ образуют ортонормированный набор (это следует из унитарности матрицы u и ортонормированности набора $|j\rangle$); аналогичное утверждение верно для $|i_B\rangle$. ■

Упражнение 2.76. Докажите теорему 2.7 о разложении Шмидта для общего случая, когда размерности пространств состояний систем A и B не совпадают.

Упражнение 2.77. Пусть ABC — квантовая система, состоящая из трех отдельных систем. Покажите (приведите пример), что существуют такие квантовые состояния $|\psi\rangle$ этой системы, которые нельзя представить в виде

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle |i_C\rangle, \quad (2.206)$$

где λ_i — действительные числа, $|i_A\rangle$, $|i_B\rangle$ и $|i_C\rangle$ — ортонормированные базисы соответствующих систем.

Базисы $|i_A\rangle$ и $|i_B\rangle$ называют *базисами Шмидта* соответственно для систем A и B , а количество ненулевых значений λ_i — *числом Шмидта* для состояния $|\psi\rangle$. Число Шмидта является важной характеристикой составной квантовой системы, определяющей в некотором количественном смысле степень запутывания между собой систем A и B . Чтобы получить представление об этой связи, рассмотрим следующее очевидное, но важное свойство: число Шмидта

сохраняется при унитарном преобразовании только системы A или только системы B . Чтобы проверить это, заметим, что если $\sum_i \lambda_i |i_A\rangle|i_B\rangle$ — разложение Шмидта для вектора $|\psi\rangle$, то $\sum_i \lambda_i (U|i_A\rangle)|i_B\rangle$ — разложение Шмидта для $U|\psi\rangle$ (U — унитарный оператор, действующий только на систему A). Такого рода свойства алгебраической инвариантности делают число Шмидта очень полезным инструментом.

Упражнение 2.78. Докажите, что состояние $|\psi\rangle$ составной системы AB может быть представлено в виде произведения состояний систем A и B тогда и только тогда, когда его число Шмидта равно 1. Докажите, что $|\psi\rangle$ можно представить в виде произведения состояний тогда и только тогда, когда ρ^A (а следовательно и ρ^B) — чистое состояние.

Второй технический прием для применения в квантовых вычислениях и обработке квантовой информации — *расширение до чистого состояния*. Предположим, задано состояние ρ^A квантовой системы A . Тогда можно ввести другую систему (обозначим ее через R) и определить чистое состояние $|AR\rangle$ для системы AR так, что $\rho^A = \text{tr}_R(|AR\rangle\langle AR|)$. Это означает, что чистое состояние $|AR\rangle$ сводится к состоянию ρ^A , когда мы рассматриваем одну систему A . Это чисто математическая процедура, называемая *расширением до чистого состояния*, которая позволяет связать чистые состояния со смешанными. Будем называть систему R *дополняющей*; это фиктивная система, не имеющая прямого физического смысла.

Чтобы доказать, что расширение до чистого состояния можно выполнить с *любым* состоянием, объясним, как построить систему R и расширение до чистого состояния $|AR\rangle$ для ρ^A . Пусть спектральное разложение для ρ^A имеет вид $\rho^A = \sum_i p_i |i^A\rangle\langle i^A|$. Чтобы расширить ρ^A до чистого состояния, введем систему R , которая имеет то же пространство состояний, что и система A , с ортонормированным базисом $|i^R\rangle$, а также определим чистое состояние для системы AR следующим образом:

$$|AR\rangle \equiv \sum_i \sqrt{p_i} |i^A\rangle |i^R\rangle. \quad (2.207)$$

Теперь вычислим редуцированный оператор плотности для системы A , соответствующий состоянию $|AR\rangle$:

$$\text{tr}_R(|AR\rangle\langle AR|) = \sum_{i,j} \sqrt{p_i p_j} |i^A\rangle \langle j^A| \text{tr}(|i^R\rangle\langle j^R|) \quad (2.208)$$

$$= \sum_{i,j} \sqrt{p_i p_j} |i^A\rangle \langle j^A| \delta_{ij} \quad (2.209)$$

$$= \sum_i p_i |i^A\rangle \langle i^A| \quad (2.210)$$

$$= \rho^A. \quad (2.211)$$

Таким образом, $|AR\rangle$ — расширение состояния ρ^A до чистого.

Отметим тесную связь разложения Шмидта с расширением до чистого состояния: расширение смешанного состояния ρ системы A до чистого состоит в

определении такого чистого состояния, в базисе Шмидта которого смешанное состояние системы A представляется диагональной матрицей; при этом коэффициенты Шмидта равны квадратному корню из собственных чисел оператора плотности ρ .

В этом разделе описаны два инструмента исследования составных квантовых систем – разложение Шмидта и расширение до чистого состояния. Они необходимы при изучении теории квантовых вычислений и обработке квантовой информации (особенно обработки квантовой информации, см. часть III книги).

Упражнение 2.79. Рассмотрим составную систему, объединяющую два кубита. Найдите разложение Шмидта для состояний

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}, \quad \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}, \quad \frac{|00\rangle + |01\rangle + |10\rangle}{\sqrt{3}}. \quad (2.212)$$

Упражнение 2.80. Пусть $|\psi\rangle$ и $|\varphi\rangle$ – два чистых состояния составной квантовой системы, содержащей системы A и B , и коэффициенты Шмидта этих состояний равны. Покажите, что существуют такие унитарные преобразования U системы A и V системы B , что $|\psi\rangle = (U \otimes V)|\varphi\rangle$.

Упражнение 2.81 (свобода в расширении до чистого состояния). Пусть $|AR_1\rangle$ и $|AR_2\rangle$ – два расширения смешанного состояния ρ^A составной системы AR до чистого состояния. Докажите, что существует такое унитарное преобразование U_R системы R , что $|AR_1\rangle = (I_A \otimes U_R)|AR_2\rangle$.

Упражнение 2.82. Пусть $\{p_i, |\psi_i\rangle\}$ – ансамбль состояний, порождающих матрицу плотности $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ для квантовой системы A . Введем систему R с ортонормированным базисом $|i\rangle$.

- Покажите, что $\sum_i \sqrt{p_i} |\psi_i\rangle |i\rangle$ – расширение ρ до чистого состояния.
- Предположим, мы производим измерение над системой L в базисе $|i\rangle$ с результатом i . С какой вероятностью мы получим этот результат и каково соответствующее состояние системы A ?
- Пусть $|AR\rangle$ – произвольное расширение ρ до чистого состояния AR . Покажите, что существует ортонормированный базис $|i\rangle$, в котором можно провести измерение над R так, что соответствующее состояние системы A после измерения будет описываться вектором $|\psi_i\rangle$ с вероятностью p_i .

2.6 Парадокс Эйнштейна–Подольского–Розена и неравенство Белла

Если человек не шокирован квантовой теорией, он ее просто не понял.

Нильс Бор

Я напомню, что во время одной прогулки Эйнштейн неожиданно остановился, повернулся ко мне и спросил, действительно ли я верю, что Луна существует только тогда, когда я смотрю на нее. Оставшаяся часть прогулки была посвящена обсуждению того, чтоб физик должен понимать под словом «существовать».

А. Пэ

...квантовые явления происходят не в гильбертовом пространстве, а в лаборатории.

Э. Перес

...доказательство невозможности свидетельствует о недостатке воображения у доказывающего.

Дж. Белл

Эта глава посвящена описанию структуры квантовой механики и ее математического аппарата, используемого в последующих главах. При этом будет постоянно повторяться принципиально важная тема необычности квантовой механики, ее *неклассических* свойств. Но в чем именно заключается различие между квантовой механикой и классическим миром? Понимание этого абсолютно необходимо при обучении таким способам обработки информации, которые невозможно выполнить в рамках классической физики. Данный раздел завершает главу обсуждением неравенства Белла — убедительного примера существенного различия между квантовой и классической физикой.

Когда мы говорим о таком объекте, как человек или книга, мы предполагаем, что физические свойства объекта существуют независимо от наблюдения. Другими словами, измерения просто *обнаруживают* эти физические свойства. Например, у теннисного мяча есть такое свойство, как *местоположение*, и обычно его измеряют с помощью света, отраженного от поверхности мяча. Во время становления квантовой механики в 20-х и 30-х гг. XX в. возникла странная точка зрения, которая заметно отличалась от классической. Как описывалось ранее в этой главе, в соответствии с принципами квантовой механики частица, над которой не производятся наблюдения, не обладает физическими характеристиками, существующими независимо от наблюдения. Эти физические характеристики возникают вследствие измерения, проведенного над системой. Например, в соответствии с принципами квантовой механики, у кубита нет определенных характеристик таких, как «проекция σ_z спина на ось z » и «проекция σ_x спина на ось x »; эти характеристики обнаруживаются в процессе проведения соответствующего измерения. Квантовая механика предлагает набор правил, которые по заданному вектору состояния определяют вероятности возможных результатов измерения, когда требуется найти значение наблюдаемой σ_z или наблюдаемой σ_x .

Вставка 2.7. Антикорреляции в эксперименте Эйнштейна–Подольского–Розена

Представьте себе, что мы приготовили состояние двух кубитов

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}, \quad (2.213)$$

по историческим причинам иногда называемое *спиновым синглетом*. Нетрудно показать, что оно является запутанным состоянием системы из двух кубитов. Предположим, мы выполнили измерение компоненты спина вдоль оси \vec{v} для обоих кубитов, т. е. измерили наблюдаемую $\vec{v} \cdot \vec{\sigma}$ (определенную в уравнении (2.116)) для каждого из кубитов, получив для каждого из них ответ +1 или −1. Оказывается, что вне зависимости от выбора направления \vec{v} результаты обоих этих измерений будут противоположными. Другими словами, если при измерении над первым кубитом получен ответ +1, то при измерении над вторым получено значение −1, и наоборот. Все выглядит так, как если бы второй кубит знал о результате измерения над первым вне зависимости от того, каким именно образом производится измерение над этим первым кубитом. Чтобы убедиться в этом, представим себе, что $|a\rangle$ и $|b\rangle$ — собственные состояния оператора $\vec{v} \cdot \vec{\sigma}$. Тогда существуют такие комплексные числа $\alpha, \beta, \gamma, \delta$, что

$$|0\rangle = \alpha|a\rangle + \beta|b\rangle, \quad (2.214)$$

$$|1\rangle = \gamma|a\rangle + \delta|b\rangle. \quad (2.215)$$

В результате подстановки получим

$$\frac{|01\rangle - |10\rangle}{\sqrt{2}} = (\alpha\delta - \beta\gamma) \frac{|ab\rangle - |ba\rangle}{\sqrt{2}}. \quad (2.216)$$

Но $\alpha\delta - \beta\gamma$ — это определитель унитарной матрицы $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$, следовательно, эта величина равна фазовому множителю $e^{i\theta}$, где θ — действительное число. Таким образом, имеем

$$\frac{|01\rangle - |10\rangle}{\sqrt{2}} = \frac{|ab\rangle - |ba\rangle}{\sqrt{2}} \quad (2.217)$$

с точностью до ненаблюдаемого общего фазового множителя. Итак, мы убедились, что если выполнено измерение величины $\vec{v} \cdot \vec{\sigma}$ для каждого из кубитов, то результат +1 (−1), полученный при измерении над первым кубитом, приводит к получению результата −1 (+1) при измерении над вторым кубитом.

Многие физики отвергли такой новый взгляд на Природу. Наиболее выдающимся противником нового подхода был Альберт Эйнштейн. В знаменитой «ЭПР-статье», написанной в соавторстве с Б. Подольским и Н. Розеном, он предложил мысленный эксперимент, показывающий, что, по его мнению, квантовая механика не является полным описанием Природы.

Суть статьи в следующем. Авторы заинтересовались тем, что они назвали «элементами действительности». Они были убеждены в том, что любой элемент действительности *должен* быть представлен в любой полной физической теории. Дискуссия была организована для того, чтобы показать, что квантовая механика не является полной физической теорией — для этого авторы хотели указать на элементы действительности, не включенные в квантовую механику.

Они собирались ввести *достаточное условие* того, что физическая характеристика есть элемент действительности. Условие, по мнению авторов, должно быть следующим: непосредственно перед измерением можно с достоверностью предсказать, какое значение физической характеристики будет получено в результате этого измерения.

Рассмотрим в качестве примера запутанное состояние двух кубитов, первый из которых принадлежит Алисе, а второй — Бобу:

$$\frac{|01\rangle - |10\rangle}{\sqrt{2}}. \quad (2.218)$$

Предположим, что Алиса и Боб находятся на большом расстоянии друг от друга. Алиса определяет величину проекции спина на ось \vec{v} , т. е. измеряет наблюдаемую $\vec{v} \cdot \vec{\sigma}$ (определенную в уравнении (2.116)). Пусть Алиса получила результат +1. Тогда простое вычисление, приведенное во вставке 2.7, показывает, что она может с достоверностью предсказать, что Боб будет иметь в результате своего измерения −1, если он также будет определять величину проекции спина на ось \vec{v} . Аналогично, если Алиса получит результат −1, она может с достоверностью предсказать, что у Боба результат будет равен +1. Поскольку Алиса в любом случае может предсказать результат, получаемый Бобом при измерении проекции его спина на ось \vec{v} , эта физическая характеристика должна соответствовать некоторому элементу действительности (согласно ЭПР-критерию), а следовательно, должна быть отражена в любой полной физической теории. Однако обычная квантовая механика, как мы ее описали, просто сообщает, как вычислить вероятности различных результатов измерения величины $\vec{v} \cdot \vec{\sigma}$. Она не содержит никаких фундаментальных элементов «сущностей», соответствующих величине $\vec{v} \cdot \vec{\sigma}$ самой по себе.

Эйнштейн, Подольский и Розен хотели показать, что квантовая механика неполна. Для этого они намеревались продемонстрировать, что в квантовой механике не хватает некоторых существенных «элементов действительности» (согласно введенному ими критерию). Они надеялись заставить мир вернуться к классическому взгляду на законы природы, в соответствии с которыми системам можно приписать свойства, существующие независимо от выполняемых над этими системами измерений. К огорчению Эйнштейна и его соавторов, большинство физиков не признало эти доводы убедительными. Пытаться

указывать Природе на правила, которым она должна подчиняться, — крайне эксцентричный способ изучения ее законов.

Действительно, в споре о парадоксе Эйнштейна–Подольского–Розена последнее слово осталось за Природой. Примерно через 30 лет после публикации упомянутой статьи был поставлен эксперимент, целью которого была проверка, правильную ли картину мира предлагали Эйнштейн с соавторами. Оказалось, что Природа экспериментально опровергла их точку зрения, подтвердив справедливость традиционных квантовомеханических законов.

Главным моментом в этом экспериментальном опровержении явился результат, известный под названием *неравенства Белла*. Это неравенство — утверждение, *не* относящееся непосредственно к квантовой механике, поэтому сейчас мы должны на некоторое время забыть все наши познания из указанной области. Чтобы получить неравенство Белла, проведем мысленный эксперимент и проанализируем его с помощью обычных представлений об устройстве мира — представлений такого типа, которым, по мнению Эйнштейна и его соавторов, должна подчиняться Природа. После того как мы выполним этот анализ с помощью обычных представлений, проведем также анализ с позиции квантовой механики, который, как мы сможем показать, *не согласуется с анализом на основе обычных представлений*. После этого можно поставить реальный эксперимент, в котором Природа сама “даст ответ” относительно того, какой из двух подходов является правильным.

Представьте себе, что мы проводим эксперимент, описанный на рис. 2.4. Чарли готовит исходное состояние двух частиц. Неважно, каким именно окажется состояние, для нас существенно лишь то, что он может сколько угодно раз повторять используемую процедуру. После приготовления исходного состояния он отправляет первую частицу Алисе, а вторую — Бобу.

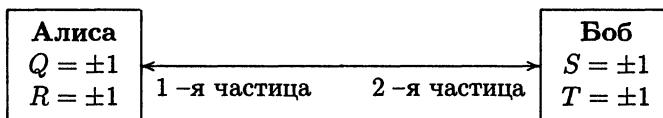


Рис. 2.4. Схема экспериментальной установки, иллюстрирующей неравенство Белла. Алиса может измерить либо характеристику Q , либо характеристику R , Боб может измерить либо S , либо T . Они выполняют свои измерения одновременно. Предполагается, что Алиса и Боб находятся на большом расстоянии друг от друга, т. е. измерение, производимое над одной из частиц, не влияет на результат измерения над другой.

Когда Алиса получит свою частицу, она должна выполнить измерение. Предположим, в ее распоряжении имеются два разных прибора, т. е. она может выбрать, какое из двух доступных измерений ей провести. Пусть это будут измерения физических величин P_Q и P_R . Алиса не знает заранее, какое из двух измерений она будет выполнять. Она просто подбрасывает монету после получения своей частицы или с помощью какого-либо датчика случайных чисел выбирает, какое из двух измерений выполнить. Будем считать для простоты, что каждое из двух измерений имеет только два возможных исхода: +1 и −1. Предположим, Алиса в результате измерения величины P_Q для своей частицы

получила значение Q . Тогда предполагается, что Q — объективная характеристика частицы, находящейся у Алисы, которая была просто обнаружена в результате измерения (вспомните пример про определение положения теннисного мяча посредством изучения отраженного от него света). Аналогичным образом, пусть R обозначает величину, обнаруженную в процессе измерения характеристики P_R .

Предположим, что Боб находится в аналогичной ситуации, т. е. может измерять одну из двух характеристик (P_S или P_T), определяя объективно существующее значение величины S или T , соответственно, причем каждая из них также может принимать значение либо $+1$, либо -1 . Боб также не решает заранее, какое именно из измерений он будет производить — только после получения своей частицы он делает случайный выбор между S и T . Временные рамки эксперимента подобраны таким образом, что Алиса и Боб выполняют измерения в одно и то же время (или, говоря на более точном языке теории относительности, события, соответствующие этим измерениям, являются абсолютно удаленными). Таким образом, проводимое Алисой измерение не может повлиять на результат измерения Боба (и наоборот), поскольку физическое воздействие не может распространяться со скоростью, превышающей скорость света.

Теперь проведем простые алгебраические преобразования выражения $QS + RS + RT - QT$:

$$QS + RS + RT - QT = (Q + R)S + (R - Q)T. \quad (2.219)$$

Поскольку $R, Q = \pm 1$, получим, что либо $(Q + R)S = 0$, либо $(R - Q)T = 0$. В обоих случаях из уравнения (2.219) следует: $QR + RS + RT - QT = \pm 2$. Обозначим через $p(q, r, s, t)$ вероятность того, что перед измерением система находится в таком состоянии, где $Q = q$, $R = r$, $S = s$, $T = t$. Эти вероятности могут зависеть от того, как именно Чарли готовит исходное состояние, а также от экспериментального шума. Обозначим через $E(\cdot)$ математическое ожидание, тогда имеем

$$E(QS + RS + RT - QT) = \sum_{q,r,s,t} p(q, r, s, t)(qs + rs + rt - qt) \quad (2.220)$$

$$\leq \sum_{q,r,s,t} p(q, r, s, t) \times 2 \quad (2.221)$$

$$= 2. \quad (2.222)$$

Кроме того, получим следующее соотношение:

$$\begin{aligned} E(QS + RS + RT - QT) &= \sum_{q,r,s,t} p(q, r, s, t)qs + \sum_{q,r,s,t} p(q, r, s, t)rs + \\ &\quad + \sum_{q,r,s,t} p(q, r, s, t)rt - \sum_{q,r,s,t} p(q, r, s, t)qt \end{aligned} \quad (2.223)$$

$$= E(QS) + E(RS) + E(RT) - E(QT). \quad (2.224)$$

Сравнив равенства (2.222) и (2.224), можно записать неравенство Белла:

$$\mathbf{E}(QS) + \mathbf{E}(RS) + \mathbf{E}(RT) - \mathbf{E}(QT) \leq 2. \quad (2.225)$$

Этот результат часто называют *CHSH-неравенством* (аббревиатура образована от имен его первооткрывателей – Clauser, Horne, Shimony, Holt). Оно является частью большего набора неравенств, собирательно называемых неравенствами Белла, поскольку авторство первого из них принадлежит Беллу.

Многократно повторяя эксперимент, Алиса и Боб могут определить каждую из величин, находящихся в левой части неравенства Белла. Например, после выполнения серии экспериментов Алиса и Боб встречаются и исследуют полученные данные. Они берут результаты экспериментов, в которых Алиса определяла P_Q , а Боб — P_S . Перемножив результаты своих экспериментов, они получат экспериментальные значения величины QS . Усреднив полученные величины, можно вычислить $\mathbf{E}(QS)$ с точностью, ограничивающей только числом проведенных измерений. Аналогичным образом можно определить остальные величины, входящие в левую часть неравенства Белла, что позволит проверить, выполняется ли оно на практике.

Теперь настало время провести рассуждение с использованием аппарата квантовой механики. Представьте себе, что мы выполняем следующий квантовомеханический эксперимент. Чарли приготавливает квантовомеханическую систему в начальном состоянии

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \quad (2.226)$$

После этого он передает первый кубит Алисе, а второй — Бобу. Те выполняют измерения следующих наблюдаемых:

$$Q = Z_1, \quad S = \frac{-Z_2 - X_2}{\sqrt{2}}, \quad (2.227)$$

$$R = X_1, \quad T = \frac{Z_2 - X_2}{\sqrt{2}}. \quad (2.228)$$

Простые вычисления показывают, что средние значения этих наблюдаемых, записанные с применением квантовомеханических обозначений $\langle \cdot \rangle$, имеют вид

$$\langle QS \rangle = \frac{1}{\sqrt{2}}, \quad \langle RS \rangle = \frac{1}{\sqrt{2}}, \quad \langle RT \rangle = \frac{1}{\sqrt{2}}, \quad \langle QT \rangle = -\frac{1}{\sqrt{2}}. \quad (2.229)$$

Таким образом, получим

$$\langle QS \rangle + \langle RS \rangle + \langle RT \rangle - \langle QT \rangle = 2\sqrt{2}. \quad (2.230)$$

Нам уже известно (см. уравнение (2.225)), что сумма средних значений величин QS , RS и RT , из которой вычтено среднее значение величины QT , не может превышать 2. А согласно квантовомеханическому расчету эта комбинация средних должна давать $2\sqrt{2}$.

Обратимся за разрешением этого парадокса к Природе. Были поставлены изящные эксперименты с использованием фотонов (т. е. частиц света) для проверки того, будет ли верным неравенство Белла (формула (2.225)), полученное в соответствии с обычными представлениями, или квантовомеханическое предсказание (уравнение (2.230)). Детали эксперимента выходят за рамки нашей книги, однако отметим, что результаты эксперимента оказались в пользу квантовомеханического прогноза. Природа не подчиняется неравенству Белла (2.225).

Что это означает? Можно заключить, что одно или несколько предположений, использованных при выводе неравенства Белла, неверно. Было написано большое количество трудов, в которых исследовались разные формы этого рассуждения и изучались слегка измененные предположения, которые позволяли получить аналоги неравенства Белла. Приведем здесь основные моменты этих рассмотрений.

При выводе формулы (2.225) было сделано два предположения, которые можно подвергнуть сомнению:

1. о том, что у физических характеристик P_Q , P_R , P_S и P_T имеются определенные значения Q , R , S и T , которые существуют независимо от наблюдения. Его иногда называют предположением *реализма*.
2. о том, что выполнение измерения Алисой не влияет на результат измерения, производимого Бобом. Его иногда называют предположением *локальности*.

Приведенные два пункта вместе называют предположениями *локального реализма*. Безусловно, это интуитивно правдоподобные предположения относительно устройства мира, и они соответствуют нашему повседневному опыту. Тем не менее неравенство Белла показывает, что по крайней мере одно из них неверно.

Что можно узнать из неравенства Белла? Для физиков наиболее важным уроком является то, что их основанная на здравом смысле интуиция о принципах устройства мира оказывается неверной. Мир не является локально реалистичным. Большинство физиков считают, что при правильном квантовомеханическом подходе должно быть опущено именно предположение о реализме, в то время как другие, напротив, полагают, что следует отказаться от представления о локальности. Как бы то ни было, неравенство Белла и надежные экспериментальные проверки приводят к заключению, что либо реализм, либо локальность, либо их обоих следует исключить из картины мира, чтобы получить хорошее интуитивное понимание квантовой механики.

Какие уроки можно извлечь из неравенства Белла для квантовых вычислений и обработки квантовой информации? Исторически наиболее полезным уроком, наверное, был самый труднообъяснимый: в запутанных состояниях, например, в ЭПР-парах, есть нечто принципиально важное. Многие достижения в области квантовых вычислений, тем более в теории квантовой информации, выросли из вопроса: «Что дает запутывание для данной задачи?» Как мы

поняли из рассмотрения телепортации и сверхплотного кодирования (и как мы будем узнавать неоднократно на протяжении остальной части книги), вводя в задачу запутывание, мы добавляем новые возможности, немыслимые в рамках классической теории информации. С более общей точки зрения, неравенство Белла показывает, что запутывание — принципиально новый ресурс, который существенно *выходит за* классические рамки. (Образно говоря, классические взгляды можно сравнить с бронзовым веком, а запутывание — с появлением железа.) Главная задача квантовых вычислений и обработки квантовой информации состоит в использовании этого нового ресурса для решения задач, неразрешимых или труднорешаемых с помощью только классических средств.

Задача 2.1 (функции от матриц Паули). Обозначьте через $f(\cdot)$ функцию, отображающую множество комплексных чисел в себя. Пусть \vec{n} — нормированный вектор в трехмерном пространстве, θ — произвольное действительное число. Покажите, что

$$f(\theta \vec{n} \cdot \vec{\sigma}) = \frac{f(\theta) + f(-\theta)}{2} I + \frac{f(\theta) - f(-\theta)}{2} \vec{n} \cdot \vec{\sigma}. \quad (2.231)$$

Задача 2.2 (свойства числа Шмидта). Пусть $|\psi\rangle$ — чистое состояние составной системы, содержащей системы A и B .

1. Докажите, что число Шмидта вектора $|\psi\rangle$ равно рангу редуцированной матрицы плотности $\rho_A \equiv \text{tr}_B(|\psi\rangle\langle\psi|)$. (Обратите внимание, что ранг эрмитова оператора равен размерности его носителя.)
2. Пусть $|\psi\rangle = \sum_j |\alpha_j\rangle |\beta_j\rangle$ — представление вектора $|\psi\rangle$, где $|\alpha_j\rangle$ и $|\beta_j\rangle$ — соответственно состояния систем A и B (вообще говоря, не обязательно нормированные). Докажите, что число членов в таком разложении не меньше $\text{Sch}(\psi)$ — числа Шмидта вектора $|\psi\rangle$.
3. Пусть $|\psi\rangle = \alpha|\varphi\rangle + \beta|\gamma\rangle$. Докажите, что

$$\text{Sch}(\psi) \geq |\text{Sch}(\varphi) - \text{Sch}(\gamma)|. \quad (2.232)$$

Задача 2.3 (неравенство Цирельсона). Пусть $Q = \vec{q} \cdot \vec{\sigma}$, $R = \vec{r} \cdot \vec{\sigma}$, $S = \vec{s} \cdot \vec{\sigma}$, $T = \vec{t} \cdot \vec{\sigma}$, где \vec{q} , \vec{r} , \vec{s} и \vec{t} — единичные векторы в действительном трехмерном пространстве. Покажите, что

$$(Q \otimes S + R \otimes S + R \otimes T - Q \otimes T)^2 = 4I + [Q, R] \otimes [S, T]. \quad (2.233)$$

Используя этот факт, докажите, что

$$\langle Q \otimes S \rangle + \langle R \otimes S \rangle + \langle R \otimes T \rangle - \langle Q \otimes T \rangle \leq 2\sqrt{2}, \quad (2.234)$$

т. е. отклонение от неравенства Белла, полученное в уравнении (2.230), является максимально возможным в рамках квантовой механики.

История и дополнительная литература

Существует огромное количество книг по линейной алгебре самого разного уровня сложности. Нам больше всего нравится двухтомник Хорна и Джонсона [183, 184], который охватывает большое количество тем, изложенных в доступном для понимания стиле. Другими полезными справочными пособиями являются книги Маркуса и Минка [288], а также Бхатиа [53]. Также хорошие введение в линейную алгебру содержатся в книгах Халмоса [175], Перлиса [317] и Стренга [376].²

Издано много отличных учебников по квантовой механике. К сожалению, в большей части из них описываются вопросы, имеющие слабое отношение к квантовым вычислениям и обработке квантовой информации. Наиболее подходящей является прекрасная книга Переса [319]. Помимо исключительно ясного изложения элементарной квантовой механики автор подробно останавливается на неравенстве Белла и связанных с ним фактах. Среди хороших учебников вводного уровня следует отметить книгу Сакурая [346], третий том замечательного курса лекций Фейнмана, Лейтона и Сэндса [151], а также двухтомник Коэна-Таннуджи, Диу и Лалоэ [107, 108]. Все три упомянутых учебника несколько ближе к теме квантовых вычислений и обработки квантовой информации, чем остальные пособия по квантовой механике, хотя и в них содержится много материала, не имеющего отношения к теме нашей книги. Поэтому если вы хотите ознакомиться с квантовыми вычислениями и обработкой квантовой информации, нет необходимости читать какой-либо из этих трех учебников полностью. Тем не менее каждая из трех указанных книг может оказаться полезной в качестве справочника, особенно при чтении физических статей. Ссылки на историю квантовой механики содержатся в конце гл. 1.³

Во многих текстах по квантовой механике используются только проективные измерения. Для применения к квантовым вычислениям и обработке квантовой информации более удобно (и, как мы полагаем, более просто для начинающих) начинать с общего описания измерений, в котором проективные измерения рассматриваются как частный случай. Естественно, как было показано выше, в конечном счете оба этих подхода оказываются эквивалентными. Теория измерений общего вида, которую мы использовали, была разработана между 40-ми и 70-ми гг. XX в. Значительная часть исторических вопросов содержится в книге Краусса [229]. Интересное обсуждение, связанное с квантовыми измерениями, имеется в разд. 2.2 книги Гардинера [159], а также у Брагинского и Хахили [55]. В разд. 2.2.6 работы Переса [318] описываются POVM-

² Из имеющихся на русском языке учебников можно порекомендовать следующие Кострикин А.И., Манин Ю И Линейная алгебра и геометрия М Изд-во МГУ, 1980; Гельфанд И.М. Лекции по линейной алгебре М-Л Государственное издательство технико-теоретической литературы, 1952. — Прим. перев.

³ Из книг по квантовой механике на русском языке советуем обратить внимание на такие, как Ландау Л Д. и Лифшиц Е М Теоретическая физика том III. (Квантовая механика: нерелятивистская теория) М . Физматлит, 2001; Галицкий В М , Корнаков Б.М., Коган В.И Задачи по квантовой механике. М Наука, 1981; Фейнман Р , Лейтон Р , Сэндс М Фейнмановские лекции по физике. Вып 8 Квантовая механика (I) 1966 Вып 9 Квантовая механика (II) 1967. М.: Мир — Прим. перев

измерения для различия неортогональных состояний. Дальнейшее развитие этого направления, описанное в упражнении 2.64, восходит к книге Дуана и Гуо [119].

Сверхплотное кодирование было разработано Беннеттом и Визнером [76]. Эксперимент, по реализации сверхплотного кодирования с помощью запутанных фононных пар выполнили Меттл, Вайнфуртер, Квят и Цайлингер [299].

Формализм операторов плотности был введен независимо Ландау [233] и фон Нейманом [403]. На унитарную свободу в представлении матриц плотности (см. теорему 2.6) впервые указал Шредингер [349], позже она была открыта независимо Джейнсом [199], а также Хьюстоном, Йожа и Буттерсом [186]. Результаты упр. 2.73 взяты из статьи Джейнса, а упр. 2.81 и 2.82 — из работы Хьюстона, Йожа и Буттерса. Класс распределений вероятностей, которые могут появляться в разложении матриц плотности для заданной матрицы, исследовался Ульманом [390] и Нильсеном [305]. Знаменитое разложение Шмидта появилось в работе [348]. Результат упражнения 2.77 получен Пересом [320].

ЭПР-эксперимент придуман Эйнштейном, Подольским и Розеном [143], а его видоизмененная форма, в которой он описывается в нашем учебнике, восходит к Бому [64]. Иногда его ошибочно называют «парадоксом Эйнштейна–Подольского–Розена». Неравенство Белла названо в честь Белла [43], впервые получившего неравенство аналогичного типа. В том виде, в котором оно приведено в нашем учебнике, это неравенство выведено Клаузером, Хорне, Шимони и Хольтом [86] (поэтому его часто называют CHSH-неравенством). Последнее неравенство было независимо получено Беллом, который не опубликовал свой результат.

Часть 3 задачи 2.2 восходит к Таплиялу (частное сообщение). Неравенство Цирельсона появилось в работе [387].

Глава 3

ВВЕДЕНИЕ В ИНФОРМАТИКУ

Когда мы занимаемся естественными науками, то имеем дело с миром, который нам дала Природа, и нам остается только открыть его законы. Когда мы имеем дело с компьютером, то можем внести в него свои законы и создать свой мир.

Алан Кей

Наша наука все еще находится в эмбриональной стадии. Это прекрасно, что у нас нет двухтысячелетней истории. Мы все еще на том этапе, когда очень и очень важные результаты появляются прямо у нас на глазах.

Майкл Рабин об информатике

Ключевое понятие информатики — *алгоритм*. Алгоритм — это точный рецепт выполнения какой-либо задачи (пример: алгоритм сложения чисел в столбик, который мы все изучаем в детстве). В этой главе мы даем набросок части современной теории алгоритмов, развившейся в связи с компьютерами. Нашей основной моделью для алгоритмов будет *машина Тьюринга*. Это — идеализированное вычислительное устройство, похожее на современный персональный компьютер, но с более простой системой команд и неограниченной памятью. То, что машины Тьюринга на первый взгляд очень просты, не должно вводить в заблуждение: это очень мощные устройства. Мы увидим, что с их помощью можно выполнять любые алгоритмы, даже такие, которые выполняются на гораздо более мощных компьютерах.

Основной вопрос, в котором мы постараемся разобраться при изучении алгоритмов, состоит в выяснении того, какие ресурсы нужны для решения задачи. Этот вопрос естественно распадается на две части. Во-первых, хотелось бы выяснить, какие вычислительные задачи разрешимы, лучше всего предъявляя конкретные алгоритмы для решения задач. Например, есть много хороших алгоритмов для быстрой сортировки последовательности чисел в возрастающем порядке. Второй аспект этого вопроса — указать *ограничения* на возможности алгоритмов решения задач. Например, можно найти нижние границы для числа операций, которые неизбежно выполнит любой алгоритм сортировки. В идеале ответы на эти два вопроса — как найти алгоритм для решения данной задачи и каковы ограничения на возможности любого такого алгоритма — полностью согласуются (т. е. мы знаем оптимальный алгоритм). На практике

тике часто остается немалый разрыв между возможностями лучших известных алгоритмов и самыми сильными ограничениями. Цель этой главы — дать обзор средств, разработанных для анализа вычислительных задач, а также для построения и анализа алгоритмов для решения этих задач.

Но почему же читатель, интересующийся *квантовыми* вычислениями и *квантовой* теорией информации, должен тратить время на изучение *классической* информатики? На это есть три веские причины. Во-первых, большое количество понятий и технических приемов классической информатики можно с большой пользой использовать в квантовых вычислениях и квантовой информатике. Многие замечательные результаты в области квантовых вычислений и квантовой информации получены в результате объединения старых идей из информатики с новыми идеями из квантовой механики. Например, некоторые быстрые алгоритмы для квантовых компьютеров основаны на преобразовании Фурье — мощном инструменте, используемом во многих классических алгоритмах. Как только было понято, что квантовые компьютеры могут осуществлять некоторую разновидность преобразования Фурье гораздо быстрее, чем классические, это дало возможность разработать много важных квантовых алгоритмов.

Во-вторых, специалисты по информатике затратили большие усилия на выяснение того, какие ресурсы необходимы для решения той или иной задачи на классическом компьютере. Эти результаты можно использовать в качестве основы для сравнения с квантовыми вычислениями и квантовой теорией информации. Например, много внимания уделялось задаче нахождения простых множителей данного числа. Считается, что эта задача не имеет «эффективного» решения на классическом компьютере (что здесь понимается под «эффективностью», будет разъяснено далее в этой главе). Однако же существует эффективное решение этой задачи на квантовом компьютере. Для задачи нахождения простых множителей существует *разрыв* между возможностями квантового и классического компьютеров. Это интересно и само по себе и в том более широком смысле, что такой разрыв может существовать и для более широкого класса задач, чем нахождение простых множителей. Возможно, в процессе дальнейшего изучения этой конкретной задачи удастся выделить ее черты, благодаря которым на квантовом компьютере решить ее оказывается легче, чем на классическом, а затем воспользоваться этими знаниями для нахождения интересных квантовых алгоритмов, пригодных для решения других задач.

В-третьих, что более важно, необходимо научиться *думать, подобно специалисту по информатике*. Мысление специалистов по информатике совсем не такое, как у физиков или специалистов других естественных наук. Тот, кто хочет глубоко понять квантовые вычисления и квантовую теорию информации, должен время от времени мыслить как специалист по информатике; нужно научиться интуитивно понимать, какая техника и, что самое важное, какие задачи наиболее интересны специалисту по информатике.

Эта глава построена следующим образом. В разд. 3.1 мы вводим две модели вычислений: машину Тьюринга и схемную модель. Нашей базовой вычис-

литературой моделью будет машина Тьюринга, но мы будем чаще использовать схемную модель, поскольку именно эта модель наиболее полезна при изучении квантовых вычислений. Познакомившись с этими двумя моделями, мы посвятим остальную часть главы обсуждению объема ресурсов, необходимого для вычислений. Раздел 3.2 начинается с обзора задач, которыми мы интересуемся, и рассмотрения некоторых связанных с ними вопросов о ресурсах. Далее в этом разделе приводятся ключевые понятия, связанные со *сложностью вычислений*, — раздела математики, в котором рассматриваются требования к времени и памяти, необходимые для решения данной задачи, и дается классификация задач по трудности их решения. Завершается этот раздел рассмотрением энергетических ресурсов, необходимых для вычислений. Как ни странно, оказывается, что энергия, требуемая для вычисления, может быть исчезающей малой, если только вычисление можно сделать обратимым. Мы объясняем, как сконструировать обратимые компьютеры, а также почему они важны как для классической, так и для квантовой теории вычислений. В завершающем главу разд. 3.3 дается обзор теоретической информатики, причем особое внимание уделяется вопросам, играющим роль в области квантовых вычислений и квантовой информации.

3.1 Вычислительные модели

... алгоритмы существуют независимо от какого бы то ни было языка программирования.

Дональд Кнут

Что это значит, что для выполнения некоторой задачи имеется *алгоритм*? В детстве мы все изучаем способ, позволяющий сложить два сколь угодно больших числа. Это — пример алгоритма. Нахождение точного математического определения для понятия алгоритма и является целью этого раздела.

Истоки понятия алгоритма уходят на много веков в историю; младшекурсники изучают алгоритм Евклида для нахождения наибольшего общего делителя двух натуральных чисел, и этому алгоритму две тысячи лет. Однако основные понятия современной теории алгоритмов (и тем самым информатики) были сформулированы только в 30-х г. XX века Алонзо Чёрчем, Алланом Тьюрингом и другими пионерами компьютерной эры. Их работы появились как ответ на глубокий вопрос, поставленный великим математиком Давидом Гильбертом в начале XX века. Гильберт задался вопросом, существует ли алгоритм, способный (в принципе) решить все математические задачи, и ожидал, что ответ на этот вопрос (известный как *Entscheidungsproblem*) будет положительным.

Удивительным образом оказалось, что на вопрос Гильберта надо ответить «нет»: не существует алгоритма, способного решить все математические задачи. Чтобы доказать это, Чёрчу и Тьюрингу потребовалось решить глубокую проблему: как дать математическое определение алгоритма, соглашающееся с его интуитивным пониманием. В процессе этой работы они заложили основы современной теории алгоритмов, а тем самым и современной информатики.

В этой главе мы пользуемся двумя на первый взгляд различными подходами к теории вычислений. Первый подход был предложен Тьюрингом. Для уточнения понятия алгоритма Тьюринг определил класс машин, известных в настоящее время машин, как *машины Тьюринга*. В подразд. 3.1.1 мы описываем машины Тьюринга, а затем обсуждаем некоторые более простые варианты модели вычислений, основанной на машине Тьюринга. Второй подход основан на *схемной модели вычислений*; этот подход особенно полезен как подготовка к дальнейшему исследованию квантовых компьютеров. Схемная модель обсуждается в подразд. 3.1.2. Хотя при поверхностном рассмотрении эти две модели вычислений представляются различными, оказывается, что они эквивалентны. Можно спросить, зачем вводить несколько разных вычислительных моделей. Причина в том, что различные модели могут помочь по-разному понять одну и ту же задачу. Два (или более) способа рассмотрения лучше, чем один.

3.1.1 Машины Тьюринга

Основные составные части машины Тьюринга изображены на рис. 3.1. Машина Тьюринга состоит из: (а) *программы* (примерно как у обычного компьютера); (б) *управляющего устройства с конечным числом состояний*, которое работает как примитивный микропроцессор, координируя действия машины; (в) *ленты*, аналогичной памяти компьютера, и (г) *читающей/пишущей головки*, указывающей на то место ленты, где в данный момент можно что-то прочитать или записать. Опишем теперь каждую из этих частей более подробно.

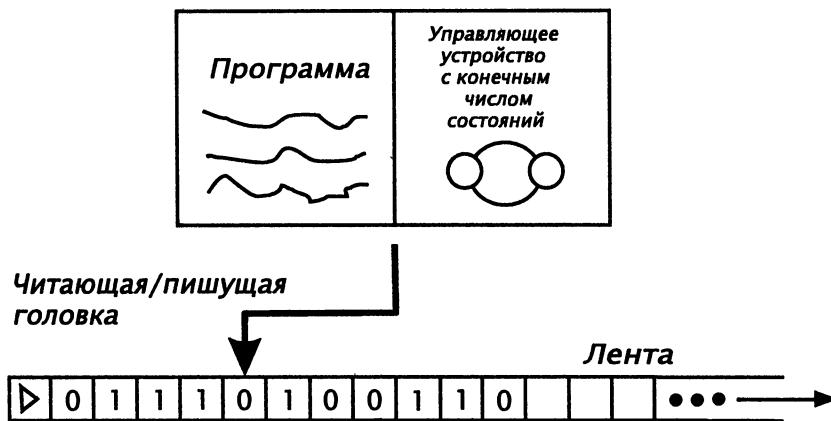


Рис. 3.1. Основные составные части машины Тьюринга В тексте пробелы обозначаются буквой *b*. Обратите внимание на знак $>$ обозначающий начало ленты

Управляющее устройство с конечным числом состояний для машины Тьюринга имеет конечное число внутренних состояний q_1, \dots, q_t . Число t можно варьировать; оказывается, что для достаточно больших t производительность машины от него по существу не зависит, так что без потери общности можно считать, что t — это некоторая фиксированная константа. Управляющее

устройство лучше всего рассматривать как разновидность микропроцессора, координирующего действия машины Тьюринга. Это устройство содержит временное хранилище данных вне ленты и является тем местом, где производятся вычисления. Наряду с состояниями q_1, \dots, q_m имеются два состояния q_s и q_h , называемые *начальным* (starting) и *заключительным* (halting) состояниями соответственно. В начале вычислений машина Тьюринга находится в начальном состоянии q_s . В процессе вычислений состояние меняется и в случае, если вычисления завершаются, машина Тьюринга оказывается в состоянии q_h . Это означает, что машина закончила работу.

Лента машины Тьюринга является одномерным объектом, простирающимся до бесконечности в одном направлении. Она представляет собой бесконечную последовательность ячеек, пронумерованных числами $0, 1, 2, 3, \dots$. Каждая ячейка содержит один символ из некоторого алфавита Γ , состоящего из конечного числа различных символов. Пока что удобно предположить, что алфавит состоит из четырех символов $0, 1, b$ (пробел) и \triangleright (символ начала ленты). Перед началом работы лента содержит \triangleright в левом конце и конечное число символов 0 и 1 , а все остальные ячейки заполнены пробелами. Читающая/пишущая головка указывает на ту ячейку ленты, которая в данный момент доступна машине Тьюринга.

Итак, машина Тьюринга начинает работу, когда ее управляющее устройство находится в состоянии q_s , а головка указывает на самую левую ячейку — ячейку номер 0 . Затем вычисления проходят шаг за шагом в соответствие с *программой*, как это будет объяснено ниже. Если текущее состояние есть q_h , то вычисления завершаются, и *результатом* вычислений — это содержимое ленты.

Программа машины Тьюринга представляет собой конечный упорядоченный список *программных строк* (program lines) вида $\langle q, x, q', x', s \rangle$. Первый элемент программной строки q — это одно из внутренних состояний машины. Второй элемент x принадлежит алфавиту Γ — множеству символов, которые могут появиться на ленте. Машина работает следующим образом. На каждом шаге машина Тьюринга последовательно просматривает список программных строк и ищет в нем строку, начинающуюся с $\langle q, x, q', x', s \rangle$, где q — текущее состояние машины, а x — символ на ленте, находящийся под головкой. Если такая программная строка не находится, внутреннее состояние машины переходит в q_h и машина останавливается. Если строка находится, то она *исполняется*. Исполнение программной строки заключается в следующем: внутреннее состояние машины переходит в q' ; на место символа x на ленту записывается символ x' ; головка смещается влево, вправо или остается на месте в зависимости от того, равно s минус единице, единице или нулю соответственно. Единственное исключение из этого правила возникает в случае, когда головка указывает на самую левую ячейку и при этом $s = -1$; в этом случае головка остается на месте.

Теперь, когда мы знаем, что такое машина Тьюринга, посмотрим, как с ее помощью можно вычислить какую-либо простую функцию. Рассмотрим следующий пример. В начале работы машины на ленте записано двоичное число x (а

за ним — пробелы). Кроме начального состояния q_s и заключительного состояния q_h машина имеет три внутренних состояния q_1 , q_2 и q_3 . Программа состоит из следующих строк (номера слева приведены только для удобства ссылок и не являются составной частью программы):

1 :	$\langle q_s, \triangleright, q_1, \triangleright, +1 \rangle$
2 :	$\langle q_1, 0, q_1, b, +1 \rangle$
3 :	$\langle q_1, 1, q_1, b, +1 \rangle$
4 :	$\langle q_1, b, q_2, b, -1 \rangle$
5 :	$\langle q_2, b, q_2, b, -1 \rangle$
6 :	$\langle q_2, \triangleright, q_3, \triangleright, +1 \rangle$
7 :	$\langle q_3, b, q_h, 1, 0 \rangle$

Какую функцию вычисляет эта программа? Вначале машина находится в состоянии q_s и в крайней левой ячейке, так что выполняется строка номер 1, т. е. $\langle q_s, \triangleright, q_1, \triangleright, +1 \rangle$, в результате чего головка сдвигается вправо, содержимое ленты не меняется, а внутреннее состояние меняется на q_1 . Программные строки 2, 3, 4 обеспечивают следующее поведение машины: если машина находится в состоянии q_1 , то головка сдвигается вправо, когда она видит 0 (строка 2) или 1 (строка 3), при этом содержимое ленты заменяется на пробелы, пока головка не дойдет до ячейки, в которой уже стоит пробел; в этот момент головка сдвигается на один шаг влево, а внутреннее состояние меняется на q_2 (строка 4). Теперь выполнение строки 5 приводит к тому, что головка сдвигается влево, а содержимое ленты не меняется, пока под головкой находится пробел. Так продолжается пока головка не дойдет до исходного положения; в этот момент машина читает символ \triangleright , внутреннее состояние меняется на q_3 , и головка сдвигается на один шаг вправо (строка 6). Страна 7 завершает программу: машина просто печатает на ленте число 1 и останавливается.

Наш анализ показывает, что эта программа вычисляет постоянную функцию $f(x) = 1$. Другими словами, независимо от того, какое число перед началом работы было записано на ленте, на выходе оказывается записанным число 1. Вообще машину Тьюринга можно рассматривать как устройство, вычисляющее функции из множества целых неотрицательных чисел в множество целых неотрицательных чисел; исходное состояние ленты является записью аргумента функции, а конечное — записью значения функции на этом аргументе.

Кажется, что мы всего лишь вычислили простую функцию очень сложным способом. Можно ли с помощью машины Тьюринга вычислять более сложные функции? Возможно ли, например, сконструировать машину, которая по заданным числам x и y , записанным на ленте через пробел, вычисляет (записывает на ленте) их сумму? И вообще, какой класс функций можно вычислить с помощью машины Тьюринга?

Оказывается, что модель вычислений, основанная на машине Тьюринга, может быть использована для вычисления очень многих функций. Например, с ее помощью можно выполнять все основные арифметические операции, проводить поиск в тексте, представленном как последовательность битов на ленте,

и выполнять много других интересных операций. Удивительно, что на машине Тьюринга можно имитировать все действия, производимые современным компьютером! В самом деле, согласно тезису, выдвинутому независимо Чёрчем и Тьюрингом, на машине Тьюринга можно вычислить *все функции, вычислимые с помощью алгоритма*. Это утверждение известно как *тезис Чёрча–Тьюринга*:

Класс функций, вычислимых на машине Тьюринга, в точности совпадает с классом функций, которые естественно рассматривать как вычислимые с помощью алгоритма.

Тезис Чёрча–Тьюринга утверждает эквивалентность строгого математического понятия – функции, вычислимой на машине Тьюринга и интуитивного понятия – вычислимой с помощью алгоритма функции. Важность этого тезиса в том, что он делает возможным изучение реальных алгоритмов (понятие алгоритма было до 1936 г. было довольно неопределенным) строгими математическими методами. Чтобы понять, почему это важно, полезно посмотреть на определение *непрерывной функции* из математического анализа. Любой ребенок скажет, что линия, нарисованная на бумаге, непрерывна, но далеко не очевидно, как оформить это интуитивное понятие в строгое определение. Математики XIX века посвятили много времени спорам о достоинствах различных определений непрерывности, пока не было принято современное определение. Когда даются определения фундаментальных понятий, таких как непрерывность или вычислимость, важно, чтобы выбранные определения обеспечивали максимальное соответствие между интуитивным понятием и точным математическим определением. С этой точки зрения тезис Чёрча–Тьюринга – это просто утверждение о том, что понятие машины Тьюринга обеспечивает хорошую основу информатики, подводя строгую базу под интуитивное понятие алгоритма.

Априори не очевидно, что любая функция, которую мы интуитивно рассматриваем как вычислимую с помощью алгоритма, может быть вычислена на машине Тьюринга. Чёрч, Тьюринг и многие другие ученые посвятили много времени сбору аргументов в пользу тезиса Чёрча–Тьюринга, и за 60 лет не было найдено ни одного аргумента против этого тезиса. Тем не менее не исключено, что в будущем мы найдем в природе процесс, вычисляющий функцию, которую нельзя вычислить с помощью машины Тьюринга. Было бы чудесно, если бы такой процесс действительно был обнаружен, поскольку тогда мы смогли бы выполнить вычисления, которые невозможно было сделать до этого. Разумеется, при этом нам пришлось бы переработать определение вычислимости, а с ним и информатику.

Упражнение 3.1 (невычислимые процессы в природе). Как можно установить, что какой-то природный процесс вычисляет функцию, невычислимую машиной Тьюринга?

Упражнение 3.2 (тьюринговы номера). Покажите, что одноленточные машины Тьюринга¹ можно пронумеровать числами $1, 2, 3, \dots$, однозначно определяющими соответствующую машину. Мы будем называть это число *тьюринг-*

¹ Это машины, которые были описаны выше. — Прим. ред.

говым номером соответствующей машины Тьюринга. (Указание. Каждое натуральное число может быть разложено единственным образом на простые множители в виде $p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, где p_i — различные простые числа и a_1, \dots, a_k — целые неотрицательные числа.)

В последующих главах мы увидим, что квантовые компьютеры также подчиняются тезису Чёрча–Тьюринга. Другими словами, квантовые компьютеры могут вычислять тот же класс функций, что и машины Тьюринга. Оказывается, что разница между квантовыми компьютерами и машинами Тьюринга состоит в *эффективности* вычислений: существуют функции, которые на квантовом компьютере можно вычислить гораздо эффективнее, чем на классическом вычислительном устройстве, таком, как машина Тьюринга.

Полное доказательство того, что на машине Тьюринга можно смоделировать все обычные конструкции языков программирования, выходит за рамки этой книги (см. раздел «История и дополнительная литература» в конце главы). Описывая алгоритмы, мы не будем в явном виде записывать программу для соответствующей машины Тьюринга. Обычно будем пользоваться псевдокодом гораздо более высокого уровня, полагаясь на тезис Чёрча–Тьюринга в том отношении, что этот псевдокод можно перевести в описание машины Тьюринга. Мы не будем давать формального описания псевдокода. Вы можете его рассматривать как формализованную версию английского языка или как неформальную версию языка программирования наподобие C++ или Бейсика. Псевдокод позволяет удобным образом записывать алгоритмы, не вдаваясь в мелкие подробности, которые были бы нужны при описании машины Тьюринга. Пример использования псевдокода можно найти во вставке 3.2; далее в книге псевдокод будет использоваться также для описания квантовых алгоритмов.

Есть много вариантов машины Тьюринга. Можно представить себе машины Тьюринга с лентами различных типов. Например, можно рассматривать ленту, бесконечную в обе стороны, или же ленту, имеющую более, чем одно измерение. Пока невозможно физически осмысленным образом изменить описание машины Тьюринга так, чтобы при этом расширился класс функций, вычислимых на такой машине.

В качестве примера рассмотрим многоленточную машину Тьюринга. Для простоты ограничимся двухленточным случаем (обобщение на большее число лент очевидно). Подобно стандартной машине Тьюринга, двухленточная машина Тьюринга имеет конечное число внутренних состояний q_1, \dots, q_m , начальное состояние q_s и заключительное состояние q_h . У этой машины есть две ленты, на каждой из которых записаны символы из некоторого конечного алфавита Γ . Как и ранее, нам будет удобно считать, что алфавит состоит из четырех символов 0, 1, b и \triangleright , где \triangleright обозначает край каждой из лент. Машина снабжена двумя головками, по одной для каждой ленты. Главное отличие между двухленточной и стандартной машинами Тьюринга состоит в формате их программных строк. Программные строки двухленточной машины имеют вид $\langle q, x_1, x_2, q', x'_1, x'_2, s_1, s_2 \rangle$; это означает следующее: если внутреннее состояние есть q , первая головка находится над символом x_1 , а вторая головка —

над символом x_2 , то внутреннее состояние машины переходит в q' , на место x_1 записывается x'_1 , на место x_2 записывается x'_2 и головки сдвигаются в соответствии со значениями чисел s_1 и s_2 (эти значения могут быть равны $+1$, -1 или 0).

В каком смысле можно утверждать, что стандартная и двухленточная машины Тьюринга представляют собой эквивалентные вычислительные модели? Эти вычислительные модели эквивалентны в том смысле, что каждая из них может *моделировать* другую. Предположим, что у нас есть двухленточная машина Тьюринга, на вход которой подаются битовая строка x на первую ленту и пробелы в остальные ячейки на обе ленты (как обычно, в начале лент записан символ \triangleright). Эта машина вычисляет функцию $f(x)$; по определению, $f(x)$ — содержимое первой ленты после того, как машина завершила работу. Замечательно то, что для любой двухленточной машины Тьюринга, вычисляющей данную функцию f , существует эквивалентная ей одноленточная машина Тьюринга, вычисляющая ту же функцию f . Мы не будем объяснять как построить такую одноленточную машину, но основная идея состоит в том, что одноленточная машина Тьюринга моделирует двухленточную машину, используя свою единственную ленту для хранения содержимого обеих лент двухленточной машины. Для такого моделирования нужно производить дополнительные вычислительные операции, но существенно здесь то, что в принципе так сделать можно. На самом деле существует универсальная машина Тьюринга (см. вставку 3.1), которая может моделировать любую другую машину Тьюринга!²

Другой интересный вариант машины Тьюринга получается, если в модель ввести элемент случайности. Предположим, например, что машина Тьюринга может выполнять программную строку, вызывающую следующие действия: если внутреннее состояние есть q , а головка «видит» символ x , то производится бросание монеты. Если выпадает орел, то внутреннее состояние меняется на $q_{i\text{н}}$, а если решка, то на $q_{i\text{т}}$, где $q_{i\text{н}}$ и $q_{i\text{т}}$ — некоторые состояния машины Тьюринга. Такую программную строку можно записать в виде $\langle q, x, q_{i\text{н}}, q_{i\text{т}} \rangle$. Однако даже эта модель по существу не меняет возможностей машины Тьюринга. Нетрудно видеть, что мы можем моделировать такой алгоритм на детерминированной машине Тьюринга, перебирая все возможные последовательности вычислений, соответствующие различным результатам бросания монеты. Разумеется, такое детерминированное моделирование может быть гораздо менее эффективно, но для нашего обсуждения существенно то, что класс вычислимых функций не увеличится, если ввести в вычислительную модель элемент случайности.

Упражнение 3.3 (обращение битовой строки с помощью машины Тьюринга). Опишите машину Тьюринга, которая получает на вход двоичное число x и выдает биты числа x в обратном порядке. (Указание: Это и следующее упражнение вам легче выполнить, используя многоленточную машину Тьюринга и/или символы, отличные от нуля, единицы, \triangleright и пробела.)

² Универсальная машина Тьюринга, описанная во вставке 3.1, не имеет прямого отношения к моделированию двухленточных машин одноленточными — Прим. ред.

Вставка 3.1. Универсальная машина Тьюринга

Мы описывали машины Тьюринга, состоящие из трех элементов, которые могли меняться от машины к машине: начальная запись на ленте, внутренние состояния управляющего устройства и программа. Остроумная конструкция, известная под названием *универсальной машины Тьюринга* (УМТ) позволяет зафиксировать программу и состояния управляющего устройства, а варьировать только начальную запись на ленте.

Универсальная машина Тьюринга (см. рисунок ниже) обладает следующим свойством. Пусть M — произвольная машина Тьюринга, и пусть T_M — тьюрингов номер, соответствующий машине M . Тогда, получив на вход двоичное представление числа T_M , за которым следует пробел, а затем — произвольная символьная строка x , на выходе универсальная машина Тьюринга даст то же, что получилось бы на выходе у машины Тьюринга M , на вход которой подали строку x . Таким образом универсальная машина Тьюринга может моделировать любую другую машину Тьюринга!



Универсальная машина Тьюринга подобна современному компьютеру, в котором действия, которые он должен совершить, — «программа» — записаны в память аналогично тому, как битовая строка T_M записана в начале ленты универсальной машины Тьюринга. Данные, которые программа должна обрабатывать, записаны в памяти в отдельном месте (как x в универсальной машине Тьюринга). Для запуска программы используются некоторые аппаратные средства (всегда одни и те же). Эти аппаратные средства аналогичны внутренним состояниям и всегда одной и той же программе, выполняемой универсальной машиной Тьюринга.

Подробное описание построения универсальной машины Тьюринга выходит за рамки этой книги (хотя трудолюбивый читатель может попытаться ее построить). Ключевым моментом является само существование такой машины, с помощью которой можно выполнить любой алгоритм. Факт существования универсальной машины Тьюринга объясняет также сделанное нами ранее утверждение о том, что количество внутренних состояний машины Тьюринга не очень существенно: если только это число превышает количество состояний, нужное универсальной машине Тьюринга, с помощью универсальной машины можно смоделировать машину Тьюринга с любым числом внутренних состояний.

Вставка 3.2. Проблема остановки

В упражнении 3.2 вы видели, что с любой машиной Тьюринга можно единственным образом связать целое положительное число. Чтобы решить проблему Гильberta, Тьюринг использовал эту нумерацию для постановки *проблемы остановки*: остановится ли машина Тьюринга номер x , на вход которой подано число y ? Это корректно поставленная и интересная математическая задача. Нам же интересно, заканчивается ли работа наших программ. Тем не менее оказывается, что алгоритма, решающего проблему остановки, не существует. Чтобы доказать это, Тьюринг задался вопросом, существует ли алгоритм, решающий хотя бы более частную задачу: останавливается ли машина Тьюринга номер x , на вход которой подано то же самое число x ? Тьюринг определил *функцию остановки*

$$h(x) \equiv \begin{cases} 0, & \text{если машина с номером } x \text{ не останавливается на входе } x \\ 1, & \text{если машина с номером } x \text{ останавливается на входе } x \end{cases}$$

Если существует алгоритм, решающий проблему остановки, то, разумеется, существует и алгоритм, вычисляющий $h(x)$. Мы предположим, что такой алгоритм (обозначим его $\text{HALT}(x)$) существует, и выведем отсюда противоречие. Рассмотрим алгоритм, вычисляющий функцию $\text{TURING}(x)$, с псевдокодом

```

TURING(x)
y = HALT(x)
if y=0 then
    halt
else
    loop forever
end if

```

Поскольку HALT – это корректная программа, TURING также является корректной программой с некоторым тьюринговым номером t . По определению, функция остановки $h(t) = 1$ тогда и только тогда, когда TURING останавливается при подаче на вход t . Однако же, посмотрев на программу TURING , мы видим, что TURING останавливается при подаче на вход числа t тогда и только тогда, когда $h(t) = 0$. Таким образом, $h(t) = 1$ тогда и только тогда, когда $h(t) = 0$ – противоречие. Следовательно, наше предположение, что существует алгоритм, вычисляющий $h(x)$, было ошибочным. Отсюда заключаем, что не существует алгоритма, решающего проблему остановки.

Упражнение 3.4 (сложение по модулю 2 на машине Тьюринга). Опишите машину Тьюринга, которая выполняет сложение двоичных чисел x и y по модулю 2. Числа подаются на вход в таком виде: x в двоичной системе, потом один пробел, а затем y в двоичной системе. Если одно число короче другого,

считайте, что оно дополнено нулями слева в таком количестве, чтобы записи этих чисел имели одинаковую длину.

Вернемся к гильбертовской проблеме разрешения (Entscheidungsproblem), вдохновившей основателей теории алгоритмов. Существует ли алгоритм, решающий все математические задачи? Чёрч и Тьюринг показали, что ответ на этот вопрос отрицателен. Во вставке 3.2 мы объясним принадлежащее Тьюрингу доказательство этого замечательного факта. Теперь известно, что явление *неразрешимости* возникает и далеко за пределами примеров, построенных Чёрчем и Тьюрингом. Например, известно, что неразрешима проблема, будут ли два данные топологические пространства топологически эквивалентны («гомеоморфны»)³. Существуют простые задачи, связанные с поведением динамических систем, которые также являются неразрешимыми (вы это увидите в задаче 3.4). Ссылки по поводу этих и других примеров даны в конце главы в разделе «История и дополнительная литература». Неразрешимость помимо того, что сама представляет интерес, указывает на тематику, важную для информатики, а также для квантовых вычислений и квантовой теории информации: различие между легко решаемыми и труднорешаемыми задачами. Неразрешимость дает крайний пример труднорешаемых задач — настолько трудно, что решить их и совсем невозможно.

Упражнение 3.5 (проблема остановки без входных данных). Покажите, что не существует алгоритма, позволяющего выяснить, остановится ли данная машина Тьюринга M , если на ее входе будут одни пробелы.

Упражнение 3.6 (вероятностная проблема остановки). Пусть мы пронумеровали вероятностные машины Тьюринга аналогично тому, как были пронумерованы стандартные машины Тьюринга в упражнении 3.2, и определили вероятностную функцию остановки $h_p(x)$ как функцию, принимающую значение 1, если машина номер x останавливается при подаче x на вход с вероятностью, не меньшей $1/2$, и принимающую значение 0 с вероятностью, меньшей $1/2$. Покажите, что не существует вероятностной машины Тьюринга, которая для всех x выдает значение $h_p(x)$ с вероятностью, строго большей $1/2$.

Упражнение 3.7 (проблема остановки с оракулом). Пусть у нас появился доступ к *чёрному ящику*, принимающему на вход целое неотрицательное число x и выдающему на выходе $h(x)$, где $h(\cdot)$ — функция остановки, определенная во вставке 3.2. Чёрный ящик такого типа иногда называется *оракулом* для проблемы остановки. Предположим, что у нас есть стандартная машина Тьюринга, дополненная возможностью обращаться к оракулу. Один из способов реализовать это — воспользоваться двухленточной машиной Тьюринга и иметь возможность пользоваться программными строками, в которых вызывается оракул, а на второй ленте печатается $h(x)$, где x — текущее содержимое второй ленты. Ясно, что эта вычислительная модель является более эффективной, чем стандартная машина Тьюринга, поскольку с ее помощью можно

³ Чтобы это утверждение имело смысл, надо считать, что речь идет не о произвольных топологических пространствах, но о многообразиях. — Прим. перев.

вычислить функцию остановки. Является ли проблема остановки неразрешимой на этой модели? Другими словами, существует ли машина Тьюринга с оракулом для проблемы остановки, которая определяет, останавливается ли заданная машина Тьюринга с оракулом для проблемы остановки при заданном входе?

3.1.2 Схемы

Машины Тьюринга — довольно идеализированные модели вычислительных устройств. Настоящие компьютеры имеют *конечные* размеры, тогда как длина ленты машины Тьюринга не ограничена. В этом разделе мы изучим альтернативную модель вычислений, а именно *схемную модель*, которая эквивалентна машине Тьюринга с точки зрения вычислительных возможностей, но более удобна и реалистична во многих приложениях. В частности, схемная модель вычислений особенно важна в качестве подготовки к нашему исследованию квантовых компьютеров.

Схема состоит из *проводов*, переносящих информацию, и *элементов*, производящих простые вычислительные операции. Например, на рис. 3.2 изображена простая схема, на вход которой поступает один бит a . Этот бит пропускается через элемент NOT, который обращает его, переводя 1 в 0 и 0 в 1. Провода перед и после элемента NOT служат только для того, чтобы перенести бит через элемент; они представляют движение бита в пространстве a , может быть, и просто во времени.

Вообще, у схемы может быть много входных и выходных битов, проводов и логических элементов. *Логическим элементом* называется функция $f: \{0, 1\}^k \rightarrow \{0, 1\}^l$, переводящая набор из k входных битов в набор из l выходных битов (k и l фиксированы). Например, элемент NOT — это элемент с одним входным и одним выходным битом, вычисляющий функцию $f(a) = 1 \oplus a$, где a — бит, $a \oplus$ — сложение по модулю 2. Обычно считают, что в схеме нет циклов (чтобы избежать неустойчивости, как на рис. 3.3). Мы будем говорить, что схема без циклов *ациклична*, и придерживаться соглашения, что все схемы в схемной модели вычислений ацикличны.

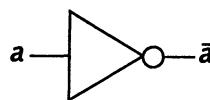


Рис. 3.2. Элементарная схема, производящая одну операцию NOT над одним битом

Существует много других элементарных логических элементов, полезных для вычислений. В частности, в их число входят элементы AND, OR, XOR, NAND и NOR. Каждый из этих элементов принимает два бита на входе и выдает один бит на выходе. Элемент AND выдает 1 тогда и только тогда, когда оба входных бита равны 1. Элемент OR выдает 1 тогда и только тогда, когда хотя бы один из входных битов равен 1. Элемент XOR выдает сумму своих входных битов

по модулю 2. Элементы NAND и NOR применяют AND и OR соответственно к своим входным битам, а затем — операцию NOT к полученным результатам. Действие этих элементов проиллюстрировано на рис. 3.4.

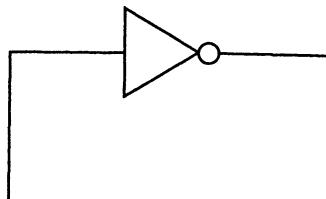


Рис. 3.3. Схемы, содержащие циклы, могут быть неустойчивы и обычно не допускаются в схемной модели вычислений.

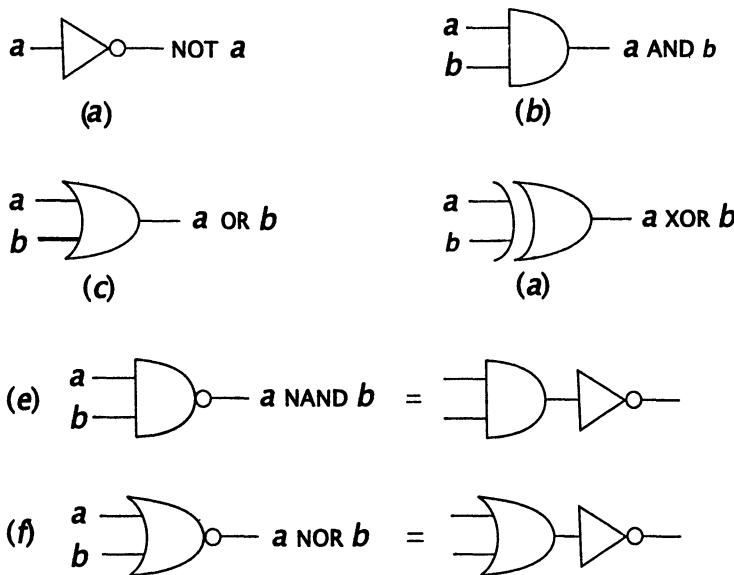


Рис. 3.4. Элементарные схемы, выполняющие операции AND, OR, XOR, NAND и NOR.

На рис. 3.4 отсутствуют два важных «элемента», а именно FANOUT и CROSSOVER. В схемах нередко приходится «заставлять» бит «делиться». Тогда вместо одного бита получаются две его копии. Эта операция и называется FANOUT. Кроме того, иногда нужно поменять местами значения двух битов. Это достигается операцией CROSSOVER. Третья операция, отсутствующая на рис. 3.4 и вообще не являющаяся логическим элементом, — это подготовка дополнительных, или рабочих, битов, что обеспечивает дополнительное рабочее пространство во время вычисления.

Эти простейшие элементы схем можно соединять и выполнять таким образом очень большое количество вычислений. Ниже мы покажем, что с помощью этих элементов можно вычислить любую функцию, а пока остановимся на простом примере схемы, складывающей два n -битовых числа с использованием по существу того же самого алгоритма, который изучают школьники во всем мире. Основной составной частью этой схемы является схема меньшего размера, известная под названием *полусумматор* (half-adder, сокращенно НА). Схема полусумматора изображена на рис. 3.5. Полусумматор получает на вход два бита x и y и выдает $x \oplus y$ — их сумму по модулю 2, бит переноса c , равный 1, если и x , и y равны 1, и 0 в противном случае.

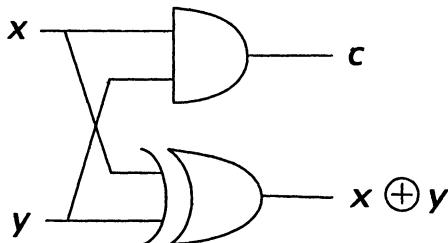


Рис. 3.5. Схема полусумматора. Бит переноса c устанавливается в единицу, если x и y равны единице, в противном случае $c = 0$.

Соединив два полусумматора, можно получить *сумматор* (full-adder, сокращенно FA), изображенный на рис. 3.6. Сумматор получает на входе три бита x , y и c . Биты x и y — это данные, которые требуется сложить, а c — бит переноса, полученный при предыдущем вычислении. Схема выдает на выходе два бита. Один из них — это сумма $x \oplus y \oplus c$ трех входных битов по модулю 2. Второй выходной бит c' является битом переноса, который устанавливается в единицу тогда и только тогда, когда два или более входных бита равны 1.

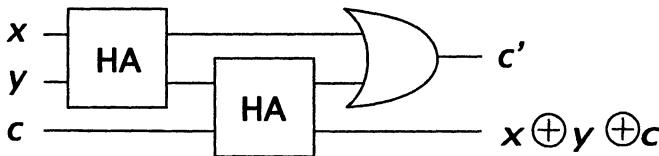


Рис. 3.6. Схема сумматора.

Соединяя сумматоры, мы получаем схему, складывающую два n -битовых целых числа (см. рис. 3.7 для случая $n = 3$).

Выше мы отмечали, что с помощью фиксированного набора элементов можно вычислить *любую* функцию $f: \{0, 1\}^n \rightarrow \{0, 1\}^m$. Теперь докажем упрощенный вариант этого утверждения: для функций $f: \{0, 1\}^n \rightarrow \{0, 1\}$ с n входными битами и одним выходным битом. Такая функция называется *булевой функцией*, а соответствующая схема — *булевой схемой*. Универсальность схем в общем

случае следует из частного случая булевых функций. Доказательство проводится индукцией по n . При $n = 1$ существуют четыре функции: тождественная, которой соответствует схема, состоящая из одного провода; обращение бита, получаемое с помощью одного элемента NOT; функция, замещающая входной бит на 0, которую можно реализовать путем применения операции AND к входному биту и рабочему биту, равному 0, и, наконец, функция, переводящая входной бит в 1, которую можно реализовать, применяя операцию OR к входному биту и рабочему биту, равному 1.

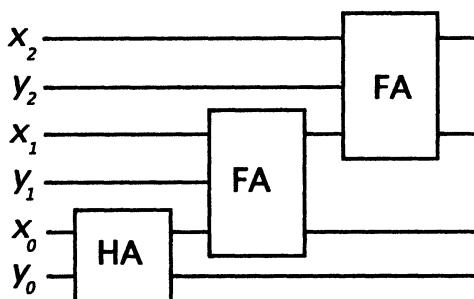


Рис. 3.7. Схема, складывающая два трехбитовых целых числа $x = x_2x_1x_0$ и $y = y_2y_1y_0$ с помощью алгоритма, изучаемого школьниками

Чтобы провести индукционный шаг, предположим, что любую функцию от n битов можно вычислить с помощью схемы и пусть f — функция от $n + 1$ бита. Определим n -битовые функции f_0 и f_1 формулами $f_0(x_1, \dots, x_n) \equiv f(0, x_1, \dots, x_n)$ и $f_1(x_1, \dots, x_n) \equiv f(1, x_1, \dots, x_n)$. Обе эти функции являются n -битовыми и, следовательно, по предположению индукции могут быть вычислены с помощью схем.

Теперь легко построить схему, вычисляющую функцию f . Эта схема, изображенная на рис. 3.8, вычисляет f_0 и f_1 от последних n битов. Затем в зависимости от того, равен первый бит нулю или единице, она выдает соответствующий ответ. Тем самым индукция завершается.

В конструкции универсальной схемы можно выделить пять компонентов: (1) провода, сохраняющие состояния битов; (2) приготовленные в стандартных состояниях вспомогательные биты, которые используются при доказательстве для случая $n = 1$; (3) элемент FANOUT, получающий на вход один бит и выдающий две копии этого бита; (4) элемент CROSSOVER, меняющий местами значения двух битов; (5) элементы AND, XOR и NOT. В главе 4 мы определим квантовые схемы подобно тому, как мы определили классические схемы. Любопытно отметить, что при построении квантовых аналогов указанных классических элементов возникают интересные проблемы: не очевидно, что хотя бы в принципе можно создать хорошие квантовые провода, в которых будут сохраняться кубиты, операцию FANOUT в квантовой механике нельзя реализовать непосредственно (ввиду теоремы о невозможности копирования, о которой шла речь в подразд. 1.3.5), а элементы AND и XOR не являются обратимыми и тем

самым не могут быть непосредственно реализованы как унитарные квантовые элементы. Конечно, при определении квантовой схемной модели есть о чём подумать!

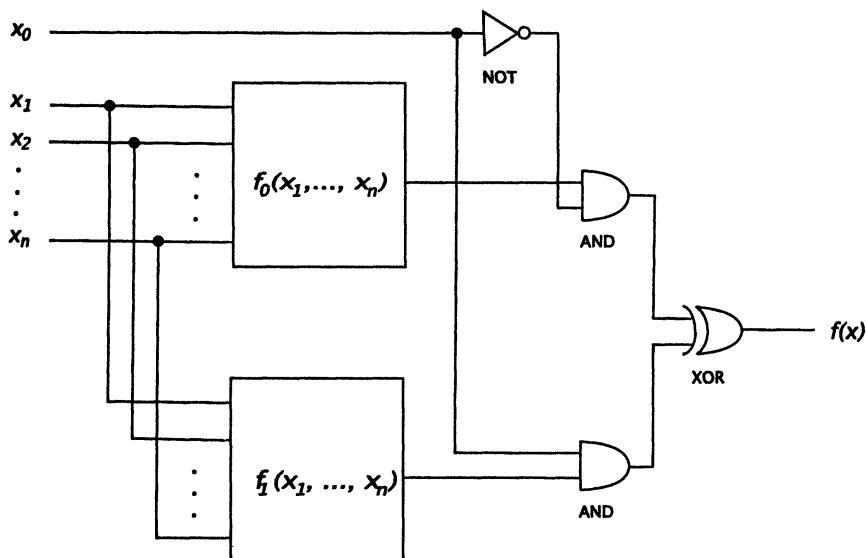


Рис. 3.8. Схема, вычисляющая произвольную $n + 1$ -битовую функцию; по предположению индукции существуют схемы, вычисляющие n -битовые функции f_0 и f_1

Упражнение 3.8 (универсальность элемента NAND). Покажите, что с помощью элемента NAND можно реализовать элементы AND, XOR и NOT, если использовать провода, вспомогательные биты и FANOUT.

Вернемся теперь к свойствам классических схем. Ранее мы отмечали, что машина Тьюринга эквивалентна схемной модели вычислений. Но что же мы понимаем под этой эквивалентностью? При поверхностном рассмотрении эти две модели представляются совершенно разными. Неограниченность машин Тьюринга делает их более полезными для абстрактного определения понятия алгоритма, тогда как схемы более удачно имитируют то, что происходит в настоящих компьютерах.

Две названные модели связываются с помощью понятия *однородного семейства схем*. По определению, семейство схем состоит из набора схем $\{C_n\}$, пронумерованных натуральными числами n . Схема C_n имеет n входных битов и может иметь любое конечное число вспомогательных и выходных битов. Результат применения схемы C_n к числу, длина записи которого не превышает n битов, обозначается $C_n(x)$. Мы накладываем условие, чтобы семейство было *совместным*, т. е. чтобы при $m < n$ выполнялось равенство $C_m(x) = C_n(x)$ для любого числа x , содержащего не более m битов. Функция, вычисляемая семейством схем $\{C_n\}$, — это такая функция $C(\cdot)$, что $C(x) = C_n(x)$, если число x содержит n битов. Если, например, C_n — схема, возводящая в квадрат

n -битовое число, то семейство схем $\{C_n\}$ вычисляет функцию $C(x) = x^2$, где x — натуральное число.

Недостаточно однако рассматривать произвольные семейства схем; на практике нам нужен алгоритм для построения схемы. В самом деле, если не налагать на семейство схем никаких ограничений, то мы сможем вычислять любую функцию в том числе и такую, про которую нельзя надеяться, что ее удастся вычислить с помощью разумной вычислительной модели. Пусть, например, $h_n(x)$ — функция остановки, ограниченная на n -битовые значения x . Тогда h_n — функция, переводящая n битов в 1 бит, и мы доказали, что существует схема C_n , вычисляющая $h_n(\cdot)$. Следовательно, семейство схем $\{C_n\}$ вычисляет функцию остановки! Однако мы не можем использовать это семейство схем для решения проблемы остановки, так как не указали алгоритм, позволяющий построить схему C_n для всех значений n . Если добавить условие, что такой алгоритм должен существовать, то мы придем к понятию равномерного семейства схем.

Семейство схем $\{C_n\}$ называется *однородным семейством схем*, если существует выполнимый на машине Тьюринга алгоритм, который, получив на входе n , генерирует описание схемы C_n . Иными словами, на выходе алгоритма получается описание того, какие элементы содержатся в схеме C_n , как они связаны друг с другом, какие нужны вспомогательные биты, где используются операции FANOUT и CROSSOVER и откуда надо считывать выходные биты. Например, описанное выше семейство схем, возводящих n -битовые числа в квадрат, бесспорно является однородным, так как существует алгоритм, который по данному n выдает описание схемы, возводящей в квадрат n -битовые числа. Вы можете рассматривать такой алгоритм как средство, с помощью которого инженер может получить описание такой схемы (а, следовательно, и построить ее) для произвольного n . Напротив, семейство схем, не являющееся однородным, называется *неоднородным*. В этом случае не существует алгоритма построения схемы для произвольного n , что не позволяет инженеру построить схемы для вычисления функций, например функции остановки.

На интуитивном уровне однородное семейство схем — это семейство, которое можно получить с помощью какого-либо разумного алгоритма. Можно показать, что класс функций, вычислимых с помощью однородных семейств схем, в точности совпадает с классом функций, вычислимых с помощью машины Тьюринга. Если наложить условие однородности, то результаты, полученные с использованием модели вычислений, основанной на машине Тьюринга, обычно можно непосредственно распространить на схемную модель, и обратно. Позже мы рассмотрим вопросы однородности для случая схемной модели квантовых вычислений.

3.2 Анализ вычислительных задач

При анализе вычислительных задач нужно ответить на три фундаментальных вопроса.

1. **Что такое вычислительная задача?** Перемножение двух чисел — вычислительная задача; написание компьютерной программы, предназначенней превзойти человеческие возможности в написании стихов, — тоже. Чтобы можно было продвинуться в общей теории анализа вычислительных задач, мы выделим специальный класс задач, называемых *задачами разрешения*, и именно на них сосредоточим свой анализ. Такое ограничение дает возможность развить элегантную и богатую теорию; что еще важнее, эта теория имеет приложения, далеко выходящие за рамки задач разрешения.
2. **Как построить алгоритмы, решающие данную вычислительную задачу?** Какие алгоритмы можно использовать для решения данной задачи? Существует ли общий метод, позволяющий решить широкий класс задач? На чем может быть основана наша уверенность в том, что алгоритм ведет себя именно так, как требуется?
3. **Каковы минимальные ресурсы, необходимые для решения данной вычислительной задачи?** При выполнении алгоритма используются различные *ресурсы*: время, память, энергия. В различных ситуациях может быть желательно минимизировать потребление тех или иных из этих ресурсов. Можно ли классифицировать задачи, исходя из количества ресурсов, необходимых для их решения?

В нескольких последующих разделах мы исследуем эти вопросы, особенно первый и третий, хотя первый вопрос, «что такое вычислительная задача», является, возможно, наиболее фундаментальным, мы отложим ответ на него до подразд. 3.2.3, а предварительно введем некоторые понятия, связанные с количественной оценкой ресурсов (подразд. 3.2.1), и сделаем обзор основных путей *теории сложности вычислений* (подразд. 3.2.2).

Второй вопрос (как построить хорошие алгоритмы) является предметом рассмотрения большого количества исследователей, и в этом кратком введении мы не можем даже начать описание основных идей, используемых при разработке хороших алгоритмов. Если вы интересуетесь этим прекрасным предметом, мы отсылаем вас к разделу «История и дополнительная литература», приведенному в конце главы. Ближе к этой тематике мы подойдем позже, когда будем рассматривать квантовые алгоритмы. Подход, используемый при построении квантовых алгоритмов, обычно представляет собой соединение глубоких идей, применяемых при разработке алгоритмов для классических компьютеров, и новых, полностью квантовомеханических приемов. По этой причине, а также поскольку разработка квантовых алгоритмов во многих отношениях весьма близка к разработке классических алгоритмов, мы призываем вас ознакомиться хотя бы с основными идеями разработки алгоритмов.

Третий вопрос (каковы минимальные ресурсы, необходимые для решения данной вычислительной задачи) рассматривается в нескольких следующих разделах. Пусть, например, у нас есть два числа, каждое длиной n битов, и мы хотим их перемножить. Если умножение производится на одноленточной ма-

шине Тьюринга, сколько операций необходимо произвести, чтобы получить результат? Сколько места на ленте машины Тьюринга будет использовано в процессе этого умножения?

Эти примеры показывают, какого типа вопросы о ресурсах мы будем задавать. Вообще говоря, компьютеры пользуются ресурсами многих различных видов, но мы в основном сосредоточим внимание на времени, памяти и энергии. Время и память были двумя основными видами ресурсов, которым уделялось внимание при анализе алгоритмов; мы посвятим им подразд. 3.2.2–3.2.4. Энергией обычно интересовались меньше; однако же изучение энергетических затрат мотивирует понятие обратимого классического вычисления, которое, в свою очередь, необходимо для квантовых вычислений, так что мы рассмотрим вопросы затрат энергии при вычислениях в подразд. 3.2.5 довольно подробно.

3.2.1 Как количественно оценивать компьютерные ресурсы

Различные вычислительные модели требуют различных затрат ресурсов. Даже простой переход от одноленточной машины Тьюринга к двухленточной, может изменить объем ресурсов, требуемых при решении данной задачи. Для очень хорошо понятой вычислительной задачи (например, такой, как сложение целых чисел) такие различия между моделями могут представлять интерес. Однако для первичного понимания задачи лучше оценивать требуемые ресурсы способом, независимым от более или менее тривиальных изменений в модели. Одним из средств, применяемых для такой оценки, являются *асимптотические обозначения*, с помощью которых можно описать существенную часть поведения функции. Эти обозначения можно, например, использовать для того, чтобы указать, сколько по существу операций использует алгоритм, не занимаясь точным подсчетом времени его работы. В настоящем разделе мы подробно опишем эти обозначения и применим их к простой задаче, иллюстрирующей количественно оценку вычислительных ресурсов, — анализу алгоритмов сортировки последовательности слов в алфавитном порядке.

Предположим, например, что нас интересует количество элементов, необходимое для сложения двух n -битовых чисел. Точное вычисление этого количества только затемняет общую картину. В самом деле, пусть некоторый алгоритм требует для этого сложения $24n + 2[\log n] + 16$ элементов; в предельном случае задач большого размера единственное слагаемое, которое играет роль, это $24n$. Далее, мы не обращаем внимание на постоянные сомножители, поскольку их значение для анализа алгоритмов второстепенно. *Существенное* поведение алгоритма можно описать, сказав, что число требуемых операций примерно пропорционально n , где n — количество битов в складываемых числах. Есть три основных асимптотических обозначений.

Обозначение O (« O большое») используется для указания *верхних оценок* функций. Пусть $f(n)$ и $g(n)$ — функции на целых неотрицательных числах. Мы говорим « $f(n)$ принадлежит классу функций $O(g(n))$ », если существуют такие константы c и n_0 , что для всех n , больших n_0 , выполняется неравенство $f(n) \leq c g(n)$. Тем самым для достаточно больших n функция $g(n)$ является верхней

оценкой для $f(n)$, с точностью до несущественного постоянного множителя. Обозначения с « O » особенно полезны при изучении поведения конкретных алгоритмов в худшем случае, когда нам часто хватает верхней оценки ресурсов, потребляемых алгоритмом.

При изучении поведения целого класса алгоритмов (например, алгоритмов умножения двух чисел) интересно найти нижние оценки требуемых ресурсов. При этом используются обозначения с буквой Ω (« Ω большое»). Говорят, что функция $f(n)$ принадлежит $\Omega(g(n))$, если существуют такие числа c и n_0 , что $cg(n) \leq f(n)$ при всех n , больших n_0 . Другими словами при достаточно больших n функция $g(n)$ является нижней оценкой для $f(n)$ с точностью до несущественного постоянного множителя.

Наконец, обозначения с буквой Θ (« Θ большое») используются, когда нужно сказать, что асимптотически $f(n)$ ведет себя так же, как $g(n)$, с точностью до несущественных постоянных множителей. Мы говорим, что $f(n)$ принадлежит $\Theta(g(n))$, если она одновременно принадлежит классам $O(g(n))$ и $\Omega(g(n))$.

Асимптотические обозначения: примеры

Рассмотрим несколько простых примеров асимптотических обозначений. Функция $2n$ принадлежит $O(n^2)$, поскольку $2n \leq 2n^2$ для всех положительных n . Функция 2^n принадлежит $\Omega(n^3)$, поскольку $n^3 \leq 2^n$ для достаточно больших n . Наконец, функция $7n^2 + \sqrt{n} \log n$ есть $\Theta(n^2)$, поскольку $7n^2 \leq 7n^2 + \sqrt{n} \log n \leq 8n^2$ при всех достаточно больших n . В следующих упражнениях вы познакомитесь с элементарными свойствами асимптотических обозначений, благодаря которым они являются полезным инструментом при анализе алгоритмов.

Упражнение 3.9. Докажите, что $f(n)$ принадлежит $O(g(n))$ тогда и только тогда, когда $g(n)$ принадлежит $\Omega(f(n))$. Выведите отсюда, что $f(n)$ принадлежит $\Theta(g(n))$ тогда и только тогда, когда $g(n)$ принадлежит $\Theta(f(n))$.

Упражнение 3.10. Пусть $g(n)$ — многочлен степени k . Покажите, что $g(n)$ принадлежит $O(n^l)$ при всех $l \geq k$.

Упражнение 3.11. Покажите, что $\log n$ принадлежит $O(n^k)$ при всех $k > 0$.

Упражнение 3.12 ($n^{\log n}$ суперполиномиальна). Покажите, что n^k принадлежит $O(n^{\log n})$ для любого k , но $n^{\log n}$ никогда не принадлежит $O(n^k)$.

Упражнение 3.13 ($n^{\log n}$ субэкспоненциальна). Покажите, что c^n принадлежит $\Omega(n^{\log n})$ для любого $c > 1$, но $n^{\log n}$ никогда не принадлежит $\Omega(c^n)$.

Упражнение 3.14. Пусть $e(n)$ принадлежит $O(f(n))$ и $g(n)$ принадлежит $O(h(n))$. Покажите, что $e(n)g(n)$ принадлежит $O(f(n)h(n))$.

Примером использования асимптотических обозначений при оценке компьютерных ресурсов является следующее простое приложение к задаче сортировки списка из n слов в алфавитном порядке. Многие алгоритмы сортировки основаны на операции «сравнение и обмен»: два элемента в n -элементном списке сравниваются и, если они идут в неправильном порядке, меняются местами. Если эта операция сравнения с обменом — единственное, что мы можем делать

со списком, то сколько таких операций нужно, чтобы гарантировать, что список отсортирован?

Простой алгоритм сортировки, основанный на сравнении и обмене, выглядит так (команда `compare-and-swap(j,k)` сравнивает записи с номерами j и k и меняет их местами, если они идут в неверном порядке):

```
for j=1 to n-1
    for k=j+1 to n
        compare-and-swap(j,k)
    end k
end j
```

Ясно, что этот алгоритм правильно сортирует список из n слов в алфавитном порядке. Заметим, что число операций «сравнение и обмен», выполняемых алгоритмом, равно $(n - 1) + (n - 2) + \dots + 1 = n(n - 1)/2$. Таким образом, число этих операций есть $\Theta(n^2)$. Можно ли обойтись меньшим количеством? Оказывается, что да. Известны алгоритмы, например «heapsort» (сортировка с помощью кучи), использующие $O(n \log n)$ сравнений. Далее в упражнении 3.15 вы покажете с помощью несложного подсчета, что любой алгоритм, основанный на операции «сравнение и обмен», использует $\Omega(n \log n)$ этих операций. Таким образом, сортировка, вообще говоря, требует $\Theta(n \log n)$ сравнений.

Упражнение 3.15 (нижние оценки для сортировки, основанной на сравнении и обмене). Пусть n -элементный список подвергается сортировке с помощью некоторой последовательности операций «сравнение и обмен». Расположить элементы в списке можно $n!$ способами. Покажите, что после k операций «сравнение и обмен» список будет отсортирован для не более чем 2^k начальных расстановок. Выведите отсюда, что для того, чтобы отсортировать способом «сравнение и обмен» любую исходную расстановку, необходимо $\Omega(n \log n)$ операций.

3.2.2 Сложность вычислений

Мысль о том, что не существует алгоритма, решающего эту задачу, — что есть что-то фундаментальное, что никогда не изменится — эта мысль мне нравится.

Стивен Кук

*Иногда это хорошо, что некоторые вещи невозможны.
Я рад, что есть много вещей, которые никто не сможет сделать со мной.*

Леонид Левин

Не следует удивляться тому, что наш выбор полиномиальных алгоритмов в качестве формализации неформального понятия «вычисление, эффективное на практике», подвержен критике со всех сторон. (...)

В конечном счете наш довод в пользу этого выбора должен звучать так: если принять полиномиальность в худшем случае за критерий эффективности, то получается элегантная и полезная теория, которая говорит нечто осмысленное о практических вычислениях и которая была бы невозможна без этого упрощения.

Кристос Пападимитриу

Сколько времени и памяти нужно для данного вычисления? Во многих случаях это самые важные вопросы, которые можно задать о вычислительной задаче. Задачи вроде сложения и умножения чисел считаются эффективно разрешимыми, поскольку у нас есть *быстрые* алгоритмы для сложения и умножения, которые в процессе выполнения используют мало памяти. Для многих других задач быстрые алгоритмы неизвестны и тем самым эти задачи по существу неразрешимы не потому, что мы не можем найти разрешающий их алгоритм, а потому, что для всех известных алгоритмов требуется настолько большие объемы времени и памяти, что это делает их практически бесполезными.

Теория сложности вычислений изучает, сколько времени и памяти необходимо для решения вычислительных задач. Задача этой теории — дать *нижние оценки* для объема ресурсов, потребляемых наилучшим возможным алгоритмом для решения данной задачи (даже если такой алгоритм в явном виде не известен). В этом и двух следующих разделах дается обзор теории сложности вычислений, ее основных понятий и некоторых из наиболее важных результатов. Отметим, что теория сложности вычислений в каком-то смысле дополнительна к разработке алгоритмов; в идеале для наиболее эффективных алгоритмов, которые мы можем создать, будут в точности достигаться нижние оценки, полученные в рамках теории сложности вычислений. К сожалению, часто дело обстоит иначе. Как уже отмечали, в этой книге мы не будем глубоко рассматривать разработку классических алгоритмов.

При формулировке утверждений теории сложности вычислений возникает одна трудность: для решения одной и той же задачи на разных вычислительных моделях может быть нужен разный объем ресурсов. Например, многоленточные машины Тьюринга могут решать многие задачи существенно быстрее, чем одноленточные. Эта трудность разрешается довольно грубым способом. Предположим, что на вход подается n битов (например, нам может быть нужно узнать, является ли простым данное n -битовое число). Главное различие, которое проводится в теории сложности, — это различие между задачами, которые можно решить с использованием ресурсов, объем которых ограничен сверху *многочленом от n* , и задачами, для которых необходимый объем ре-

сурсов растет быстрее, чем любой многочлен от n . В последнем случае обычно говорят, что задача требует *экспоненциальных* ресурсов (злоупотребляя словом «экспоненциальный»: существуют функции, например $n^{\log n}$, которые растут быстрее любого полинома и тем самым являются «экспоненциальными» в нашем смысле, но при этом растут медленнее любой настоящей экспоненты). Задача считается *легкой*, *простой* или *решаемой*, если для ее решения существует полиномиальный алгоритм, и *трудной*, *сложной* или *нерешаемой*, если наилучший возможный алгоритм требует экспоненциального объема ресурсов.

В качестве простого примера рассмотрим два числа с двоичными записями $x_1 \dots x_{m_1}$ и $y_1 \dots y_{m_2}$ и предположим, что нужно найти их сумму. Общий объем входных данных равен $n \equiv m_1 + m_2$. Легко видеть, что числа можно сложить, используя $\Theta(m)$ элементарных операций; этот алгоритм использует полиномиальное (а именно, линейное) число операций. Напротив, считается (хотя это так и не доказано!), что задача разложения числа на простые множители является сложной и, что не существует алгоритма, с помощью которого произвольное n -битовое число можно разложить на простые множители с помощью $O(p(n))$ операций, где p — некоторый фиксированный многочлен от n . Ниже мы приведем много других примеров задач, считающихся сложными в этом смысле.

Разделение задач на полиномиальные и экспоненциальные является довольно грубой классификацией. На практике алгоритм, решающий задачу за $2^{n/1000}$ операций, является, возможно, более полезным, чем тот, который использует n^{1000} операций. Только при очень большом ($n \approx 10^8$) объеме входных данных этот «эффективный» полиномиальный алгоритм будет предпочтительнее «неэффективного» экспоненциального и для многих целей разумнее будет пользоваться именно «неэффективным» алгоритмом.

Однако существует много причин, по которым имеет смысл основывать теорию сложности вычислений именно на разделении алгоритмов на полиномиальные и экспоненциальные. Во-первых, исторически за малым числом исключений сложилось так, что полиномиальные алгоритмы работали существенно быстрее экспоненциальных. Можно подумать, что причина этого в недостатке нашего воображения: разработать алгоритм, в котором число операций равно n , n^2 или какому-нибудь еще многочлену маленькой степени, часто гораздо проще, чем алгоритм, требующий n^{1000} операций, хотя и такие примеры существуют. Так что склонность человека к построению относительно простых алгоритмов привела к тому, что на практике полиномиальные алгоритмы работают достаточно эффективно.

Вторая и более серьезная причина того, что имеет смысл настаивать на разделении алгоритмов на полиномиальные и экспоненциальные, связана с *сильной формой тезиса Чёрча–Тьюринга*. В разд. 1.1 мы уже обсуждали, что в 60-70-х гг. было замечено, что вероятностная машина Тьюринга является сильнейшей из «разумных» вычислительных моделей. Точнее говоря, различные исследователи независимо пришли к выводу, что если можно вычислить функцию с помощью k операций на некоторой модели, *не являющейся* вероятностной машиной Тьюринга, то на вероятностной машине Тьюринга ту же

самую функцию можно вычислить не более чем за $p(k)$ операций, где $p(\cdot)$ — некоторый многочлен. Это утверждение известно как *усиленный тезис Чёрча–Тьюринга*:

Тезис Чёрча–Тьюринга (усиленная форма). *Любая вычислительная модель может быть смоделирована на вероятностной машине Тьюринга с не более чем полиномиальным увеличением числа операций.*

Усиленный тезис Чёрча–Тьюринга имеет большое значение для теории сложности вычислений в том отношении, что из него вытекает, что все внимание можно сосредоточить на вероятностной машине Тьюринга. Если задача не допускает полиномиального решения на вероятностной машине Тьюринга, то из этого тезиса следует, что ни на каком вычислительном устройстве она не имеет эффективного решения. Теория сложности вычислений принимает элегантный вид и перестает зависеть от выбора модели, если только отождествить эффективность алгоритма с его полиномиальностью, и именно эта элегантность подтолкнула исследователей на отождествление понятий «разрешимость с полиномиальными ресурсами» и «эффективная разрешимость». Конечно, одна из основных причин, по которым квантовые компьютеры представляют интерес, это то, что они подвергают усиленный тезис Чёрча–Тьюринга сомнению, так как позволяют эффективно решить задачи, которые считаются сложными для всех классических компьютеров, включая вероятностные машины Тьюринга! Тем не менее полезно понять и оценить ту роль, которую усиленный тезис Чёрча–Тьюринга сыграл в процессе построения не зависящей от модели теории сложности вычислений.

Отметим в заключение, что специалисты по информатике интересуются не только разделением задач на полиномиальные и экспоненциальные. Это лишь первый и самый грубый способ оценки трудности вычислительных задач. Тем не менее такое разделение является исключительно важным; оно иллюстрирует многие более общие вопросы, связанные с проблемой потребления ресурсов при вычислениях. В большей части этой книги при оценке эффективности алгоритма мы будем в первую очередь руководствоваться именно отличием полиномиальности от экспоненциальности.

Теперь, когда мы объяснили, чем хорошо разделение алгоритмов на полиномиальные и экспоненциальные, следует признаться, что у теории сложности вычислений имеется один крупный недостаток: по-видимому, очень трудно доказать, что существуют интересные классы задач, для которых нет полиномиальных алгоритмов. Совсем легко дать неконструктивное доказательство того факта, что для большинства задач требуются экспоненциальные ресурсы (см. упр. 3.16), и более того, существуют гипотезы, согласно которым для многих задач требуются экспоненциальные ресурсы, но строгих доказательств этих гипотез нет и представляется, что найти эти доказательства очень трудно, по крайней мере, при современном состоянии предмета. Этот недостаток теории сложности вычислений имеет важные последствия и для квантовых вычислений, поскольку эффективность квантовых компьютеров сравнивается с эффек-

тивностью *классических* вычислительных моделей. До тех пор, пока основные проблемы классической теории сложности вычислений не будут решены, об эффективности квантовых компьютеров нельзя сказать ничего определенного; нельзя даже сказать, действительно ли квантовый компьютер эффективнее классического компьютера.

Упражнение 3.16 (экспоненциально вычислимые функции существуют). Покажите, что существуют булевы функции с n аргументами, для вычисления которых требуется не менее $2^n / \log n$ логических элементов.

3.2.3 Задачи разрешения и классы сложности P и NP

Многие вычислительные задачи лучше всего формулируются как *задачи разрешения*, т. е. задачи, дающие ответ в виде «да» или «нет». Пример: является данное число t простым или нет? (это *задача определения простоты*). Основными для теории сложности вычислений являются именно задачи разрешения по двум причинам: во-первых, при этом теория принимает наиболее простой и элегантный вид, но при этом остается возможность ее естественного обобщения на более сложные случаи и, во-вторых, исторически теория сложности вычислений возникла прежде всего из анализа задач разрешения.

Хотя большинство задач разрешения легко сформулировать на простом и знакомом языке, обсуждение общих задач разрешения сильно облегчается, если воспользоваться понятием *формального языка*. Языком L в алфавите Σ называется подмножество множества Σ^* , состоящего из всех конечных строк символов алфавита. Если, например, $\Sigma = \{0, 1\}$, то множество двоичных записей четных чисел $L = \{0, 10, 100, 110, \dots\}$ является языком в алфавите Σ .

Задачи разрешения можно очевидным образом переформулировать как задачи о языках. Например, задача определения простоты может быть сформулирована с помощью двоичного алфавита $\Sigma = \{0, 1\}$. Строки из Σ^* можно интерпретировать как целые неотрицательные числа (например, 0010 — это число 2). Язык L определим как состоящий из двоичных строк, соответствующих простым числам.

Чтобы решить задачу определения простоты, нам нужна машина Тьюринга, которая, при подаче числа n на вход выдает какой-то эквивалент ответа «да», если число простое, и выдает «нет», если число составное. Для того, чтобы уточнить это определение, нам будет удобно слегка модифицировать наше прежнее определение машины Тьюринга (подразд. 3.1.1), заменив заключительное состояние q_h на пару состояний q_Y и q_N , представляющих ответы «да» и «нет» соответственно. Во всех остальных отношениях машина ведет себя по-прежнему, а останавливается, когда приходит в состояние q_Y или q_N . Язык L распознается машиной Тьюринга, если машина может определить, принадлежит ли входное слово языку L , следующим образом: она останавливается в состоянии q_Y , если $x \in L$, и останавливается в состоянии q_N , если $x \notin L$. Мы будем говорить, что машина *приняла* или *отвергла* слово x в зависимости от того, какое из этих событий произошло.

Как быстро сможем мы определить, является ли число простым? Другими словами, какова максимальная скорость машины Тьюринга, распознающей

язык, который соответствует задаче определения простоты? Будем говорить, что задача принадлежит классу $\text{TIME}(f(n))$, если существует машина Тьюринга, выясняющая, принадлежит ли слово x данному языку, за время $O(f(n))$, где n — длина x . Говорят, что задача *разрешима за полиномиальное время*, если она принадлежит классу $\text{TIME}(n^k)$ для некоторого конечного k . Множество всех языков, принадлежащих классу $\text{TIME}(n^k)$ для некоторого k , обозначается P . Класс P — это наш первый пример *класса сложности*. Вообще, класс сложности — это некоторое множество языков. Значительная часть теории сложности состоит в определении различных классов сложности и выяснении отношений между ними.

Не удивительно, что существуют задачи, неразрешимые за полиномиальное время. К сожалению, доказательство того, что какая-то конкретная задача неразрешима за полиномиальное время, представляется очень трудным, хотя существует очень много гипотез. Простым примером интересной задачи разрешения, про которую принято считать, что она не принадлежит классу P , является *задача о существовании делителя*.

ЗАДАЧА О СУЩЕСТВОВАНИИ ДЕЛИТЕЛЯ. Дано составное число m и целое число $l < m$. Есть ли у числа m нетривиальный делитель, меньший, чем l ?

Интересным свойством этой задачи является то, что если кто-то заявит «Да, у числа m есть нетривиальный делитель, меньший, чем l », то истинность этого утверждения может быть эффективно проверена делением в столбик. Мы будем называть такой делитель *свидетельством* в пользу того, что у m есть делитель, меньший, чем l . Это понятие легко проверяемого свидетельства лежит в основе определения класса сложности NP , которое будет дано ниже. Мы сформулировали задачу о существовании делителя как задачу разрешения, но легко проверить, что эта задача эквивалентна разложению числа на простые множители:

Упражнение 3.17. Докажите, что алгоритм, выполняющий задачу разложения числа m на простые множители за полиномиальное время, существует тогда и только тогда, когда задача о существовании делителя принадлежит классу P .

Задача о существовании делителя — пример задачи разрешения, принадлежащей важному классу сложности, известному под названием NP . Задачи класса NP характерны тем, что в них ответ «да» может быть легко проверен с помощью подходящего свидетельства. Точнее говоря, язык L принадлежит классу NP , если существует машина Тьюринга M со следующими свойствами:

1. Если $x \in L$, то существует такая строка (свидетельство) w , что M останавливается в состоянии q_Y через время, полиномиальное по $|x|$, если в момент запуска машины на ленте записана строка x , пробел, а затем w .
2. Если $x \notin L$, то для любой строки w машина останавливается в состоянии q_N через время, полиномиальное по $|x|$, если в момент запуска на ленте стоит x , пробел и w .

В определении класса NP есть интересная асимметрия. В то время как мы должны иметь возможность быстро проверить, действительно ли данное свидетельство в пользу того, что $x \in L$, истинно, у нас нет необходимости предъявлять свидетельство в пользу того, что $x \notin L$. В задаче о существовании делителя мы можем легко убедиться, что данное число имеет делитель, меньший m , но нахождение свидетельства в пользу того, что у числа нет делителей, меньших m , более серьезная задача. Эта асимметрия подсказывает определение класса coNP, а именно класса языков, допускающих свидетельства в пользу ответа «нет»; очевидно, что coNP-языки являются дополнениями к NP-языкам.

Как связаны классы P и NP? Ясно, что P является подмножеством NP; самая знаменитая нерешенная проблема в теории сложности — выяснить, существуют ли NP-задачи, не принадлежащие классу P; часто эту проблему называют просто $P \neq NP$. Большинство специалистов по информатике считает, что $P \neq NP$, но, несмотря на десятилетия работы, никому не удалось это доказать, и остается возможность того, что $P = NP$.

Упражнение 3.18. Докажите, что если $\text{coNP} \neq NP$, то и $P \neq NP$.

При первом знакомстве с проблемой $P \neq NP$ возникает впечатление, что решить ее совсем просто. Чтобы понять, почему на самом деле эта проблема довольно тонкая, полезно рассмотреть несколько примеров задач, принадлежащих классам P и NP. Мы будем брать примеры из *теории графов*, являющейся богатым источником задач разрешения, имеющих удивительно много практических приложений. Графом называется конечное множество вершин $\{v_1, \dots, v_n\}$, соединенных ребрами, которые задаются парами вершин $\{v_i, v_j\}$. Здесь мы будем рассматривать только *неориентированные графы*, в которых порядок вершин в каждой из этих пар не играет роли; аналогичным образом могут быть рассмотрены *ориентированные графы*, в которых порядок вершин имеет значение. Типичный график изображен на рис. 3.9.

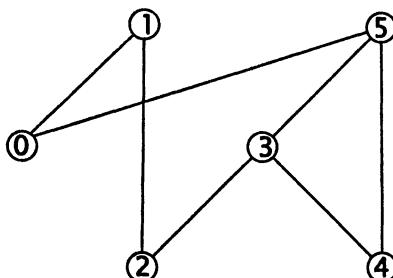


Рис. 3.9. Граф.

Цикл в графе — это такая последовательность вершин v_1, \dots, v_m , что каждая пара (v_j, v_{j+1}) , а также пара (v_1, v_m) , являются ребрами. *Простой цикл* — это цикл, в котором вершины, кроме первой и последней, не повторяются. *Гамильтонов цикл* — это простой цикл, в который входят все вершины графа.

Примеры графов, обладающих и не обладающих гамильтоновыми циклами, приведены на рис. 3.10.

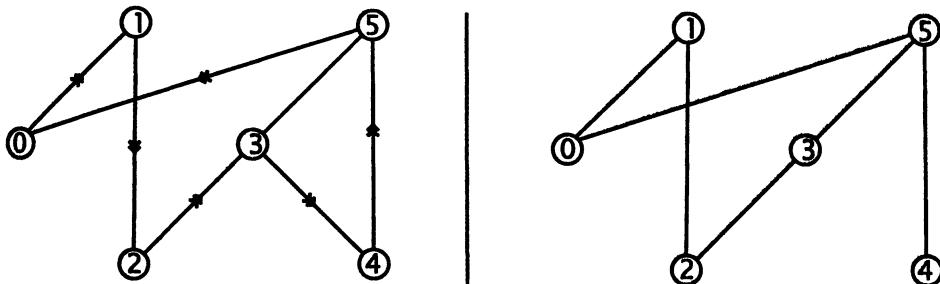


Рис. 3.10. Левый график содержит гамильтонов цикл 0, 1, 2, 3, 4, 5, 0. Граф справа гамильтонова цикла не содержит, что может быть проверено перебором.

Задача о гамильтоновом цикле (НС) состоит в том, что надо выяснить, обладает ли данный график гамильтоновым циклом. НС — это задача разрешения, принадлежащая классу NP, поскольку если гамильтонов цикл у данного графа есть, то он может быть использован в качестве легко проверяемого свидетельства. Более того, для задачи НС не известно никакого полиномиального алгоритма. На самом деле НС относится к классу так называемых NP-полных задач, которые могут рассматриваться как «самые трудные» в классе NP: если задачу НС можно решить за время t , то любая другая задача из класса NP может быть решена за время $O(\text{poly}(t))$. Это означает также, что если какая-либо NP-полная задача имеет решение за полиномиальное время, то $P = NP$.

Существует другая задача разрешения — задача об эйлеровом цикле, которая, несмотря на поверхностное сходство с задачей о гамильтоновом цикле, имеет совершенно другие свойства. Эйлеров цикл — это цикл в графике, в котором каждое ребро проходится ровно один раз. Задача об эйлеровом цикле (ЕС) состоит в том, что для данного графа G с n вершинами надо выяснить, есть ли у него эйлеров цикл. Таким образом, формулировка у задачи ЕС такая же, как у НС, только с заменой вершин на ребра. А теперь давайте посмотрим на следующую замечательную теорему, которую мы предложим вам доказать в упражнении 3.20.

Теорема 3.1 (теорема Эйлера). Связный график содержит эйлеров цикл тогда и только тогда, когда из каждой вершины исходит четное число ребер. Теорема Эйлера дает нам метод эффективного решения задачи ЕС. Во-первых, надо проверить, является ли график связным; это легко сделать за $O(n^2)$ операций (см. упр. 3.19). Если график не связан, то, очевидно, что эйлерова цикла нет. Если график связан, то для каждой вершины надо проверить, четно ли число исходящих из нее ребер. Если найдена вершина, для которой это не так, то эйлерова цикла нет, в противном случае он существует. Поскольку в графике n вершин и не более $n(n - 1)/2$ ребер, этот алгоритм использует $O(n^3)$ элементарных операций. Следовательно, задача ЕС принадлежит классу P! В задаче обхода ребер скрыта какая-то структура, которой можно воспользоваться для

создания эффективного алгоритма, решающего задачу ЕС, но в задаче обхода вершин такой структуры по-видимому, нет. Совершенно не очевидно, почему такая структура есть в одной задаче и нет в другой (если, конечно, в задаче НС ее действительно нет).

Упражнение 3.19. Задача о достижимости состоит в том, что надо выяснить, существует ли путь, соединяющий две данные вершины графа. Покажите, что задачу достижимости можно решить за $O(n)$ операций, если граф содержит n вершин.⁴ Воспользуйтесь решением задачи о достижимости для доказательства того, что можно за $O(n^2)$ операций выяснить, связан ли граф.

Упражнение 3.20 (теорема Эйлера). Докажите теорему Эйлера. Для случая, когда из каждой вершины выходит четное число ребер, дайте конструктивную процедуру нахождения эйлерова цикла.

Эквивалентность задачи о существовании делителя и задачи о разложении на множители (задачи факторизации целого числа) является частным случаем одного из наиболее важных понятий в теории сложности, а именно понятия *сводимости*. Интуитивно мы понимаем, что некоторые задачи являются частными случаями других задач. Менее тривиальный пример сводимости — это сведение задачи НС к задаче коммивояжера (TSP — «traveling salesman problem»). Задача коммивояжера состоит в следующем: дано n городов $1, 2, \dots, n$, расстояния между которыми (обозначим их d_{ij}) являются целыми неотрицательными числами. Для данного числа d надо выяснить, существует ли обход всех этих городов, общая длина которого меньше d .

Сведение задачи НС к задаче TSP осуществляется следующим образом. Пусть у нас есть граф с n вершинами. Будем считать, что каждая вершина — это город, что расстояние d_{ij} между городами i и j равно единице, если вершины i и j соединены, и двум, если они не соединены. Тогда любой обход этих городов, длина которого меньше $n + 1$, — это в точности гамильтонов цикл. Следовательно, если у нас есть алгоритм для решения задачи TSP, мы можем переделать его в алгоритм для решения задачи НС без больших дополнительных затрат. Это и есть пример *сводимости*: мы свели задачу НС к задаче TSP. Сводимостью мы будем пользоваться на протяжении всей книги.

Более общее понятие сводимости проиллюстрировано на рис. 3.11. Говорят, что язык B сводится к языку A , если существует такая машина Тьюринга R , работающая полиномиальное время, что $x \in B$ тогда и только тогда, когда $R(x) \in A$ (здесь $R(x)$ — результат применения машины R к слову x). Таким образом, если у нас имеется алгоритм, распознающий язык A , то за счет небольших дополнительных затрат мы можем распознать и язык B . В этом смысле язык B является по существу не труднее языка A .

⁴ Утверждение сформулировано неверно: количество ребер в графе может быть $\Omega(n^2)$. Выполните это упражнение, полагая, что n — размер представления графа (скажем сумма числа вершин и ребер). При этом связность графа также проверяется за $O(n)$ операций — *Прим. ред.*

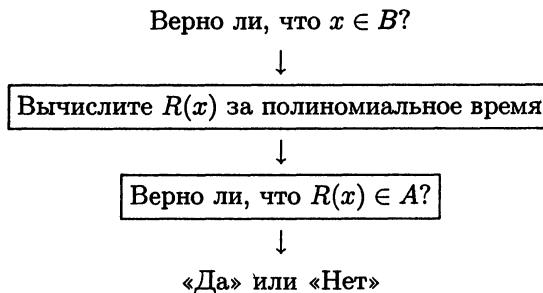


Рис. 3.11. Сводимость языка B к языку A .

Упражнение 3.21 (транзитивность сводимости). Покажите, что если язык L_1 сводится к языку L_2 , а язык L_2 сводится к языку L_3 , то язык L_1 сводится к языку L_3 .

В некоторых классах сложности есть задачи, являющиеся *полными* по отношению к этим классам; это означает, что в данном классе содержится язык L , являющийся в нем «наиболее трудным» для распознавания в том смысле, что любой другой язык в этом классе сводится к L . Не во всяком классе сложности существует полная задача, но многие из тех классов, которые мы будем рассматривать, этим свойством обладают. Тривиальный пример — класс **P**. Пусть L — любой язык в классе **P**, не являющийся пустым и не совпадающий с множеством всех слов (т. е. существует слово x_1 , не принадлежащее L , и слово x_2 , принадлежащее L). Тогда любой другой язык L' из класса **P** можно свести к L , используя для данного слова x процедуру, работающую полиномиальное время, для того, чтобы выяснить, лежит ли x в L' . Если нет, положить $R(x) = x_1$, если да, положить $R(x) = x_2$.

Упражнение 3.22. Предположим, что язык L полон в некотором классе сложности и что L' — другой язык в том же классе, причем L сводится к L' . Покажите, что L' также полон в этом классе.

Менее тривиальным обстоятельством является то, что класс **NP** также содержит полные задачи. Важным примером такой задачи (и прототипом для всех остальных **NP**-полных задач) является *задача выполнимости схемы*, сокращенно называемая **CSAT**: пусть дана булева схема, состоящая из элементов AND, OR и NOT; существуют ли значения входов, при которых на выходе получится 1, или, другими словами, *выполнима* ли схема на каком-нибудь входе? Утверждение о **NP**-полноте задачи **CSAT** известно как *теорема Кука–Левина*; дадим набросок ее доказательства.

Теорема 3.2 (Кука–Левина). Задача **CSAT** является **NP**-полной.

Доказательство состоит из двух частей. В первой части мы показываем, что задача **CSAT** принадлежит классу **NP**, а во второй — что любой язык класса **NP** можно свести к **CSAT**. Обе части доказательства основаны на технике

моделирования: в первой части мы по существу показываем, что машина Тьюринга может эффективно моделировать схему, а во второй — что схема может эффективно моделировать машину Тьюринга. Обе части доказательства проводятся довольно просто; для иллюстрации вторую часть мы излагаем более или менее подробно.

Итак, в первой части доказательства покажем, что задача CSAT принадлежит NP. В самом деле, если дана схема из n элементов и потенциальное свидетельство выполнимости w (набор значений входных переменных), то, очевидно, можно проверить на машине Тьюринга за полиномиальное время, выполнима ли схема на входе w , откуда и следует, что CSAT принадлежит NP.

Во второй части доказательства покажем, что любой язык $L \in NP$ можно свести к CSAT. Другими словами, мы хотим доказать, что существует такое сведение R , вычислимое за полиномиальное время, что $x \in L$ тогда и только тогда, когда схема $R(x)$ выполнима. Идея доказательства — построить схему, моделирующую машину Тьюринга M , которая проверяет пары (x, w) («слово-свидетельство») для языка L . Входные переменные схемы будут представлять свидетельство w ; при этом выполнимость схемы будет равносильна тому, что, машина M принимает пары (x, w) для некоторого w .

Без потери общности, можно предположить следующее:

1. Алфавит машины M состоит из символов $>$, $0, 1$ и пробела.
2. Время работы машины M не превышает $t(n)$, и используется память, не превосходящая $s(n)$, где $t(n)$ и $s(n)$ — полиномы от n .
3. На всех входных словах длины n время работы машины M точно равно $t(n)$. Чтобы добиться этого нужно добавить строки вида $\langle q_Y, x, q_Y, x, 0 \rangle$ и $\langle q_N, x, q_N, x, 0 \rangle$ для всех x из алфавита и принудительно остановить машину после $t(n)$ тактов работы.

Идея, на которой основана имитация работы машины M с помощью схемы, проиллюстрирована на рис. 3.12. Каждое внутреннее состояние машины Тьюринга представлено одним битом; обозначим эти биты $\tilde{q}_s, \tilde{q}_1, \dots, \tilde{q}_m, \tilde{q}_Y, \tilde{q}_N$. Первоначально бит \tilde{q}_s установлен в единицу, а все остальные биты, представляющие внутренние состояния, равны нулю. Каждая ячейка на ленте содержит три бита: два из них представляют символ из алфавита ($>$, $0, 1$ или пробел), записанный в эту ячейку, третий является флагом, равным единице, если головка находится над ячейкой, и нулю в противном случае. Биты, представляющие содержимое ленты, будем обозначать $(u_0, v_0), \dots, (u_{s(n)}, v_{s(n)})$, а соответствующие флаги как $f_0, \dots, f_{s(n)}$. Существует также еще один бит F , называемый глобальным флагом, смысл которого будет объяснен позже. Первоначально F равен нулю. Все входные биты мы рассматриваем как фиксированные, за исключением битов, представляющих слово-свидетельство w .

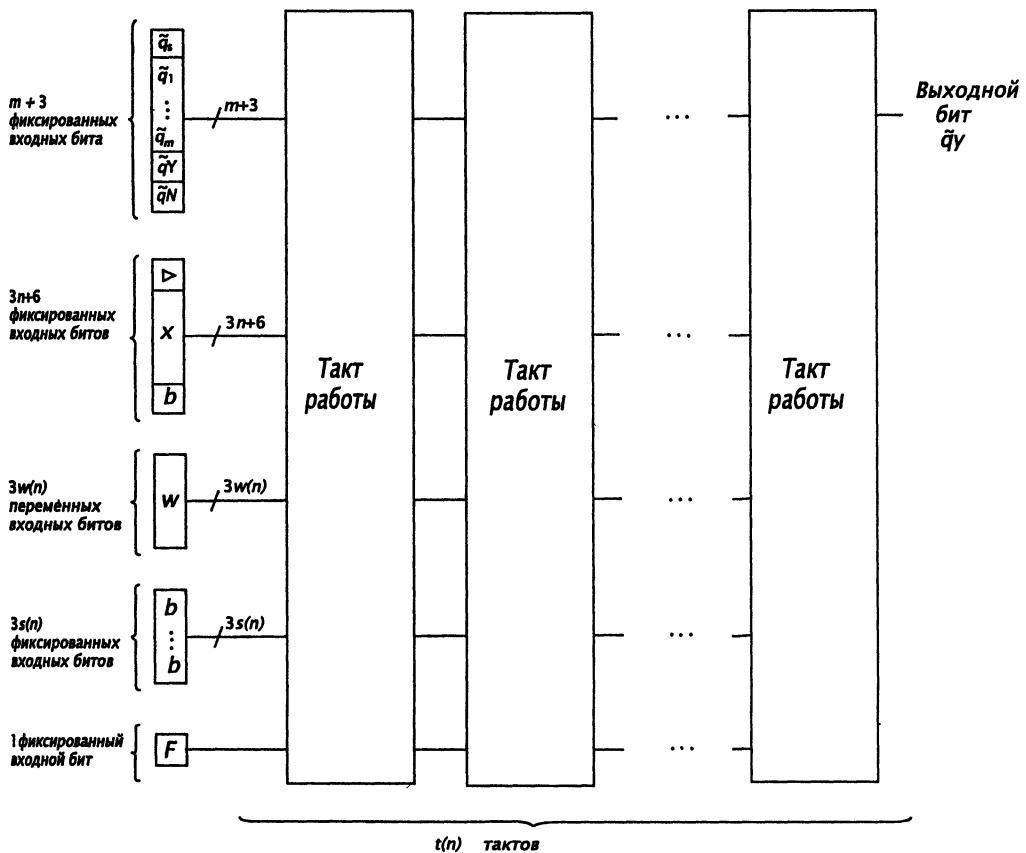


Рис. 3.12. Имитация машины Тьюринга с помощью схемы

В схеме, имитирующей работу машины M , $t(n)$ раз повторяются фрагменты, каждый из которых имитирует один такт работы машины Тьюринга. Каждый такой фрагмент можно разбить на последовательность шагов, каждый из которых соответствует одной программной строке; в конце этой последовательности глобальный флаг F устанавливается в нуль, как показано на рис. 3.13.



Рис. 3.13. Схема, имитирующая один такт работы машины Тьюринга

Чтобы завершить описание, нужно только объяснить, как именно программа строка $\langle q_i, x, q_j, x', s \rangle$ обрабатывается схемой. Предположим для удобства,

что $q_i \neq q_j$ (аналогичная конструкция работает и при $q_i = q_j$). Итак, здесь нужно выполнить следующие действия:

- (1) Проверить, что $\tilde{q}_i = 1$ (это указывает на то, что текущее состояние машины есть q_i).
- (2) Для каждой ячейки ленты:
 - (а) проверить, что глобальный флаг установлен в нуль (это означает, что машина Тьюринга еще ничего не сделала для выполнения данной программной строки);
 - (б) проверить, что флаг, соответствующий этой ячейке, установлен в единицу (это указывает на то, что головка находится над данной ячейкой);
 - (в) проверить, что содержимое этой ячейки есть x ;
 - (г) если все вышеперечисленные условия выполнены, то
 - 1) установить $\tilde{q}_i = 0$ и $\tilde{q}_j = 1$,
 - 2) установить содержимое ячейки в x' ,
 - 3) обновить флаги данной и двух соседних ячеек в зависимости от значения s (+1, 0, -1) и от того, находимся ли мы на краю ленты,
 - 4) установить глобальный флаг в единицу, что указывает на то, что данный тик вычислений завершен.

Описанная в п. (2) процедура оперирует с фиксированным числом битов; ввиду установленного в подразд. 3.1.2 результата об универсальности эта процедура может быть реализована с помощью схемы с фиксированным числом используемых элементов.

Легко видеть, что общее число элементов в схеме есть $O(t(n)(s(n) + n))$, т. е. полиномиально. Ясно, что $\tilde{q}_Y = 1$ тогда и только тогда, когда машина M принимает (x, w) . Таким образом, схема выполнима тогда и только тогда, когда M принимает (x, w) , и мы нашли искомое сведение L к CSAT.

Задача CSAT открывает нам легкий путь к доказательству NP-полноты многих других задач. Вместо того, чтобы доказывать NP-полноту какой-либо задачи непосредственно, мы можем просто установить, что она принадлежит NP и что задача CSAT к ней сводится. Тогда ввиду упражнения 3.22 наша задача также будет NP-полной. Небольшая подборка NP-полных задач приводится во вставке 3.3. Примером еще одной NP-полной задачи является задача выполнимости (SAT), формулируемая в терминах булевых формул. Напомним, что булева формула φ строится из следующих элементов: булевых переменных x_1, x_2, \dots , булевых связок, т. е. булевых функций \wedge (AND), \vee (OR) и \neg (NOT), и скобок. Истинность или ложность булевой формулы при данных значениях булевых переменных устанавливается по обычным правилам булевой алгебры. Например, формула $\varphi = x_1 \vee \neg x_2$ выполняется при $x_1 = 0$

и $x_2 = 0$ и не выполняется при $x_1 = 0$ и $x_2 = 1$. Задача выполнимости состоит в том, чтобы установить, будет ли данная булева формула φ истинной при каких-нибудь значениях переменных.

Упражнение 3.23. Покажите, что задача SAT NP-полна, доказав, что она принадлежит NP и что CSAT к ней сводится. (Указание. Для сведения может быть полезно представить каждый провод в виде отдельной переменной в булевой формуле.)

Важным частным случаем задачи SAT также является NP-полная задача 3-выполнимости (3SAT), относящаяся к формулам в 3-конъюнктивной нормальной форме. Говорят, что формула представлена в конъюнктивной нормальной форме, если она является конъюнкцией набора дизъюнктов, каждый из которых в свою очередь представляет собой дизъюнкцию одного или нескольких литералов, где литерал — выражение вида x или $\neg x$. Например, формула $(\neg x_1 \vee x_2 \vee x_3) \wedge (\neg x_1 \vee x_3 \vee \neg x_4) \wedge (x_2 \vee x_3 \vee x_4)$ представлена в 3-конъюнктивной нормальной форме. Задача 3-выполнимости состоит в том, чтобы выяснить, выполнима ли данная формула, представленная в 3-конъюнктивной нормальной форме.

Доказательство того, что задача 3SAT является NP-полной, проводится непосредственно, но оно слишком длинное, чтобы можно было включить его в этот обзор. Задача 3SAT является в некотором смысле NP-полной задачей даже в большей степени, чем CSAT и SAT, и именно на ее NP-полноте основаны бесчисленные доказательства NP-полноты конкретных задач. Мы завершим наше обсуждение NP-полноты тем удивительным фактом, что задача 2SAT, аналог 3SAT, в которой каждый дизъюнкт состоит из двух литералов, разрешима за полиномиальное время.

Упражнение 3.24 (у задачи 2SAT есть эффективное решение). Пусть φ — булева формула в конъюнктивной нормальной форме, в которой каждый дизъюнкт содержит только два литерала.

- (1) Постройте ориентированный граф $G(\varphi)$ следующим образом. Вершины G соответствуют переменным x_i и их отрицаниям $\neg x_i$; ребро соединяет α и β тогда и только тогда, когда φ содержит дизъюнкт вида $(\neg \alpha \vee \beta)$ или $(\beta \vee \neg \alpha)$. Покажите, что φ не является выполнимой тогда и только тогда, когда для некоторой переменной x в графе G существует как путь из x в $\neg x$, так и путь из $\neg x$ в x .
- (2) Докажите, что для данного ориентированного графа с n вершинами можно за полиномиальное время выяснить, существует ли путь из данной вершины v_1 в данную вершину v_2 .
- (3) Постройте эффективный алгоритм, решающий задачу 2SAT.

Если предположить, что $P \neq NP$, то можно доказать, что существует *непустой* класс NPI, состоящий, по определению, из задач, не являющихся ни разрешимыми за полиномиальное время, ни NP-полными. Разумеется, ни про одну задачу не доказано, что она принадлежит классу NPI (иначе мы знали

Вставка 3.3. Примеры NP-полных задач

Класс **NP** важен, в частности, и потому, что огромное количество задач принадлежит этому классу. Мы даже и не пытаемся дать здесь полный обзор (см. раздел «История и дополнительная литература»); приводимые ниже примеры, взятые из многих различных разделов математики, дают представление о необычайном разнообразии NP-полных задач.

- **ЗАДАЧА О КЛИКЕ** (*теория графов*). Кликой в (неориентированном) графе G называется множество вершин, каждая пара из которых соединена ребром; число вершин в этом множестве называется *размером клики*. Дано целое число t и граф G ; содержит ли G клику размера t ?
- **ЗАДАЧА О СУММАХ ПОДМНОЖЕСТВ** (*арифметика*). Дано конечное множество S , состоящее из целых положительных чисел, и число t . Существует ли в S подмножество, сумма элементов которого равна t ?
- **0–1 ЦЕЛОЧИСЛЕННОЕ ПРОГРАММИРОВАНИЕ** (*линейное программирование*). Даны целочисленная $(m \times n)$ -матрица A и m -мерный целочисленный вектор y ; существует ли такой n -мерный вектор x , координаты которого принадлежат множеству $\{0, 1\}$, что $Ax \leqslant y$?
- **ВЕРШИННОЕ ПОКРЫТИЕ** (*теория графов*). *Вершинным покрытием* неориентированного графа G называется такое множество вершин V' , что у каждого ребра хотя бы одна вершина содержится в V' . Для данных целого числа t и графа G существует ли у графа G вершинное покрытие, содержащее t вершин?

бы, что $P \neq NP$), но есть несколько задач, считающихся кандидатами на принадлежность к этому классу. Два наиболее вероятных кандидата — это задача о существовании делителя и задача об изоморфизме графов.

ЗАДАЧА ОБ ИЗОМОРФИЗМЕ ГРАФОВ. Пусть G и G' — неориентированные графы с множеством вершин $V = \{v_1, \dots, v_n\}$. Являются ли графы G и G' изоморфными? Другими словами, существует ли такое взаимно однозначное отображение $\varphi: V \rightarrow V'$, что ребро (v_i, v_j) содержится в G тогда и только тогда, когда ребро $(\varphi(v_i), \varphi(v_j))$ содержится в G' ?

Задачи класса **NPI** интересны для специалистов по квантовым вычислениям и квантовой теории информации по двум причинам. Во-первых, желательно найти быстрые квантовые алгоритмы для задач, не принадлежащих P . Во-вторых, многие считают, что квантовые компьютеры не смогут эффективно решать все задачи из класса NP , включая NP -полные задачи. Поэтому естественно сосредоточиться на классе **NPI**. И действительно быстрый квантовый алгоритм разложения на множители найден (гл. 5), что побуждает искать

быстрые квантовые алгоритмы для других задач, предположительно принадлежащих NP.

3.2.4 Другие классы сложности

Мы рассмотрели элементарные свойства некоторых классов сложности. На самом деле этих классов очень много, и между ними имеется множество доказанных или гипотетических нетривиальных соотношений. Для исследователей в области квантовых вычислений и квантовой теории информации нет необходимости знать все различные классы сложности, но важно иметь представление о наиболее важных из них, у многих из которых есть квантовые аналоги. Далее, если мы хотим выяснить вычислительные возможности квантовых компьютеров, то надо понять, как класс задач, разрешимых на квантовых компьютерах, вписывается в иерархию классов сложности, определенных для классических компьютеров.

При определении классов сложности можно учитывать три параметра: интересующий нас ресурс (время, память...), тип рассматриваемых задач (задачи разрешения, задачи оптимизации...) и используемая вычислительная модель (детерминированная машина Тьюринга, вероятностная машина Тьюринга, квантовый компьютер...). Не удивительно, что при этом получаются определения огромного числа классов сложности. В этом разделе мы коротко обсудим несколько наиболее важных из них, а также их элементарные свойства. Начнем мы с класса сложности, получаемого, если задать ограничения не на время, а на *память*.

Наиболее естественный из классов сложности, определяемых с использованием ограничений на память, — это класс **PSPACE**, состоящий из задач разрешения, которые могут быть решены на машине Тьюринга с учетом полиномиального количества рабочих битов, но без ограничений на время работы (см. упр. 3.25). Очевидно, что **P** содержится в **PSPACE**, поскольку машина Тьюринга, останавливающаяся за полиномиальное время, может использовать только полиномиальное количество ячеек. Кроме того, в **PSPACE** также содержится класс **NP**. В самом деле, пусть L — язык класса **NP**. Предположим, что у задач размера n имеется свидетельство размера, не превосходящего $p(n)$, где $p(n)$ — полином от n .⁵ Чтобы выяснить, есть ли у задачи решение, можно последовательно проверить все $2^{p(n)}$ возможных свидетельств. Каждая проверка может быть проведена за полиномиальное время, и тем самым с использованием полиномиальной памяти. Если будем стирать все промежуточные вычисления перед очередной проверкой, то проверим все возможности, используя лишь полиномиальную память.

К сожалению, в настоящее время неизвестно даже, содержит ли **PSPACE** задачи, не принадлежащие **P**! Эта ситуация весьма замечательна: представляется совершенно очевидным, что неограниченные временные ресурсы и поли-

⁵ Хорошим упражнением будет доказательство существования такого короткого свидетельства: ведь в данном выше определении класса **NP** ничего не говорится о длине записи свидетельства. — Прим. ред.

номиальная память дают нам большую вычислительную эффективность, чем полиномиальное время. Однако, несмотря на серьезные усилия и изобретательность, проявленные различными исследователями, это так и не было доказано! В дальнейшем мы увидим, что класс задач, разрешимых на квантовом компьютере за полиномиальное время, содержится в **PSPACE**, так что доказательство того, что некоторая задача, эффективно разрешимая на квантовом компьютере, неразрешима при использовании классического компьютера, показало бы, что $P \neq PSPACE$ и тем самым решило бы одну из важнейших проблем информатики. С оптимистической точки зрения это означает, что идеи квантовой теории вычислений могут быть использованы для доказательства того, что $P \neq PSPACE$. С пессимистической точки зрения можно заключить, что еще нескоро удастся строго доказать, что квантовые компьютеры могут эффективно решать задачи, практически неразрешимые на классическом компьютере. Если быть еще большим пессимистом, то можно предположить, что $P = PSPACE$. В этом случае у квантовых компьютеров вообще нет никаких преимуществ перед классическими! Однако, вряд ли кто-нибудь из специалистов по теоретической информатике считает, что $P = PSPACE$.

Упражнение 3.25 ($PSPACE \subseteq EXP$). Класс сложности **EXP** (задачи, разрешимые за экспоненциальное время) состоит из задач разрешения, которые могут быть решены на машине Тьюринга за время $O(2^{n^k})$, где k — какая-либо константа. Докажите, что $PSPACE \subseteq EXP$. (Указание. Если машина Тьюринга использует l внутренних состояний, алфавит из t букв и память размера $p(n)$, то общее число ее состояний не превышает $l t p^{(n)}$, а так как она не зацикливается, то не может попасть в одно и то же состояние дважды.)

Упражнение 3.26 ($L \subseteq P$). Класс сложности **L** (логарифмическая память) состоит из задач разрешения, которые могут быть решены на машине Тьюринга с использованием логарифмической памяти, т. е. памяти размера $O(\log n)$. Точнее говоря, класс **L** определяется с помощью двухленточной машины Тьюринга. Одна лента содержит входные данные (размера n) и на нее нельзя ничего записывать; допустимы только программные строки, не меняющие ее содержимого. Другая лента — это рабочая лента, изначально содержащая только пробелы; требование логарифмической памяти накладывается только на эту рабочую ленту. Покажите, что $L \subseteq P$.

Повысится ли эффективность вычислений, если разрешить использовать больше времени или больше памяти? Ответ на этот вопрос положителен в обоих случаях. Грубо говоря, *теорема о временной иерархии* утверждает, что класс $\text{TIME}(f(n))$ является собственным подклассом $\text{TIME}(f(n) \log^2 f(n))$. Аналогичным образом *теорема об иерархии по памяти* гласит, что класс $\text{SPACE}(f(n))$ является собственным подклассом $\text{SPACE}(f(n) \log f(n))$, где, конечно, $\text{SPACE}(f(n))$ — это класс языков, распознаваемых на памяти $O(f(n))$. Эти теоремы об иерархии имеют интересные следствия, касающиеся отношений между сложностными классами. Известно, что

$$L \subseteq P \subseteq NP \subseteq PSPACE \subseteq EXP. \quad (3.1)$$

К сожалению, хотя общепринято, что каждое из этих включений является

строгим, ни про одно из них это не доказано. Однако из теоремы о временной иерархии следует, что P является собственным подклассом EXP , а из теоремы об иерархии по памяти следует, что L является собственным подклассом PSPACE ! Таким образом, можно заключить, что хотя бы одно из включений в (3.1) является строгим, хотя мы и не знаем, какое именно.

Что можно сделать с задачей, про которую мы знаем, что она является NP -полной (или выполняется какой-либо другой критерий трудности)? Оказывается, что на этом анализ задачи далеко не кончается. Один из возможных подходов заключается в том, чтобы выделить частные случаи задачи, которые можно все-таки эффективно решить. В упр. 3.24 мы видели, что задача 2SAT имеет эффективное решение, несмотря на то, что задача SAT является NP -полной. Другой подход состоит в том, чтобы изменить трактовку понятия «решение задачи» — при этом обычно получаются определения новых классов сложности. Например, вместо точного решения NP -полной задачи можно искать ее *приближенное решение*. Например, задача о вершинном покрытии является NP -полной. Однако в упр. 3.27 мы показываем, что можно эффективно найти вершинное покрытие, в котором количество вершин не более чем вдвое превышает количество вершин в оптимальном вершинном покрытии. С другой стороны, в задаче 3.6 мы покажем, что для задачи коммивояжера невозможно найти приближенное решение, отличающееся от оптимального не более, чем на любой фиксированный множитель (если, конечно, $P \neq \text{NP}$).

Упражнение 3.27 (приближенное решение задачи о вершинном покрытии). Пусть $G = (V, E)$ — неориентированный граф. Докажите, что приведенный ниже алгоритм находит вершинное покрытие для G , число вершин в котором не более, чем вдвое превосходит минимально возможное.

```

 $VC = \emptyset$ 
 $E' = E$ 
do until  $E' = \emptyset$ 
    пусть  $(\alpha, \beta)$  — произвольное ребро из  $E'$ 
     $VC = VC \cup \{\alpha, \beta\}$ 
    удалить из  $E'$  все ребра, инцидентные  $\alpha$  или  $\beta$ 
return  $VC$ 
```

Почему у одних NP -полных задач приближенные решения существуют, а у других — нет? Ведь, казалось бы, возможно эффективное сведение одних задач к другим? Это, бесспорно, так, но сведение не обязательно переводит хорошие приближения в хорошие. В результате анализ приближенных алгоритмов для задач из класса NP оказывается более сложным. На эту тему существует целая теория, которая, к сожалению, выходит за рамки нашей книги. Основная идея тут в том, чтобы определить новое понятие сводимости, при котором сохраняются хорошие приближения. Имея в виду такую сводимость, можно определить класс сложности MAXSNP , аналогичный классу NP , как множество задач, для которых можно эффективно проверить приближенное решение. Для класса MAXSNP , как и для NP , существуют полные задачи;

интересный открытый вопрос — выяснить, как класс **MAXSNP** соотносится с классом задач, для которых имеется эффективное приближенное решение.

Мы завершим наше обсуждение примером класса сложности, определение которого основано на измененной вычислительной модели. Предположим, что машина Тьюринга наделена способностью бросать монету и использовать результат такого бросания для того, чтобы решать, какое действие произвести в процессе вычислений. Такая машина Тьюринга может принимать или отвергать входные данные только с некоторой вероятностью. Класс сложности **BPP** (*вероятностные вычисления, за полиномиальное время и с ограниченными ошибками*) состоит из языков L , для которых существует такая вероятностная машина Тьюринга M , что при $x \in L$ она принимает x с вероятностью не менее $3/4$, а при $x \notin L$ отвергает x с вероятностью не менее $3/4$ (за полиномиальное время в обоих случаях). Следующее упражнение показывает, что выбор $3/4$ в качестве константы по существу произволен.

Упражнение 3.28 (независимость класса BPP от выбора константы). Пусть k — фиксированное число, $1/2 < k \leq 1$, и пусть язык L таков, что существует машина Тьюринга M , которая при $x \in L$ принимает x с вероятностью не менее k , а при $x \notin L$ отвергает x с вероятностью не менее k (за полиномиальное время в обоих случаях). Покажите, что $L \in \text{BPP}$.

На самом деле *неравенство Чернова*, обсуждаемое во вставке 3.4, показывает, что после нескольких повторений алгоритма, распознающего язык из класса **BPP**, вероятность успеха может быть увеличена до значения, которое для всех практических целей можно считать равным единице. По этой причине класс **BPP** можно даже в большей степени, чем класс **P**, считать классом задач, эффективно разрешимых на классическом компьютере, и именно квантовый аналог класса **BPP**, известный как **BQP**, будет нам наиболее интересен при изучении квантовых алгоритмов.

3.2.5 Вычисления и энергия

Теория сложности вычислений изучает, сколько времени и памяти тратится на решение вычислительной задачи. Другой важный вычислительный ресурс — это *энергия*. В этом подразделе мы изучим, сколько энергии требуется для вычислений. Удивительно, что вычисления (как классические, так и квантовые) можно в принципе проводить без энергетических затрат! Потребление энергии при вычислениях оказывается глубоко связанным с *обратимостью* вычислений. Рассмотрим элемент, например **NAND**, получающий на вход два бита и выдающий один бит на выходе. Этот элемент по сути своей *необратим*, поскольку вход невозможно однозначно определить по выходу. Если, например, на выходе получена 1, на входе могло быть и 00, и 10, и 01. С другой стороны, **NOT** — пример *обратимого* элемента, поскольку по его выходу можно определить, каков был вход.

Другой способ представлять себе необратимость — это рассматривать ее в терминах уничтожения информации. Если логический элемент необратим, то

Вставка 3.4. ВРР и неравенство Чернова

Пусть у нас есть алгоритм, дающий правильный ответ с вероятностью $1/2 + \varepsilon$ и неверный ответ с вероятностью $1/2 - \varepsilon$. Если запустить этот алгоритм n раз, то представляется естественным, что правильный ответ — этот тот, который появляется наиболее часто. Насколько надежна эта процедура? *Неравенство Чернова* — это простой результат из элементарной теории вероятностей, дающий ответ на этот вопрос.

Теорема 3.3 (Неравенство Чернова). Пусть X_1, \dots, X_n — независимые и одинаково распределенные случайные величины, каждая из которых принимает значение 1 с вероятностью $1/2 + \varepsilon$ и значение 0 с вероятностью $1/2 - \varepsilon$. Тогда

$$p\left(\sum_{i=1}^n X_i \leq n/2\right) \leq e^{-2\varepsilon^2 n} \quad (3.2)$$

Доказательство.

Рассмотрим произвольную последовательность (x_1, \dots, x_n) , содержащую не более $n/2$ единиц. Вероятность появления такой последовательности максимальна, когда она содержит $\lfloor n/2 \rfloor$ единиц, так что

$$p(X_1 = x_1, \dots, X_n = x_n) \leq \left(\frac{1}{2} - \varepsilon\right)^{\frac{n}{2}} \left(\frac{1}{2} + \varepsilon\right)^{\frac{n}{2}} \quad (3.3)$$

$$= \frac{(1-4\varepsilon^2)^{\frac{n}{2}}}{2^n} \quad (3.4)$$

Число таких последовательностей не превышает 2^n , так что

$$p\left(\sum_{i=1}^n X_i \leq n/2\right) \leq 2^n \times \frac{(1-4\varepsilon^2)^{\frac{n}{2}}}{2^n} = (1-4\varepsilon^2)^{\frac{n}{2}} \quad (3.5)$$

Наконец, из математического анализа известно, что $1 - x \leq \exp(-x)$, так что

$$p\left(\sum_{i=1}^n X_i \leq n/2\right) \leq e^{-4\varepsilon^2 n/2} = e^{-2\varepsilon^2 n} \quad (3.6)$$

Все это говорит о том, что для фиксированного ε вероятность ошибки экспоненциально убывает с ростом числа повторений алгоритма. В случае ВРР имеем $\varepsilon = 1/4$, так что после всего лишь нескольких сотен повторений вероятность ошибки будет меньше, чем 10^{-20} , и тут уже ошибки в работе компьютера становятся более значимыми, чем ошибки, обусловленные вероятностным характером алгоритма.

часть информации, подаваемой на его вход, безвозвратно пропадает в результате его работы, т. е. уничтожается этим элементом. При обратимых вычислениях, напротив, никакая информация не уничтожается, поскольку вход всегда может быть восстановлен по выходу. Другими словами, обратимое вычисление — это вычисление, не уничтожающее информацию.

Как связаны потребление энергии и необратимость вычислений? Эта связь описывается *принципом Ландауэра*, утверждающим, что при уничтожении информации неизбежно происходит диссипация энергии. Точнее говоря, принцип Ландауэра можно сформулировать следующим образом.

Принцип Ландауэра (первая форма). При стирании компьютером одного бита информации в окружающую среду неминуемо диссирирует энергия в количестве, не меньшем, чем $k_B T \ln 2$, где k_B — универсальная константа, известная как *постоянная Больцмана*, а T — температура окружающей среды.

С помощью законов термодинамики принципу Ландауэра можно придать другую форму с использованием энтропии, а не энергии.

Принцип Ландауэра (вторая форма). При стирании компьютером одного бита информации энтропия окружающей среды возрастает не менее, чем на $k_B \ln 2$, где k_B — постоянная Больцмана.

Обоснование принципа Ландауэра — это физическая задача, выходящая за рамки нашей книги (см. по этому поводу раздел «История и дополнительная литература» в конце главы). Если, однако, принять принцип Ландауэра как данность, то возникает целый ряд интересных вопросов. Прежде всего принцип Ландауэра дает только *нижнюю границу* для количества энергии, диссирируемой при уничтожении информации. Насколько существующие компьютеры близки к этой границе? Оказывается не очень близки: компьютеры 2000 г. диссирируют энергию в размере примерно $500 k_B T \ln 2$ на каждую логическую операцию.

Хотя существующие компьютеры и далеки от границы Ландауэра, проблема сокращения энергопотребления является принципиальной и интересной, причем наряду с теоретическим интересом есть и практический интерес: если производительность компьютеров будет возрастать согласно закону Мура, то будет возрастать и количество диссирируемой энергии, если только величина энергии, диссирируемой за одну операцию, не будет уменьшаться по меньшей мере с той же скоростью, с какой растет производительность компьютеров.

Если бы все вычисления производились обратимым образом, то из принципа Ландауэра не следовала бы диссипация энергии, поскольку никакая информация при таком вычислении не уничтожается. Конечно, не исключено, что потери энергии при вычислениях могут быть неизбежны ввиду какого-то другого физического принципа; к счастью, оказывается, что это не так. Но возможно ли проводить универсальные вычисления без потери информации? Физики могут схитрить, сказав, что ответ на этот вопрос *должен* быть положительным, поскольку согласно нашему современному пониманию физических законов они в основе своей обратимы. Зная начальное состояние замкнутой

физической системы, на основе законов физики можно определить начальное состояние системы. Если мы верим в эти законы, то должны заключить, что в необратимых логических элементах, таких как AND или OR, скрыты какие-то обратимые вычисления. Но где же она, эта скрытая обратимость, и можно ли ее использовать для построения явным образом обратимых компьютеров?

Для реализации обратимых универсальных вычислений, мы будем использовать модели двух типов. Первая модель — компьютер, построенный из биллиардных шаров и стенок, — обеспечивает красивую конкретную реализацию принципов обратимых вычислений. Вторая модель, основанная на обратимом логическом элементе, известном как элемент *Тоффоли* (с которым мы впервые встретились в подразд. 1.4.1), реализует более абстрактный подход к обратимым вычислениям, который будет нам в дальнейшем очень полезен при обсуждении квантовых вычислений. Возможно также построить обратимые машины Тьюринга, обладающие свойством универсальности; мы, однако, не будем ими заниматься, поскольку для квантовых вычислений схемные модели оказываются гораздо полезнее.

Основной принцип работы компьютера на биллиардных шарах проиллюстрирован на рис. 3.14. Биллиардные шары вводятся в компьютер слева, отскакивают от стенок и друг от друга и выходят из компьютера справа. Наличие или отсутствие шара в данном месте интерпретируется как логическая единица или нуль соответственно. Эта модель замечательна тем, что она явным образом обратима, поскольку ее работа основана на законах классической механики. Более того, эта модель оказывается *универсальной* в том смысле, что с ее помощью можно имитировать любое вычисление в стандартной схемной модели.

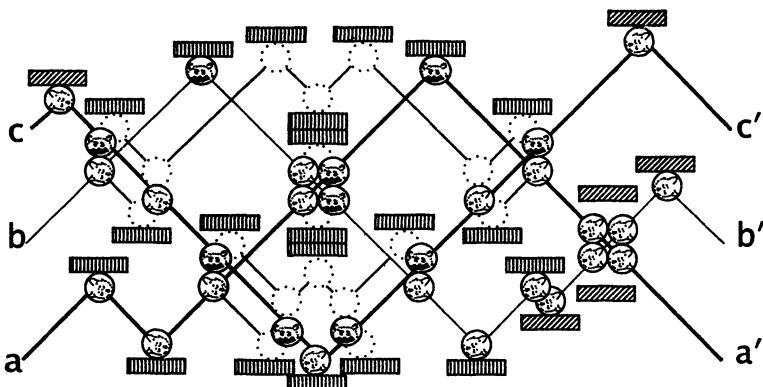


Рис. 3.14. Простой компьютер на биллиардных шарах с тремя входными и тремя выходными битами (входные биты слева, выходные — справа). Наличие или отсутствие шара интерпретируется как 1 или 0 соответственно. Пустые кружки обозначают потенциальные пути. В данном примере реализован классический обратимый элемент Фредкина, обсуждаемый в тексте.

Разумеется, компьютер на биллиардных шарах, если его когда-нибудь построят, окажется весьма неустойчивым. Как подтвердит любой игрок в биллиард, биллиардный шар, катящийся без трения по гладкой поверхности, легко

отклоняется от пути даже при малых возмущениях. Для реализации вычислений на биллиардной модели необходимо ее безупречное функционирование и отсутствие внешних возмущений, вызываемых, например, тепловыми шумами. В противном случае необходимо периодически вносить поправки, а информацию, полученную при этих поправках, надо будет уничтожать, что требует затрат энергии. Затраты энергии необходимы для того, чтобы уменьшить влияние шумов, без чего реальный компьютер работать не может. В нашем изложении мы проигнорируем влияние шумов на биллиардный компьютер и сконцентрируем внимание на основные принципы обратимых вычислений.

a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Рис. 3.15. Таблица значений для элемента Фредкина и его условное обозначение. Биты a и b меняются местами, если управляющий бит c установлен в единицу, в противном случае они не меняются.

С помощью биллиардного компьютера можно элегантно реализовать обратимый универсальный логический элемент, известный как элемент Фредкина, свойства которого хорошо отражают общие принципы обратимых логических элементов и схем. Элемент Фредкина имеет три входных бита a , b и c и три выходных бита a' , b' и c' . Бит c — это *управляющий бит*, значение которого под действием элемента Фредкина не меняется, т. е. $c' = c$. Этот бит называется *управляющим*, поскольку от него зависит, что происходит с остальными двумя битами a и b . Если c равен 0, то a и b не меняются, т. е. $a' = a$, $b' = b$. Если c равен 1, то значения битов a и b обмениваются: $a' = b$, $b' = a$. Таблица значений для элемента Фредкина приведена на рис. 3.15. Легко видеть, что элемент Фредкина обратим, поскольку по выходным битам a' , b' и c' можно определить входные биты a , b и c . Для этого достаточно подать a' , b' и c' на вход еще одного элемента Фредкина.

Упражнение 3.29 (элемент Фредкина обратен самому себе). Покажите, что при последовательном использовании двух элементов Фредкина выход будет совпадать со входом.

Изучая пути биллиардных шаров на рис. 3.14, нетрудно понять, что изображенный на этом рисунке биллиардный компьютер реализует элемент Фредкина:

Упражнение 3.30. Проверьте, что изображенный на рис. 3.14 биллиардный компьютер реализует элемент Фредкина.

В дополнение к обратимости элемент Фредкина обладает еще одним интересным свойством: при его применении число единиц не меняется. В терминах биллиардного компьютера это соответствует тому, что из элемента Фредкина выходит столько же шаров, сколько в него входит. Иногда эту мысль выражают такими словами: элемент Фредкина является *консервативным*. Эти свойства обратимости и консервативности представляют интерес для физиков, поскольку их можно мотивировать с помощью основных физических принципов. Законы природы обратимы (за возможным исключением постулата измерения в квантовой механике, который обсуждался в подразд. 2.2.3). Консервативность логического элемента можно рассматривать как свойство, аналогичное сохранению массы или энергии (в биллиардной модели она в точности соответствует сохранению массы).

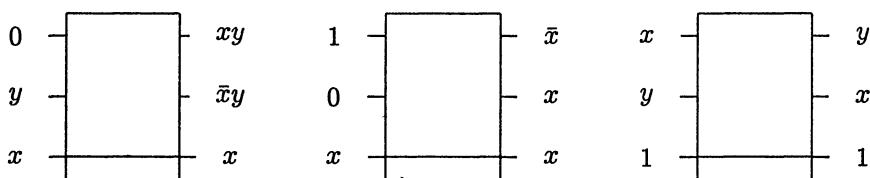


Рис. 3.16. Конфигурации элемента Фредкина эквивалентны элементам AND (слева) и NOT (в центре), а также функции CROSSOVER (справа). Конфигурация, указанная в центре, выполняет также операцию FANOUT, поскольку на выходе выдаются две копии бита x . Обратите внимание, что для каждой из этих операций требуются вспомогательные биты, приготовленные в стандартных состояниях (например, 0 в первой строке элемента AND) и что выход, вообще говоря, содержит «мусор», не нужный для дальнейших вычислений.

Элемент Фредкина не только обратим и консервативен, он является еще и универсальным логическим элементом! Как показано на рис. 3.16, с помощью этого элемента можно реализовать функции AND, NOT, CROSSOVER и FANOUT, так что с помощью комбинации элементов Фредкина можно моделировать любую классическую схему!

Чтобы реализовать с помощью элемента Фредкина необратимые элементы, например AND, использовались две идеи. Во-первых, мы допускаем на входе вспомогательные биты, приготовленные в стандартных состояниях 0 и 1. Во-вторых, на выходе допускаем «мусор», не нужный для дальнейших вычислений. Роль этих мусорных и вспомогательных битов только в том, что они делают вычисление обратимым. В качестве причины необратимости элементов, таких как AND и OR, можно рассматривать то обстоятельство, что в них эти вспомогательные и мусорные биты «спрятаны». Итак, по любой классической схеме, вычисляющей функцию $f(x)$, можно построить обратимую схему, состоящую исключительно из элементов Фредкина, которая, получив на входе x и вспомогательные биты в стандартном состоянии a , вычисляет $f(x)$ и «мусорный» результат $g(x)$. Действие этой схемы можно представить в виде $(x, a) \rightarrow (f(x), g(x))$.

Теперь мы знаем, как вычислять функции обратимым образом. К сожалению, при таком вычислении возникают нежелательные мусорные биты. Если

слегка модифицировать этот метод, то окажется, что можно провести вычисления таким образом, что все мусорные биты окажутся в *стандартном состоянии*. Эта конструкция является ключевой для квантовых компьютеров, поскольку мусорные биты, значения которых зависят от x , будут, вообще говоря, разрушать свойства интерференции, необходимые для квантовых вычислений. Чтобы понять эту конструкцию, удобно предположить, что мы имеем в своем распоряжении элемент NOT, так что можно считать, что все вспомогательные биты равны нулю (для превращения вспомогательных нулей во вспомогательные единицы установим элементы NOTтам, где это необходимо). Удобно также предположить, что в нашем распоряжении есть классический элемент «управляемое NOT», определенный аналогично квантовому определению из подразд. 1.3.2, т. е. этот элемент переводит вход (c, t) в выход $(c, c \oplus t)$, где \oplus обозначает сложение по модулю 2. Отметим, что при $t = 0$ получаем $(c, 0) \rightarrow (c, c)$, так что управляемое NOTможно использовать как обратимый вариант операции FANOUT, не оставляющий мусора на выходе.

Добавив дополнительные элементы NOTна входе, можно записать действие схемы в виде $(x, 0) \rightarrow (f(x), g(x))$. Мы могли бы также добавить на входе схемы элементы CNOT, чтобы создать копию x , сохраняемую в процессе последующих вычислений. С учетом этих модификаций действие схемы можно записать в виде

$$(x, 0, 0) \rightarrow (x, f(x), g(x)). \quad (3.7)$$

Формула (3.7) — это очень удобный способ записи действия обратимой схемы, поскольку она приводит к идею *обращения вычисления*, с помощью которого можно избавиться от мусорных битов за счет небольшого увеличения времени работы. Предположим, что мы имеем четырехрегистровый компьютер с начальным состоянием $(x, 0, 0, y)$. Во втором регистре будет храниться результат вычислений, в третьем — мусорные биты $g(x)$. Зачем нужен четвертый регистр, мы объясним позже, а пока будем считать, что в начальном состоянии в нем хранится произвольная информация y .

Начнем, как и выше, с вычисления f с помощью обратимой схемы, что даст на выходе $(x, f(x), g(x), y)$. Затем воспользуемся элементами CNOT для побитового сложения $f(x)$ с содержимым четвертого регистра, в результате получим состояние $(x, f(x), g(x), y \oplus f(x))$. Однако все этапы вычисления $f(x)$ были обратимы и не затрагивали четвертого регистра, так что применения элементы исходной схемы, использованной для вычисления f , в обратном порядке получим $(x, 0, 0, y \oplus f(x))$. Обычно в таких записях мы будем опускать вспомогательные нули и записывать действие схемы в виде

$$(x, y) \rightarrow (x, y \oplus f(x)) \quad (3.8)$$

Обычно под обратимой схемой, вычисляющей f , мы будем иметь в виду именно эту схему, хотя в принципе существует и много других обратимых схем, с помощью которых можно вычислять f .

Какие дополнительные ресурсы нужны для обратимого вычисления? Чтобы ответить на этот вопрос, нужно сосчитать количество требуемых вспомогательных битов и сравнить количество элементов в обратимой и классической

схемах. Ясно, что число элементов в обратимой схеме то же, что и в классической, с точностью до постоянного множителя, указывающего, сколько элементов Фредкина необходимо для реализации одного элемента в необратимой схеме (этот множитель надо еще умножить на два для учета обращения вычисления), плюс количество элементов CNOT, участвующих в обратимом вычислении, которое линейно зависит от количества битов. Аналогично количество требуемых вспомогательных битов линейно зависит от количества элементов в необратимой схеме, поскольку каждый элемент в необратимой схеме реализуется с помощью постоянного числа вспомогательных битов. В результате, классы сложности P и NP получаются один и те же независимо от того, обратимая или необратимая вычислительная модель используется для их определения. Для других классов сложности, например PSPACE, ситуация не настолько очевидна; см. задачу 3.9 и разд. «История и дополнительная литература» по поводу этих тонкостей.

Упражнение 3.31 (обратимый полусумматор). Постройте обратимую схему, которая, получив на входе биты x и y , выдает $(x, y, c, x \oplus y)$, где c — бит переноса.

Элемент Фредкина и его биллиардная модель обеспечивают красивую реализацию обратимых вычислений. Существует еще один обратимый логический элемент, элемент *Тоффоли*, также являющийся универсальным с точки зрения классических вычислений. Хотя элемент Тоффоли не обладает такой же элегантной физической простотой, что и элемент Фредкина, при исследовании квантовых вычислений он будет полезнее. Мы уже имели дело с элементом Тоффоли в подразд. 1.4.1, но для удобства укажем его свойства и здесь.

У элемента Тоффоли три входных бита a , b и c ; биты a и b называются первым и вторым управляющими битами, бит c называется управляемым битом. Элемент оставляет оба управляющих бита неизменными, меняет значение управляемого бита на противоположное, если оба управляющих бита установлены в единицу, и оставляет управляемый бит неизменным в противном случае. Таблица значений для элемента Тоффоли и его условное обозначение представлены на рис. 3.17.

a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

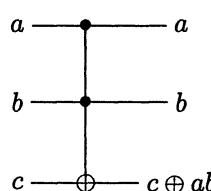


Рис. 3.17. Таблица значений для элемента Тоффоли и его условное обозначение

Как можно проводить универсальные вычисления с помощью элемента Тоффоли? Предположим, что мы хотим провести операцию NAND над битами a и b . Чтобы сделать это с помощью элемента Тоффоли, подадим a и b на вход в качестве управляющих битов, а вспомогательный бит, установленный в 1, подадим в качестве управляемого бита (см. рис. 3.18). Как следовало ожидать из предыдущего рассмотрения элемента Фредкина, реализация NAND с помощью элемента Тоффоли требует вспомогательного бита на входе, а некоторые из выходных битов являются мусором.

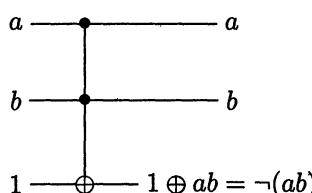


Рис. 3.18. Реализация элемента NAND при помощи элемента Тoffоли. Два верхних бита представляют вход элемента NAND, третий бит устанавливают в состояние 1. Выход элемента NAND — третий бит

С помощью элемента Тoffоли можно также реализовать операцию FANOUT, подав вспомогательный бит 1 в качестве первого управляющего бита, а бит a — в качестве второго управляющего бита, что даст на выходе 1, a , a . Это проиллюстрировано на рис. 3.19. Вспоминая, что элементы NAND и FANOUT позволяют реализовать любое вычисление, мы получаем, что любую схему можно эффективно моделировать с помощью обратимой схемы, состоящей только из элементов Тoffоли и вспомогательных битов, и что обращения вычислений можно добиться теми же методами, которые были использованы при обсуждении элемента Фредкина.

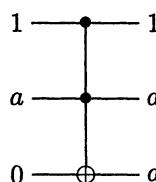


Рис. 3.19. Реализация FANOUT при помощи элемента Тoffоли. Второй бит — вход элемента FANOUT, два других входных бита — вспомогательные. Выход элемента FANOUT — второй и третий биты.

Наш интерес к обратимым вычислениям вызван желанием понять, какие затраты энергии требуются для вычислений. Ясно, что при отсутствии шума биллиардная модель вычислений энергии не потребляет; что можно сказать о моделях, основанных на элементе Тoffоли? На этот вопрос можно ответить,

только рассматривая конкретные реализации этого элемента. В гл. 7 мы обсудим некоторые из них и увидим, что элемент Тоффоли действительно можно реализовать без затрат энергии.

Говоря о том, что вычисления можно проводить без затрат энергии, следует проявлять большую осторожность. Как мы уже отмечали, биллиардная модель вычислений весьма чувствительна к шуму, и это же верно применительно ко многим другим моделям обратимых вычислений. Чтобы ликвидировать воздействие шума, необходимо в той или иной форме производить исправление ошибок. Обычно исправление ошибок подразумевает проведение измерений с тем, чтобы выяснить, ведет ли себя система ожидаемым образом или произошли ошибки. Поскольку память компьютера конечна, результаты этих измерений должны быть в какой-то момент уничтожены, чтобы освободить место для записи новых измерений. Согласно принципу Ландауэра, при этом расходуется энергия, которую необходимо учитывать при вычислении энергетических затрат на вычисления. Более подробно мы рассмотрим энергозатраты, связанные с исправлением ошибок, в подразд. 12.4.4.

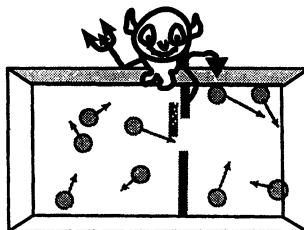
Итак, что же мы можем заключить, исходя из нашего рассмотрения обратимых вычислений? Основных выводов три. Во-первых, обратимость получается, когда мы следим за каждым битом информации; необратимость возникает только тогда, когда информация теряется или уничтожается. Во-вторых, проводя обратимые вычисления, мы избавляемся от необходимости тратить энергию на вычисления. В принципе любое вычисление можно провести без затрат энергии. В-третьих, обратимые вычисления можно провести эффективно, не выдавая мусорных битов, значения которых зависят от входных битов. Другими словами, если существует необратимая схема, вычисляющая функцию f , то она может быть эффективно смоделирована с помощью обратимой схемы, действующей по правилу $(x, y) \rightarrow (x, y \oplus f(x))$.

Каковы следствия всего этого для физики, информатики, а также для квантовых вычислений и квантовой теории информации? С точки зрения физика или инженера-компьютерщика, которого беспокоит выделение тепла, хорошие новости состоят в том, что в принципе возможно проводить вычисления без диссипации энергии, сделав их обратимыми, хотя на практике диссипация энергии придает системе устойчивую нечувствительность к шуму. На еще более фундаментальном уровне идеи, ведущие к обратимым вычислениям, приводят также к решению стоявшей сто лет проблемы физики — знаменитой проблемы *демона Максвелла*. История этой проблемы и ее решение приведены во вставке 3.5. С точки зрения специалиста по информатике обратимые вычисления оправдывают использование необратимых элементов в вычислительных моделях, например в машине Тьюринга (поскольку модели с необратимыми элементами и без них полиномиально эквивалентны). Более того, поскольку физический мир в основе своей обратим, можно заключить, что классы сложности, основанные на обратимых моделях, более естественны, чем классы, основанные на необратимых моделях (мы еще вернемся к этому замечанию в задаче 3.9 и в разделе «История и дополнительная литература»). С точки зрения квантовых вычислений и квантовой информации обратимые вычисления

крайне важны. Чтобы использовать эффективность квантовых вычислений в полную силу, все классические подпрограммы в квантовых алгоритмах должны быть обратимы и не выдавать мусорных битов, зависящих от классических входных данных.

Вставка 3.5. Демон Максвелла

Законы термодинамики показывают, какая работа может быть совершена системой, находящейся в термодинамическом равновесии. Один из этих законов — второе начало термодинамики — утверждает, что энтропия замкнутой системы не может уменьшаться. В 1871 г. Джеймс Кларк Максвелл предложил устройство, которое, этот закон нарушает. Представьте себе миниатюрного «демона», вроде того, что изображен на рисунке, который может уменьшить энтропию цилиндра с газом, первоначально находящегося в равновесии, разделяя быстрые и медленные молекулы по двум половинам цилиндра. Этот демон сидит у дверки, сделанной в середине перегородки цилиндра. Когда быстрая молекула приближается слева, демон открывает дверку, пропускает молекулы, а затем дверку закрывает. Если проделать это много раз, то общая энтропия цилиндра уменьшится, что явно противоречит второму началу термодинамики.



Решение этого парадокса состоит в том, что демон должен измерять скорости молекул; результаты этих измерений должны храниться в памяти демона. Поскольку любая память конечна, в какой-то момент демону придется стирать информацию, чтобы было куда записывать результаты новых измерений. Согласно принципу Ландауэра, акт стирания информации увеличивает полную энтропию системы, состоящей из демона, цилиндра и окружающей среды. На самом деле более тщательный анализ показывает, что из принципа Ландауэра вытекает, что полная энтропия при этом увеличивается *как минимум на столько же*, на сколько энтропия уменьшается в результате действий демона, так что в итоге второе начало термодинамики выполняется.

3.3 Перспективы информатики

В таком кратком введении, как эта глава, совершенно невозможно подробно описать все важные идеи из такой богатой области, как информатика. Мы на-

деемся, что смогли лишь отчасти объяснить, что означает *мыслить* как специалист по информатике, и познакомить с основными терминами и концепциями, связанными с теорией вычислений. В завершение этой главы мы коротко коснемся некоторых более общих тем, чтобы вы смогли уяснить, как квантовые вычисления и квантовая теория информации вписываются в общие концепции информатики.

Наше обсуждение проводилось вокруг вычислительной модели, основанной на машине Тьюринга. Попробуем сравнить с этой моделью такие нестандартные модели вычислений, как компьютеры с широким использованием параллельных вычислений, ДНК-компьютеры и аналоговые компьютеры. Начнем с параллельных компьютеров. Подавляющее большинство реальных компьютеров являются последовательными. Они обрабатывают инструкции одну за другой в некотором центральном процессоре. Параллельные компьютеры, напротив, могут обрабатывать несколько инструкций одновременно, что приводит к значительной экономии времени и денег. Тем не менее, в отношении эффективности параллельные вычисления не дают фундаментального преимущества по сравнению со стандартной машиной Тьюринга, поскольку машина Тьюринга может моделировать параллельный компьютер, причем ресурсы, требуемые для вычисления, — память и время — останутся полиномиально эквивалентными исходным. Что параллельный компьютер выигрывает во времени, то он теряет в памяти, и в результате никакого существенного изменения эффективности вычислительной модели не происходит.

Интересным частным случаем параллельных вычислений является техника *ДНК-вычислений*. Цепочка ДНК (дезоксирибонуклеиновой кислоты) представляет собой полимерную молекулу, состоящую из нуклеотидов четырех типов, обозначаемых буквами А (аденин), Ц (цитозин), Г (гуанин) и Т (тимин). При определенных условиях две цепочки могут соединяться и образовать двойную цепочку, если соответственно расположенные основания в этих цепочках комплементарны друг другу (А комплементарно Т, а Г комплементарно Ц). С помощью различных химических приемов можно увеличивать количество цепочек, начинаяющихся или заканчивающихся определенными последовательностями оснований (реакция полимеразы), разделять цепочки по длине (гелевый электрофорез), разделять двойные цепочки на одинарные (изменяя температуру и pH), читать последовательность нуклеотидов на цепочке, разрезать цепочку и проверять, присутствует ли в пробирке определенная последовательность ДНК. Процедура надежного использования этой техники довольно сложна, но основную идею можно понять на примере.

Задача об упорядоченном гамильтоновом пути — это простой вариант задачи о гамильтоновом цикле из подразд 3.2.2; она состоит в том, чтобы определить, существует ли в данном ориентированном графе G с N вершинами путь между двумя данными вершинами j_1 и j_N , в который каждая вершина входит ровно один раз. Эту задачу можно решить на ДНК-компьютере следующим образом. Обозначим различные последовательности оснований через x_j (а через \bar{x}_j обозначим их комплементарные дополнения), пары $x_j x_k$ кодируют ребра графа, а пары $\bar{x}_j \bar{x}_k$ кодируют вершины. Тёперь задача решается за пять шагов.

(1) Сгенерировать случайным образом пути в графе G , создав смесь всевозможных цепочек ДНК, соответствующих вершинам и ребрам, и подождать, пока эти цепочки объединятся в пары. (2) Оставить только пути, начинающиеся с j_1 и заканчивающиеся на j_N (увеличивая только количество удвоенных цепочек, начинающихся с \bar{x}_{j_1} и заканчивающихся на \bar{x}_{j_N}). (3) Оставить только цепочки длины N , разделив цепочки по длинам. (4) Выбрать пути, в которые каждая вершина входит один раз: разделить ДНК на отдельные цепочки и по очереди пробовать объединять эти цепочки с цепочками, соответствующими вершинами, каждый раз отбирая лишь те цепочки, которые действительно объединяются. (5) Наконец, выяснить, осталось ли что-нибудь после этого отбора; если да, то путь существует, в противном случае нет. Чтобы обеспечить верный ответ с достаточно большой вероятностью, цепочки x_j можно выбирать достаточно длинными (порядка 30 нуклеотидов), и в реакции надо использовать большое количество цепочек (порядка 10^{14}).⁶

Эту схему можно улучшать с помощью различных эвристических методов, но, конечно, методы полного перебора, подобные вышеприведенному, применимы лишь тогда, когда можно эффективно получать все возможные пути, так что число молекул должно экспоненциально расти с увеличением размера задачи (в нашем примере — с числом вершин). Молекулы ДНК относительно небольшие и легко синтезируются, а то обстоятельство, что огромное количество комбинаций нуклеотидов может умещаться в одной пробирке, может на некоторое время скомпенсировать экспоненциальный рост сложности (пока речь идет о нескольких десятках вершин), но в конечном счете экспоненциальный рост сложности ограничивает применимость этого метода. Таким образом, хотя ДНК-вычисления представляют собой привлекательную и физически реализуемую модель вычислений, пригодную для решения некоторых задач, эта модель является классической, и никакого принципиального улучшения производительности по сравнению с машиной Тьюринга не дает.

Еще одним вариантом вычислительной модели является *аналоговый компьютер*. Компьютер называется аналоговым, если используемое в нем физическое представление информации основано на непрерывно меняющихся величинах, а не на нулях и единицах. Например, термометр представляет информацию в аналоговой форме. Аналоговые схемы, использующие резисторы, конденсаторы и усилители, также называются аналоговыми вычислителями. В идеале ресурсы таких машин неограничены, поскольку непрерывные переменные, например координаты или разности потенциалов, могут содержать неограниченный объем информации. Но это утверждение верно только в отсутствие шума. При наличии шума число различимых состояний аналогового устройства будет конечно, и благодаря этому аналоговые компьютеры могут обрабатывать только конечное количество информации. На практике при наличии шума аналоговые компьютеры оказываются не более производительными,

⁶ Число 10^{14} подходит при решении задачи на графе с числом вершин, меньшим 20. Если решать задачу на графе с 200 вершинами (такие задачи удается решать на обычных суперкомпьютерах), то потребуется больше 10^{200} цепочек, что значительно превышает число элементарных частиц в наблюдаемой части Вселенной — Прим. ред.

чем цифровые и машины Тьюринга. Можно было бы подумать, что квантовые компьютеры являются разновидностью аналоговых компьютеров, поскольку при описании состояний кубитов используются непрерывные параметры; однако оказывается, что влияние шума на квантовый компьютер может быть *оцифровано*. В результате преимущества квантовых компьютеров сохраняются даже при наличии конечного шума (мы увидим это в гл. 10).

А как влияет шум на цифровые компьютеры? В начале компьютерной эры шум был серьезной проблемой. У некоторых из первых компьютеров вакуумные трубы давали сбой раз в несколько минут. Даже в наши дни шум представляет собой проблему для таких устройств, как модемы и жесткие диски. Значительные усилия были затрачены на то, чтобы понять, как можно строить надежные компьютеры из ненадежных компонент. Фон Нейман доказал, что это действительно возможно, причем ресурсы, необходимые для вычислений, возрастают при этом лишь полиномиально. Однако по иронии судьбы в современных компьютерах результаты этих разработок не используются, поскольку компоненты современных компьютеров фантастически надежны. Вероятности ошибки в 10^{-17} и ниже — это обычные показатели для современной электроники. По этой причине сбои случаются столь редко, что никто не считает нужным предпринимать дополнительные усилия, направленные на борьбу с ними. С другой стороны, мы увидим, что квантовые компьютеры — устройства весьма деликатные и требуют надежной техники для исправления ошибок.

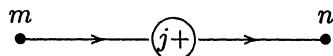
В компьютерах разной архитектуры влияние шума проявляется по-разному. Если, например, шум влияния не оказывает, то переход на параллельные вычисления может и не повлиять на количество операций, необходимое для выполнения задачи. Однако параллельная система может оказаться значительно более устойчивой к шуму, чем последовательная, поскольку у шума будет меньше времени на то, чтобы его эффекты накопились. Следовательно, при реалистическом анализе параллельная версия алгоритма может иметь существенные преимущества перед последовательной. Проблемы архитектуры хорошо разработаны для классических компьютеров. Для квантовых компьютеров аналогичных исследований почти не проводилось, но изучение влияния шума уже подсказывает некоторые желательные черты будущих квантовых компьютеров, в частности, высокую степень параллелизма.

Четвертая модель вычислений — это *распределенные вычисления*, при которых два или более разнесенных в пространстве вычислительных устройства используются для решения одной задачи. Разумеется, эта вычислительная модель не более производительна, чем машина Тьюринга, в том смысле, что на машине Тьюринга ее можно эффективно моделировать. Однако распределенные вычисления подсказывают новую и интригующую задачу о ресурсах: как наилучшим образом использовать несколько вычислительных устройств в условиях, когда высока цена *передачи информации* от одного устройства к другому. Эта задача становится особенно интересной, если компьютеры соединены высокоскоростной сетью: хотя суммарная вычислительная производительность всех компьютеров в сети может быть весьма высока, использовать этот потенциал непросто. Наиболее интересные задачи трудно разбить на незави-

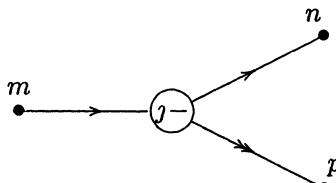
смые части, которыми можно заниматься по отдельности. Часто требуется связь между различными компьютерами в сети для обмена промежуточными результатами или синхронизации состояний. С целью изучения этих проблем была развита теория *коммуникационной сложности*, в которой вычисляется стоимость обмена информацией при решении задач. Если доступны квантовые ресурсы, которыми можно обмениваться по сетям, то в некоторых случаях коммуникационную сложность можно значительно уменьшить.

Основная мысль, которая проходит через эти заключительные замечания, да и через всю эту книгу, такова: несмотря на то, что традиционно информатика не зависит от физических ограничений, в конечном счете законы физики оказывают огромное влияние не только на физическую реализацию компьютеров, но и на то, какого рода задачи поддаются решению. Успех квантовых вычислений и квантовой теории информации как физически осмыслинной альтернативной модели вычислений выдвигает идеи информатики на передний край физики. Цель, преследуемая авторами остальной части данной книги — соединить идеи этих двух далеких областей знания и получить удовольствие от полученного результата.

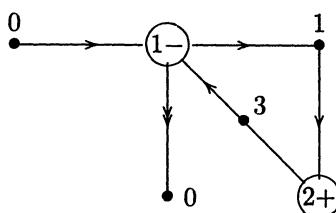
Задача 3.1 (машины Минского). Машина Минского состоит из конечного числа *регистров* $r_1, r_2 \dots, r_k$, в каждом из которых может храниться произвольное целое неотрицательное число, и *программы*, состоящей из *директив* двух типов. Директивы первого типа имеют следующий вид:



Интерпретировать это надо следующим образом: при выполнении директивы m содержание регистра r_j увеличивается на единицу, и управление передается в точку, соответствующую директиве n . Второй тип директив таков



Эта директива интерпретируется так: при выполнении директивы m содержание регистра r_j уменьшается на единицу, если в нем записано положительное число, и управление передается в точку, соответствующую директиве n ; если же в регистре r_j записан нуль, то его значение не меняется, а управление передается в точку, соответствующую директиве p . Программа для машины Минского состоит из набора таких директив, записанного, например, в виде



Начало программы (а также все возможные точки остановки) обычно обозначается числом нуль. Эта программа берет содержимое регистра r_1 и прибавляет его к содержимому регистра r_2 , последовательно уменьшая содержимое регистра r_1 до нуля.

- (1) Докажите, что все вычислимые (с помощью машины Тьюринга) функции вычислимы и на машине Минского в том смысле, что для данной вычислимой функции $f(\cdot)$ существует такая программа для машины Минского, что если в начале работы регистры находятся в состоянии $(n, 0, \dots, 0)$, то в конце они будут в состоянии $(f(n), 0, \dots, 0)$.
- (2) Дайте набросок доказательства того факта, что любая функция, вычислимая на машине Минского в описанном выше смысле, вычислима и на машине Тьюринга.

Задача 3.2 (векторные игры). Векторная игра задается конечным списком целочисленных векторов одной размерности. Сама игра состоит в следующем: берется вектор x с целыми неотрицательными координатами и к нему прибавляется первый из тех векторов списка, сумма которого с x имеет неотрицательные координаты; далее процесс повторяется, пока это возможно. Докажите, что для любой вычислимой функции $f(\cdot)$ существует векторная игра, которая, будучи начатой с вектора $(n, 0, \dots, 0)$, завершается на векторе $(f(n), 0, \dots, 0)$. (Указание. Покажите, что с помощью векторной игры размерности $k + 2$ можно моделировать машину Минского с k регистрами.)

Задача 3.3 (Фрактран). Программа на языке Фрактран задается с помощью последовательности положительных рациональных чисел q_1, \dots, q_n . При подаче на вход целого положительного числа m оно заменяется на $q_i m$, где i — наименьший номер, для которого число $q_i m$ целое, после чего процесс повторяется. Если в какой-то момент такого i не находится, программа останавливается. Докажите, что для любой вычислимой функции $f(\cdot)$ существует программа на Фрактране, которая при подаче на вход числа 2^n останавливается на числе $2^{f(n)}$, причем в процессе вычислений другие степени двойки не появляются. (Указание. Воспользуйтесь предыдущей задачей.)

Задача 3.4 (неразрешимость динамических систем). Программа на Фрактране является по существу очень простой динамической системой на множестве целых положительных чисел. Покажите, что не существует алгоритма, позволяющего выяснить, содержит ли какая-либо траектория такой системы число 1.

Задача 3.5 (двухбитовая обратимая логика не универсальна). Пусть мы пытаемся строить схемы, используя только одно- и двухбитовые обратимые элементы, а также вспомогательные биты. Докажите, что существуют булевые функции, которые нельзя вычислить таким образом. Выведите отсюда, что элемент Тоффоли невозможно реализовать с помощью одно- и двухбитовых обратимых элементов даже с использованием вспомогательных битов.

Задача 3.6 (трудность приближенного решения задачи коммивояжера). Пусть $r \geq 1$, и предположим, что для задачи коммивояжера существует приближенный алгоритм, позволяющий найти обход n городов кратчайшим с точностью до множителя r . Пусть $G = (V, E)$ — произвольный граф с n вершинами. Рассмотрим следующую задачу коммивояжера: города — это вершины графа, причем расстояние между городами i и j равно 1, если (i, j) — ребро графа G , и $\lceil r \rceil |V| + 1$ в противном случае. Покажите, что если применить наш приближенный алгоритм к этой задаче, то на выходе получится либо гамильтонов цикл, если такой существует, либо маршрут, длина которого превышает $\lceil r \rceil |V|$. Из NP-полноты задачи о гамильтоновом цикле выведите, что такой приближенный алгоритм существовать не может, если неверно, что $P = NP$.

Задача 3.7 (обратимые машины Тьюринга).

- (1) Объясните, как сконструировать обратимую машину Тьюринга, которая может вычислять те же функции, что и обычная машина Тьюринга. (*Указание.* Вам может помочь многоленточная конструкция.)
- (2) Дайте оценки памяти и времени, необходимых вашей обратимой машине Тьюринга, через время $t(x)$ и память $s(x)$, требуемые обычной одноленточной машине Тьюринга для вычисления той же функции $f(x)$.

Задача 3.8 (найти трудновычислимый класс функций — задача для исследования). Найдите естественный класс функций от n переменных, для вычисления которых булевыми схемами требуется сверхполиномиальное количество булевых элементов.

Задача 3.9 (обратимый PSPACE = PSPACE). Можно показать, что «задача выполнимости с кванторами», или QSAT, является PSPACE-полной. Это означает, что любой другой язык из класса PSPACE сводится к языку QSAT за полиномиальное время. По определению, язык QSAT состоит из таких булевых формул φ от n переменных x_1, \dots, x_n , записанных в конъюнктивной нормальной форме, что

$$\exists_{x_1} \forall_{x_2} \exists_{x_3} \dots \forall_{x_n} \varphi, \quad \text{если } n \text{ четно} \quad (3.9)$$

$$\forall_{x_1} \exists_{x_2} \forall_{x_3} \dots \exists_{x_n} \varphi, \quad \text{если } n \text{ нечетно} \quad (3.10)$$

Докажите, что с помощью обратимой машины Тьюринга, работающей на полиномиальной памяти, язык QSAT можно распознать. Таким образом, класс языков, распознаваемых обратимым компьютером, который работает на полиномиальной памяти, совпадает с PSPACE.

Задача 3.10 (вспомогательные биты и эффективность обратимых вычислений). Пусть p_m — m -ое простое число. Дайте набросок конструкции обратимой схемы, которая, получив на вход числа m и n , где $n > m$, выдает произведение $p_m p_n$, т. е., $(m, n) \rightarrow (p_m p_n, g(m, n))$, где $g(m, n)$ — конечное состояние вспомогательных битов. Оцените количество вспомогательных битов,

необходимых вашей схеме. Докажите, что если можно построить обратимую схему, размер которой полиномиален (относительно $\log n$) и которая использует $O(\log(\log n))$ вспомогательных битов, то задача представления числа в виде произведения двух простых чисел принадлежит классу **P**.

История и дополнительная литература

Информатика — это большой предмет, в котором есть много интересных подразделов. Мы не будем пытаться дать ее полный обзор, но порекомендуем несколько изданий, представляющих общий интерес, а также некоторые работы, непосредственно связанные с тематикой нашей книги.

Современная информатика началась с работы Тьюринга [388], датированной 1936 г. Тезис Чёрча–Тьюринга был впервые сформулирован Чёрчем в 1936 г. [87]; в дальнейшем он был более полно рассмотрен Тьюрингом с другой точки зрения. Примерно в то же время несколько других исследователей пришли к аналогичным выводам. Многие из этих работ обсуждаются в книге под редакцией Дэвиса [113]. Интересное обсуждение тезиса Чёрча–Тьюринга можно найти у Хофтадтера [189] и Пенроуза [316].

Существует много прекрасных книг, посвященных разработке алгоритмов; мы упомянем только три. Во-первых, это классический трехтомник Кнута [224, 225, 226]. Во-вторых, отметим замечательную книгу Кормена, Лейзерсона и Ривеста [92]. Эта большая и хорошо написанная книга содержит много материала о разработке различных алгоритмов. Наконец, книга Мотвани и Рагавана [295] является превосходным обзором алгоритмов, использующих случайные числа.

Современная теория вычислительной сложности возникла в значительной степени благодаря статьям Кука [99] и Карпа [209]. В России ко многим аналогичным идеям независимо пришел Левин [242], но, к сожалению, на Запад эти идеи проникли не сразу. Классическая книга Гэри и Джонсона [162] также оказала огромное влияние на работы по этой тематике. Пападимитриу написал прекрасную книгу [312], содержащую обзор многих идей теории сложности; большая часть материала, излагаемого в этой главе, основана на книге Пападимитриу. В настоящей главе мы рассматривали только один тип сводимости, а именно сводимость за полиномиальное время. На самом деле понятий сводимости существует несколько; их давний обзор можно найти у Ладнера, Линча и Селмана [256]. Изучение различных понятий сводимости выросло в отдельный предмет — *теорию структурной сложности*. Обзор на эту тему можно найти у Бальказара, Диаса и Габарро [38, 39].

Изучение связи между информацией, диссипацией энергии и вычислениями имеет долгую историю. Современное понимание возникло после вышедшей в 1961 г. статьи Ландауэра [234], в которой был впервые сформулирован принцип Ландауэра. Сциллард [383] и фон Нейман в своей лекции в 1949 г. [405] (с. 66) приходят к близким выводам, но они не в полной мере осознавали, что именно *стирание информации* приводит к диссипации энергии.

Обратимые машины Тьюринга были изобретены Лесерфом [240], а позднее (независимо) переоткрыты в оказавшей большое влияние статье Беннета [44].

Фредкин и Тоффоли [156] ввели вычислительную модель, основанную на обратимых схемах. Исторический интерес представляют курсовая работа Бартона в МИТ [18] и дипломная работа Ресслера [338], в которой разработан проект обратимого аналога машины PDP-10. В наши дни обратимая логика имеет важное значение для разработки схем CMOS малой мощности [426].

Демон Maxwella — интересная тема, имеющая долгую и захватывающую историю. Maxwell выдвинул эту идею в 1871 г. [277]. В 1929 г. Сциллард опубликовал ключевую статью [383], в которой были предвосхищены многие детали полного решения проблемы демона Maxwella. В 1965 г. Фейнман [152] опубликовал решение частного случая задачи о демоне Maxwella. Беннет, основываясь на работе Ландауэра [234], написал две прекрасные работы на эту тему [46, 47], в которых решение проблемы было завершено. Интересная книга об истории демона Maxwella и его изгнании — сборник статей под редакцией Леффа и Рекса [267].

DНК-вычисления были предложены Эдльманом; описываемое нами решение задачи об ориентированном гамильтоновом пути содержится в его статье [5]. Липтон показал, что задачи 3SAT и выполнимости схемы также могут быть решены при помощи этой модели. Хорошая обзорная статья Эдльмана на эту тему опубликована в *Scientific American* [6]; относительно универсальности DНК-операций см. работу Уинфри [419]. По поводу надежных операций при наличии шума интересно посмотреть книгу Винограда и Коуэна [412]; мы еще обратимся к этой теме в гл. 10. Хорошим учебником по архитектуре компьютеров является книга Хенкесси, Гольдберга и Паттерсона [177].

Задачи 3.1–3.4 следуют идеям, введенным Минским (в его прекрасной книге о вычислительных машинах [287]) и развитым Конуэем [97, 98]. Язык Фрактран представляет собой одну из наиболее красивых и элегантных вычислительных моделей; мы продемонстрируем это на следующем примере, известном под названием PRIMEGAME[98]. PRIMEGAME задается списком рациональных чисел:

$$\frac{17}{91}; \frac{78}{85}; \frac{19}{51}; \frac{23}{38}; \frac{29}{33}; \frac{77}{29}; \frac{95}{23}; \frac{77}{19}; \frac{1}{17}; \frac{11}{13}; \frac{13}{11}; \frac{15}{2}; \frac{1}{7}; \frac{55}{1}. \quad (3.11)$$

Удивительно, что, если подать на вход этой фрактрановской программы число 2, то все остальные возникающие степени двойки, а именно $2^2, 2^3, 2^5, 2^7, 2^{11}, 2^{17}, \dots$, будут в точности числом 2 в простых степенях в порядке возрастания. Задача 3.9 — пример из области исследований, занимающейся проблемами памяти при обратимых вычислениях. См. статьи Беннета [48], а также Ли, Тромпа и Витаньи [272, 271].

Часть II

Квантовые вычисления

Глава 4

КВАНТОВЫЕ СХЕМЫ

Теория вычислений традиционно изучалась абстрактно, как раздел чистой математики. При этом теряется ее суть. Компьютеры – это физические объекты, а вычисления – физические процессы. Чтобы компьютеры могут вычислить, а чтобы – не могут, определяется исключительно законами физики, а не чистой математикой.

Д. Дойч

Подобно математике, теоретическая информатика несколько отличается от остальных наук в том отношении, что имеет дело с искусственными законами, которые могут быть доказаны, в отличие от законов природы, которые никогда не будут известны до конца.

Д. Кнут

Противоположностью глубокой истины может быть и другая глубокая истина.

Н. Бор

Эта глава открывает вторую часть книги, где подробно рассматривается квантовые вычисления. Здесь разрабатываются фундаментальные принципы квантовых вычислений и обсуждаются основные компоненты квантовых схем, являющихся основным языком описания сложных квантовых вычислений. Два основных квантовых алгоритма, известных в настоящее время, строятся с помощью квантовых схем в двух последующих главах. В гл. 5 речь идет о квантовом преобразовании Фурье и его приложениях к задачам определения собственного числа, вычисления периода и факторизации целого числа. Гл. 6 описывает квантовый алгоритм поиска и его приложения к поиску в базах

данных, задачам перечисления и ускорению решения *NP*-полных задач. В завершающей вторую часть гл. 7 обсуждается, каким образом квантовые вычисления могут быть когда-нибудь реализованы на практике. Две другие темы, вызывающие большой интерес в связи с квантовыми вычислениями, — квантовый шум и квантовое исправление ошибок, — вошли в третью часть книги, так как они представляют самостоятельный интерес независимо от квантовых вычислений.

В данной главе вводятся две основные идеи. Во-первых, подробно объясняется фундаментальная модель квантовых вычислений — квантовые схемы. Во-вторых, показывается, что существует небольшой по размеру набор элементов квантовых схем, являющийся *универсальным* в том смысле, что любое квантовое вычисление может быть реализовано с помощью схемы, составленной из этих элементов.

По ходу изложения у нас будет случай рассмотреть и много других фундаментальных результатов, относящихся к квантовым вычислениям. В открывавшем главу разд. 4.1 содержится обзор квантовых алгоритмов, причем особое внимание уделяется тому, какие алгоритмы известны и какие общие принципы лежат в их основе. В разд. 4.2 подробно описываются операции над одним кубитом. Несмотря на простоту, такие операции предоставляют богатые возможности для построения примеров и разработки технических приемов, и их необходимо изучить подробно. Разд. 4.3 посвящен выполнению *условных,-unitарных операций* над несколькими кубитами, а в разд. 4.4 обсуждается измерение в модели квантовых схем. Затем все эти ингредиенты соединяются в разд. 4.5, где формулируется и доказывается теорема универсальности. В разд. 4.6 еще раз рассматриваются все основные компоненты квантовых вычислений и обсуждаются возможные варианты модели квантовых схем, а также важный вопрос о сравнении эффективности классического и квантового компьютеров. Завершающий главу разд. 4.7 посвящен важному и поучительному приложению квантовых вычислений, а именно — *моделированию* реальных квантовых систем.

Данная глава, содержащая большое количество упражнений, для изучения, вероятно, наиболее сложная, так что объясним, почему следует затратить труд на ее освоение. Научиться работать с основными элементами квантовых схем нетрудно, но для этого необходимо знать большое количество простых результатов и владеть техническими приемами, что поможет перейти к более трудной задаче разработки квантовых алгоритмов. По этой причине глава насыщена примерами и во многих случаях читателю предлагается самостоятельно восполнить детали. Можно ознакомиться с упрощенным (но несколько поверхностью) обзором первооснов квантовых вычислений, для этого следует начать изучение материала с разд. 4.6.

4.1 Квантовые алгоритмы

Зачем нужен квантовый компьютер? Нам всем знакомо отчаяние, когда обнаруживается, что для решения некоторой задачи не хватает вычислительных

возможностей. Собственно говоря, многие интересные задачи нельзя решить на классическом компьютере не из-за их неразрешимости, а потому, что объем требуемых ресурсов выражается астрономическим числом.

Создание квантовых компьютеров дает надежду на то, что можно будет реализовать новые алгоритмы, которые позволяют решать задачи, требующие чрезмерно больших ресурсов при использовании классического компьютера. На момент написания книги известны два широких класса квантовых алгоритмов, соответствующих этим ожиданиям. Первый из них основан на принадлежащем Шору *квантовом преобразовании Фурье* и включает замечательные алгоритмы решения задач факторизации и вычисления дискретного логарифма с экспоненциальным ускорением по сравнению с наилучшими известными классическими алгоритмами. Второй класс алгоритмов связан с алгоритмом Гровера для *квантового поиска*. Эти алгоритмы обеспечивают *квадратичное* ускорение наилучших возможных классических алгоритмов, но не столь поразительное, как в первом случае. Алгоритм квантового поиска важен ввиду широкого использования поиска в классических алгоритмах, так что во многих случаях оказывается возможным прямое преобразование классического алгоритма в более быстрый квантовый.

На рис. 4.1 представлены известные в настоящее время квантовые алгоритмы и некоторые примеры их применения. Разумеется, в основе приведенной диаграммы лежат квантовое преобразование Фурье и квантовый поиск. Особенно интересен алгоритм квантового перечисления. Этот алгоритм, представляющий собой остроумную комбинацию из квантового поиска и преобразования Фурье, может быть использован для более быстрой, чем это возможно в случае использования классического компьютера, оценки числа решений задачи поиска.

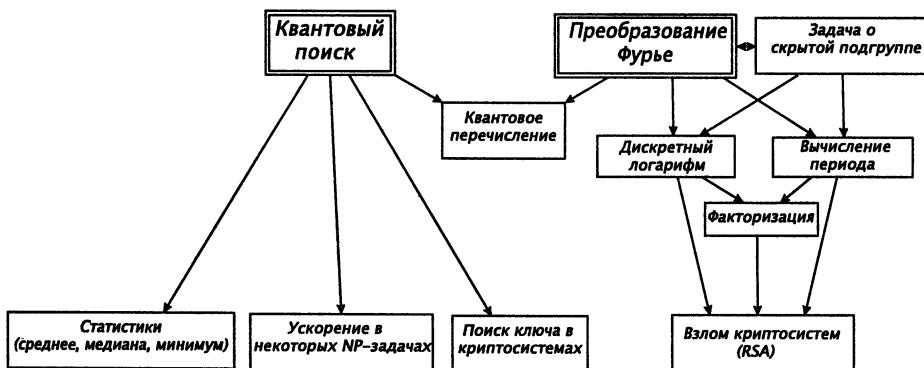


Рис. 4.1. Основные квантовые алгоритмы и их взаимосвязь (а также некоторые приложения)

Алгоритм квантового поиска имеет много потенциальных приложений, некоторые из них приведены на рисунке. Так его можно использовать для более быстрого, чем на классическом компьютере, нахождения статистик (например, наименьшего элемента) в неупорядоченном наборе данных. С его помощью

можно ускорить алгоритмы для решения некоторых задач класса NP — тех задач, для которых не известен лучший алгоритм, чем прямой перебор. Наконец, его применение позволит ускорить поиск ключа к таким криптосистемам, как широко используемая Data Encryption Standard (DES). Эти и другие приложения будут рассмотрены в гл. 6.

Квантовое преобразование Фурье также имеет много интересных приложений. С его помощью можно решить задачи вычисления дискретного логарифма и факторизации. Это в свою очередь позволяет “взломать” с помощью квантового компьютера многие из наиболее популярных криптосистем, включая RSA. Помимо этого, оказывается, что преобразование Фурье тесно связано с важной математической задачей о скрытой подгруппе (обобщение задачи нахождения периода периодической функции). Квантовому преобразованию Фурье и некоторым его приложениям, в том числе быстрым квантовым алгоритмам для факторизации и вычисления дискретного логарифма, посвящена гл. 5.

Почему известно так мало квантовых алгоритмов, превосходящих свои классические аналоги? Ответ состоит в том, что разработка хорошего квантового алгоритма является, похоже, трудной задачей. На это имеются по меньшей мере две причины. Прежде всего разработка любых алгоритмов — классических или квантовых — непростое дело! История показывает, что даже в очень простых на первый взгляд задачах, подобных умножению двух чисел, зачастую приходится проявлять изобретательность для того, чтобы получить алгоритм, близкий к оптимальному. Искать хорошие квантовые алгоритмы трудно вдвое, поскольку при этом необходимо удовлетворить дополнительное условие: квантовые алгоритмы должны быть лучше, чем известные классические. Вторая состоит в том, что наша интуиция гораздо лучше приспособлена к классическому миру, чем к квантовому. Если исходить из интуиции, то построенные алгоритмы будут классическими. Чтобы получались хорошие квантовые алгоритмы, необходимы особая интуиция и особые ухищрения.

Более глубокому изучению квантовых алгоритмов будет посвящена следующая глава. Здесь же мы введем эффективный и мощный язык для их описания — язык квантовых схем, которые являются агрегатами из конечного набора компонентов и описывают вычислительные процедуры. Эта конструкция позволяет нам оценить качество алгоритма или через общее количество элементов в схеме, или через глубину схемы. Вместе с языком схем вводится и набор приемов, позволяющих упростить разработку алгоритмов и достичь их концептуального понимания.

4.2 Операции на одном кубите

Рассмотрение нашего инструментария для квантовых вычислений начнем с операций на простейшей возможной квантовой системе — одном кубите. Понятие кубита было введено в подразд. 1.3.1. Напомним вкратце, о чём там шла речь.

Кубит — это вектор $|\psi\rangle = a|0\rangle + b|1\rangle$, параметризованный двумя комплексными числами, удовлетворяющими условию $|a|^2 + |b|^2 = 1$. Операции над кубитами

должны сохранять эту нормализацию и тем самым описываются унитарными матрицами 2×2 , из которых одними из наиболее полезных являются матрицы Паули; стоит выписать их еще раз:

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; \quad Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}; \quad Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \quad (4.1)$$

В дальнейшем большую роль будут играть три других квантовых элемента: оператор Адамара (обозначаемый символом « H »), оператор сдвига фазы (« S ») и элемент $\pi/8$ (« T »):

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}; \quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}; \quad T = \begin{bmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{bmatrix}. \quad (4.2)$$

Вот два полезных алгебраических факта, которые стоит помнить: $H = (X + Z)/\sqrt{2}$ и $S = T^2$. Можно задаться вопросом почему T называется элементом $\pi/8$, если в определении присутствует $\pi/4$? Причина заключается в том, что с точностью до не играющей роли общей фазы элемент T есть матрица, на диагонали которой стоят числа $\exp(\pm i\pi/8)$:

$$T = \exp(i\pi/8) \begin{bmatrix} \exp(-i\pi/8) & 0 \\ 0 & \exp(i\pi/8) \end{bmatrix}, \quad (4.3)$$

откуда и возникло в свое время название « $\pi/8$ ». Все же данный термин является довольно неудачным, и мы часто будем называть этот элемент просто «элемент T ».

Напомним также, что кубит в состоянии $a|0\rangle + b|1\rangle$ можно представить себе как точку (θ, φ) на единичной сфере, где $a = \cos(\theta/2)$, $b = e^{i\varphi} \sin(\theta/2)$, а число a можно считать действительным, поскольку общая фаза состояния ненаблюдаема. Это — уже обсуждавшееся в гл. 1 представление на сфере Блоха, и вектор $(\cos \varphi \sin \theta, \sin \varphi \cos \theta, \cos \theta)$ называется блоховским. Мы будем часто обращаться к этому представлению из соображений наглядности.

Упражнение 4.1. В упр. 2.11 вы вычислили собственные векторы матриц Паули. Найдите точки на сфере Блоха, соответствующие нормализованным собственным векторам различных матриц Паули.

Путем взятия экспоненты из матриц Паули получают три важных класса унитарных матриц — *операторы поворота* относительно осей \hat{x} , \hat{y} и \hat{z} , задаваемые следующими формулами:

$$R_x(\theta) \equiv e^{-i\theta X/2} = \cos \frac{\theta}{2} I - i \sin \frac{\theta}{2} X = \begin{bmatrix} \cos \frac{\theta}{2} & -i \sin \frac{\theta}{2} \\ -i \sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{bmatrix}, \quad (4.4)$$

$$R_y(\theta) \equiv e^{-i\theta Y/2} = \cos \frac{\theta}{2} I - i \sin \frac{\theta}{2} Y = \begin{bmatrix} \cos \frac{\theta}{2} & -\sin \frac{\theta}{2} \\ \sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{bmatrix}, \quad (4.5)$$

$$R_z(\theta) \equiv e^{-i\theta Z/2} = \cos \frac{\theta}{2} I - i \sin \frac{\theta}{2} Z = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}. \quad (4.6)$$

Упражнение 4.2. Пусть x — действительное число и A — такая матрица, что $A^2 = I$. Покажите, что

$$\exp(iAx) = \cos(x)I + i \sin(x)A. \quad (4.7)$$

С помощью этого соотношения проверьте формулы (4.4)–(4.6).

Упражнение 4.3. Покажите, что с точностью до общей фазы элемент $\pi/8$ удовлетворяет условию $T = R_z(\pi/4)$.

Упражнение 4.4. Представьте оператор Адамара H в виде произведения поворота операторов R_x и R_z и общего фазового множителя $e^{i\varphi}$ для некоторого действительного φ .

Если $\hat{n} = (n_x, n_y, n_z)$ — вещественный трехмерный единичный вектор, то можно обобщить предыдущие определения и определить поворот на угол θ вокруг оси \hat{n} по формуле

$$R_{\hat{n}}(\theta) \equiv \exp(-i\theta\hat{n} \cdot \vec{\sigma}/2) = \cos\left(\frac{\theta}{2}\right)I - i \sin\left(\frac{\theta}{2}\right)(n_xX + n_yY + n_zZ), \quad (4.8)$$

где $\vec{\sigma}$ — трехкомпонентный вектор (X, Y, Z) матриц Паули.

Упражнение 4.5. Докажите, что $(\hat{n} \cdot \vec{\sigma})^2 = I$, и проверьте с помощью этого равенства формулу (4.8).

Упражнение 4.6 (интерпретация поворотов на сфере Блоха). Одна из причин того, что операторы $R_{\hat{n}}(\theta)$ называют операторами поворота, состоит в следующем факте, который вы должны доказать. Предположим, кубит находится в состоянии, представленном блоховским вектором $\vec{\lambda}$. Тогда оператор $R_{\hat{n}}(\theta)$ поворачивает это состояние на блоховской сфере на угол θ относительно оси \hat{n} . Это объясняет, откуда берется загадочный множитель $1/2$ в определении матриц поворота.

Упражнение 4.7. Покажите, что $XYX = -Y$, и выведите отсюда уравнение $XR_y(\theta)X = R_y(-\theta)$.

Упражнение 4.8. Произвольный унитарный оператор, действующий на кубитах, можно записать в виде

$$U = \exp(i\alpha)R_{\hat{n}}(\theta) \quad (4.9)$$

для некоторых вещественных чисел α и θ и вещественного трехмерного единичного вектора \hat{n} .

1. Докажите это.
2. Найдите значения α , θ и \hat{n} , при которых получится оператор Адамара H .
3. Найдите значения α , θ и \hat{n} , при которых получится оператор сдвига фазы

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}. \quad (4.10)$$

Произвольный унитарный оператор, действующий на одном кубите, можно представить многими способами в виде композиции поворотов и общего фазового сдвига. Следующая теорема дает такое представление, которое будет особенно полезно в дальнейшем при изучении условных операций.

Теорема 4.1 ($Z - Y$ - разложение для одного кубита). Пусть U – унитарная операция на одном кубите. Тогда существуют такие действительные числа α, β, γ и δ , что справедливо уравнение

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta). \quad (4.11)$$

Доказательство. Ввиду унитарности U строки и столбцы матрицы U ортогональны, откуда следует наличие таких действительных чисел α, β, γ и δ , что

$$U = \begin{bmatrix} e^{i(\alpha-\beta/2-\delta/2)} \cos \frac{\gamma}{2} & -e^{i(\alpha-\beta/2+\delta/2)} \sin \frac{\gamma}{2} \\ e^{i(\alpha+\beta/2-\delta/2)} \sin \frac{\gamma}{2} & e^{i(\alpha+\beta/2+\delta/2)} \cos \frac{\gamma}{2} \end{bmatrix}. \quad (4.12)$$

Уравнение (4.11) непосредственно вытекает из определения матриц поворота и правила умножения матриц. ■

Упражнение 4.9. Объясните, почему любая операция на одном кубите может быть записана в виде (4.12).

Упражнение 4.10 ($X-Y$ - разложение поворотов). Постройте разложение, аналогичное данному в теореме 4.1, используя R_x вместо R_z .

Упражнение 4.11. Пусть \hat{m} и \hat{n} – непараллельные единичные вещественные трехмерные векторы. Покажите, что любая унитарная операция U на одном кубите может быть записана в виде

$$U = e^{i\alpha} R_{\hat{n}}(\beta_1) R_{\hat{m}}(\gamma_1) R_{\hat{n}}(\beta_2) R_{\hat{m}}(\gamma_2) \dots \quad (4.13)$$

при соответствующих значениях α, β_k и γ_k .

Теорема 4.1 полезна благодаря своему загадочному на первый взгляд следствию, которое, как будет ясно из следующего подраздела, является ключом к построению условных операций на нескольких кубитах:

Следствие 4.2 Пусть U – унитарный элемент, действующий на одном кубите. Тогда существуют такие унитарные операторы A, B и C , действующие на одном кубите, что $ABC = I$ и $U = e^{i\alpha} AXBXC$, где $e^{i\alpha}$ – фазовый множитель.

Доказательство. В соответствии с обозначениями теоремы 4.1 положим $A \equiv R_z(\beta)R_y(\gamma/2)$, $B \equiv R_y(-\gamma/2)R_z(-(\delta + \beta)/2)$ и $C \equiv R_z((\delta - \beta)/2)$. Заметим, что

$$ABC = R_z(\beta)R_y\left(\frac{\gamma}{2}\right)R_y\left(-\frac{\gamma}{2}\right)R_z\left(-\frac{\delta + \beta}{2}\right)R_z\left(\frac{\delta - \beta}{2}\right) = I. \quad (4.14)$$

Используя упр. 4.7 и принимая во внимание равенство $X^2 = T$, получим уравнение

$$XBX = X R_y\left(-\frac{\gamma}{2}\right) XX R_z\left(-\frac{\delta + \beta}{2}\right) X = R_y\left(\frac{\gamma}{2}\right) R_z\left(\frac{\delta + \beta}{2}\right). \quad (4.15)$$

Тогда имеем

$$AXBXC = R_z(\beta)R_y\left(\frac{\gamma}{2}\right)R_y\left(\frac{\gamma}{2}\right)R_z\left(\frac{\delta+\beta}{2}\right)R_z\left(\frac{\delta-\beta}{2}\right) \quad (4.16)$$

$$= R_z(\beta)R_y(\gamma)R_z(\delta). \quad (4.17)$$

Отсюда $U = e^{i\alpha}AXBXC$, что и требовалось доказать. ■

Элемент Адамара		$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Элемент Паули X		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Элемент Паули Y		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Элемент Паули Z		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Фазовый элемент		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
Элемент $\pi/8$		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/8} \end{bmatrix}$

Рис. 4.2. Названия, условные обозначения и унитарные матрицы наиболее распространенных элементов, действующих на одном кубите

Упражнение 4.12. Укажите A , B , C и α для элемента Адамара.

Упражнение 4.13 (тождества для схем). Полезно уметь упрощать схемы «с первого взгляда» с использованием тождеств для операторов. Докажите три следующих тождества:

$$H X H = Z; \quad H Y H = -Y; \quad H Z H = X. \quad (4.18)$$

Упражнение 4.14. С помощью предыдущего упражнения покажите, что, с точностью до общего фазового множителя $H T H = R_x(\pi/4)$.

Упражнение 4.15 (композиции операций на одном кубите). Блоховское представление дает хороший способ увидеть, как действует композиция поворотов.

- Покажите, что если сначала мы делаем поворот на угол β_1 относительно оси \hat{n}_1 , а затем — поворот на угол β_2 относительно оси \hat{n}_2 , то в композиции получим поворот на угол β_{12} относительно оси \hat{n}_{12} , где

$$c_{12} = c_1 c_2 - s_1 s_2 \hat{n}_1 \cdot \hat{n}_2, \quad (4.19)$$

$$s_{12} \hat{n}_{12} = s_1 c_2 \hat{n}_1 + c_1 s_2 \hat{n}_2 - s_1 s_2 \hat{n}_2 \times \hat{n}_1, \quad (4.20)$$

причем $c_i = \cos(\beta_i/2)$, $s_i = \sin(\beta_i/2)$, $c_{12} = \cos(\beta_{12}/2)$ и $s_{12} = \sin(\beta_{12}/2)$.

2. Покажите, что если $\beta_1 = \beta_2$ и $\hat{n}_1 = \hat{z}$, то уравнения принимают более простой вид

$$c_{12} = c^2 - s^2 \hat{z} \cdot \hat{n}_2, \quad (4.21)$$

$$s_{12} \hat{n}_{12} = sc(\hat{z} + \hat{n}_2) - s^2 \hat{n}_2 \times \hat{z}, \quad (4.22)$$

где $c = c_1$ и $s = s_1$.

Обозначения для наиболее распространенных элементов, действующих на одном кубите, приведены на рис. 4.2. Напомним основные правила для изображения квантовых схем: время течет слева направо, провода обозначают кубиты, а провод, перечеркнутый символом «/» — набор кубитов.

4.3 Условные операции

«Если A истинно, сделай B » — *условные операции* такого типа t часто используются в вычислениях как классических, так и квантовых. В этом подразделе будет объяснено, как можно реализовать сложные условные операции с помощью квантовых схем, построенных из простых элементов.

Простейшая и типичная условная операция — “управляемое NOT” (см. подразд. 1.2.1). Напомним, что этот элемент, который мы будем обозначать как CNOT, есть квантовый элемент с двумя входными кубитами, называемыми соответственно *управляющим* и *управляемым* (рис. 4.3).

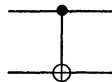


Рис. 4.3. Условное обозначение элемента CNOT. Верхний отрезок изображает управляющий кубит, нижний — управляемый

В терминах вычислительного базиса действие элемента CNOT задается формулой $|c\rangle|t\rangle \rightarrow |c\rangle|t \oplus c\rangle$; иными словами, если управляющий кубит установлен в единицу, то значение управляемого кубита меняется на противоположное, в противном случае управляемый кубит не изменяется. Таким образом, в вычислительном базисе $|\text{управляющий}, \text{управляемый}\rangle$ матричное представление элемента CNOT имеет вид

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \quad (4.23)$$

Более общим образом, предположим, что U — произвольная унитарная операция на одном кубите. Тогда *управляемое U* — это операция на двух кубитах, по-прежнему с управляющим и управляемым кубитами. Если управляющий

кубит установлен в единицу, то к управляемому кубиту применяется операция U , в противном случае управляемый кубит не меняется; иными словами, $|c\rangle|t\rangle \rightarrow |c\rangle U^c|t\rangle$. Графическое изображение элемента «управляемое U » показано на рис. 4.4.

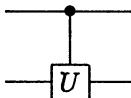
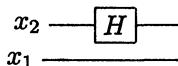
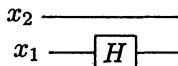


Рис. 4.4. Операция «управляемое U ». Верхний отрезок изображает управляющий кубит, нижний — управляемый. Если управляющий кубит установлен в единицу, то к управляемому кубиту применяется операция U , в противном случае управляемый кубит не меняется

Упражнение 4.16 (матричное представление элементов, действующих на нескольких кубитах). Как выглядит унитарная матрица 4×4 , соответствующая (в вычислительном базисе) нижеприведенной схеме



А какова унитарная матрица для следующей схемы?

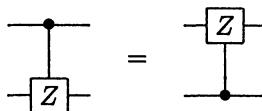


Упражнение 4.17 (построение СНОТ из управляемых Z-элементов). Постройте СНОТ из одного элемента «управляемый Z » (т. е. элемента, записывающегося в вычислительном базисе матрицей

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix},$$

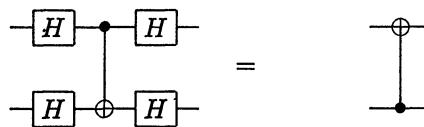
и двух элементов Адамара; укажите, какой кубит будет управляющим, а какой — управляемым.

Упражнение 4.18. Докажите, что



Упражнение 4.19 (действие СНОТ на матрицах плотности). Элемент СНОТ действует как перестановка базисных векторов, так что его действие на матрице плотности ρ сводится к перестановке матричных элементов. Выпишите это действие в явном виде (в вычислительном базисе).

Упражнение 4.20 (CNOT в измененном базисе). В отличие от классических элементов идеальные квантовые элементы не имеют, как сказал бы инженер-электрик, «входов с высоким импедансом». Действительно, выбор «управляющего» и «управляемого» кубитов произволен и зависит от того, в каком базисе действует оператор. Мы описали действие CNOT в вычислительном базисе, и в этом базисе значение управляющего кубита действительно не изменяется. Если, однако, сменить базис, то значение управляющего кубита изменяется: покажем, что в некотором базисе его фаза переворачивается в зависимости от состояния управляемого кубита! Докажите справедливость утверждения



Выберите в качестве базисных состояний $|\pm\rangle \equiv (|0\rangle \pm |1\rangle)/\sqrt{2}$ и покажите с помощью изображенного на рисунке тождества, что CNOT, у которого первый кубит считается управляющим, а второй — управляемым, действует следующим образом:

$$|+\rangle|+\rangle \rightarrow |+\rangle|+\rangle, \quad (4.24)$$

$$|-\rangle|+\rangle \rightarrow |-\rangle|+\rangle, \quad (4.25)$$

$$|+\rangle|- \rangle \rightarrow |-\rangle|- \rangle, \quad (4.26)$$

$$|-\rangle|- \rangle \rightarrow |+\rangle|- \rangle. \quad (4.27)$$

В этом новом базисе состояние управляемого кубита остается, тогда как состояние управляющего кубита изменяется, если управляемый кубит находится в состоянии $|-\rangle$, и не изменяется в противном случае. Таким образом, в этом базисе управляющий и управляемый кубиты поменялись ролями!

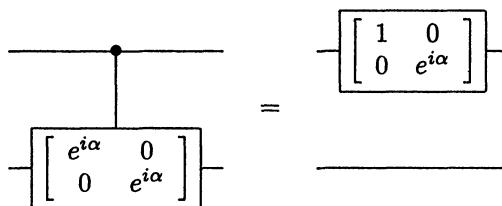


Рис. 4.5. Управляемый сдвиг фазы и эквивалентная ему схема на двух кубитах

Наша ближайшая цель — понять, как можно реализовать операцию «управляемое U » для произвольного U , действующего на одном кубите, с помощью операций на одном кубите и элемента CNOT. Наш план, основанный на разложении $U = e^{i\alpha}AXBXC$ (см. следствие 4.2) состоит из двух частей.

Вначале применим к управляемому кубиту сдвиг фазы $\exp(i\alpha)$, но не просто так, а в зависимости от состояния управляющего кубита. То есть, если управляющий кубит $|0\rangle$, то управляемый кубит не меняется, если же он равен $|1\rangle$, то к управляемому кубиту применяется сдвиг фазы на α . Схема, реализующая такую операцию с использованием элемента, действующего на одном кубите, изображена в правой части рис. 4.5. Чтобы убедиться в том, что данная схема действует именно так, как показано, заметим, что в вычислительном базисе это действие записывается следующим образом:

$$|00\rangle \rightarrow |00\rangle, \quad |01\rangle \rightarrow |01\rangle, \quad |10\rangle \rightarrow e^{i\alpha}|10\rangle, \quad |11\rangle \rightarrow e^{i\alpha}|11\rangle, \quad (4.28)$$

и это согласуется с нашим описанием.

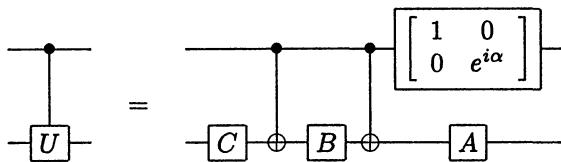


Рис. 4.6. Схема, реализующая операцию «управляемое U », где U — операция на одном кубите α , A , B и C удовлетворяют соотношениям $U = \exp(i\alpha)AXBXC$, $ABC = I$

Далее мы утверждаем, что схема, изложенная на рис. 4.6, реализует операцию «управляемое U ». Чтобы понять, почему это так, вспомним, что, согласно следствию 4.2, оператор U можно записать в виде $U = e^{i\alpha}AXBXC$, где A , B и C — такие операции на одном кубите, что $ABC = I$. Предположим, управляющий кубит установлен в единицу. Тогда операция $e^{i\alpha}AXBXC = U$ применяется ко второму кубиту. Если же управляющий кубит установлен в ноль, то ко второму кубиту применяется операция $ABC = I$, т. е. он не меняется. Значит, эта схема действительно реализует операцию «управляемое U ».

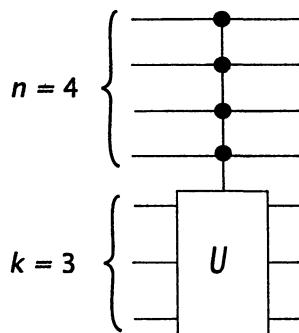


Рис. 4.7. Изображение операции $C^n(U)$, где U — унитарный оператор на k кубитах, $n = 4$, $k = 3$.

Теперь, когда мы знаем, как схемы выполняют условные операции, зависящие от состояния одного кубита, подумаем, как можно реализовать условные

операторы, зависящие от нескольких кубитов. Выше приводится пример такого оператора — это элемент Тоффоли, который меняет состояние третьего (управляемого) кубита при условии, что оба управляющих кубита установлены в единицу. Более общая ситуация: $(n+k)$ кубит, и U — унитарный оператор, действующий на k кубит. Определим операцию $C^n(U)$ по формуле

$$C^n(U)|x_1x_2\dots x_n\rangle|\psi\rangle=|x_1x_2\dots x_n\rangle U^{x_1x_2\dots x_n}|\psi\rangle, \quad (4.29)$$

где $x_1x_2\dots x_n$ в верхнем индексе U есть произведение битов x_1, x_2, \dots, x_n . Это означает, что оператор U применяется к k последним кубитам, если n первых кубитов установлены в единицу; в противном случае ничего не происходит. Такие условные операторы настолько важны, что полезно ввести для них специальное обозначение, рис. 4.7. В дальнейшем для простоты примем $k = 1$; случай больших k может быть разобран аналогичным способом, но при $k \geq 2$ возникает дополнительная трудность, состоящая в том, что мы (пока) не умеем выполнять произвольные операции на k кубитах.

Пусть U — унитарный оператор, действующий на одном кубите, и V — такой унитарный оператор, что $V^2 = U$. Тогда операция $C^2(U)$ может быть реализована с помощью схемы, изображенной на рис. 4.8.

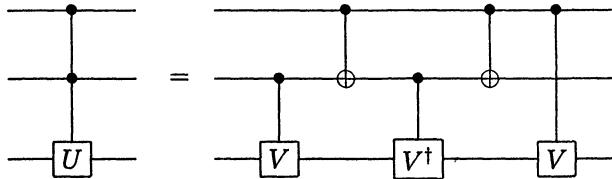


Рис. 4.8. Схема, реализующая элемент $C^2(U)$. V — произвольный унитарный оператор, удовлетворяющий условию $V^2 = U$. Если $V \equiv (1 - i)(I + iX)/2$, то получится элемент Тоффоли

Упражнение 4.21. Проверьте, что схема на рис. 4.8 выполняет операцию $C^2(U)$.

Упражнение 4.22. Докажите, что $C^2(U)$ для любого однокубитового оператора U может быть представлено схемой, состоящей из ≤ 8 однокубитовых элементов и 6 элементов CNOT.

Упражнение 4.23. Постройте схемы, реализующие $C^1(U)$ для $U = R_x(\theta)$ и $U = R_y(\theta)$, с помощью элемента CNOT и операций на одном кубите. Можно ли сократить число последних с трех до двух?

Знакомый нам элемент Тоффоли является особенно важным частным случаем операции $C^2(U)$, а именно операцией $C^2(X)$. Если определить V по формуле $V \equiv (1 - i)(I + iX)/2$ и заметить, что $V^2 = X$, то окажется, что на рис. 4.8 изображена реализация элемента Тоффоли с помощью одно- и двухкубитовых операций. С классической точки зрения это — удивительный результат: вспомните, что в задаче 3.5 мы убедились, что классических одно- и двухкубитовых обратимых элементов недостаточно для того, чтобы реализовать элемент

Тоффоли и тем самым универсальное вычисление. В квантовом случае мы, напротив, видим, что одно- и двухкубитовых обратимых элементов достаточно, чтобы реализовать элемент Тоффоли, а в дальнейшем мы докажем, что их достаточно и для выполнения универсального вычисления.

Ниже мы покажем, что всякую унитарную операцию можно с любой точностью аппроксимировать композицией таких элементов, как элемент Адамара, сдвиг фазы, CNOT и $\pi/8$. На рис. 4.9 изображена простая схема, реализующая элемент Тоффоли.

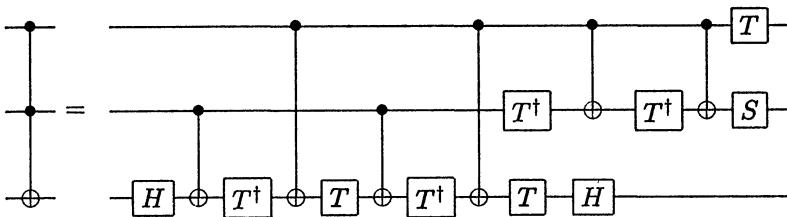


Рис. 4.9. Реализация элемента Тоффоли с помощью элемента Адамара, сдвига фазы, CNOT и $\pi/8$

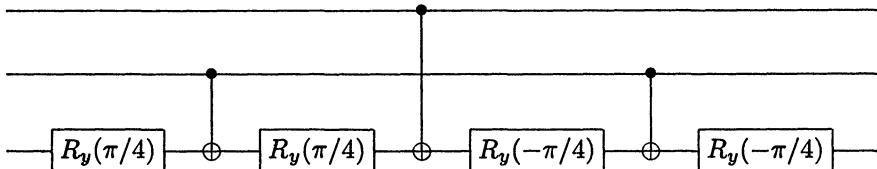
Упражнение 4.24. Проверьте, что на рис. 4.9 действительно изображена реализация элемента Тоффоли.

Упражнение 4.25 (реализация элемента Фредкина). Напомним, что элемент Фредкина (управляемый обмен) — это преобразование

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}. \quad (4.30)$$

1. Реализуйте элемент Фредкина с помощью квантовой схемы, использующей три элемента Тоффоли. (Указание: подумайте, как поменять местами значения двух булевых переменных с помощью трех сложений по модулю 2.)
2. Покажите, что первый и последний из этих элементов Тоффоли можно заменить на CNOT.
3. Замените средний элемент Тоффоли на схему, приведенную на рис. 4.8, и получите реализацию элемента Фредкина с использованием только шести двухкубитовых элементов.
4. Можно ли в этой последней конструкции обойтись лишь пятью двухкубитовыми элементами?

Упражнение 4.26. Покажите, что схема



отличается от элемента Тoffoli только относительными фазами: она переводит $|c_1, c_2, t\rangle$ в $e^{i\theta(c_1, c_2, t)}|c_1, c_2, t \oplus c_1 c_2\rangle$, где $e^{i\theta(c_1, c_2, t)}$ — относительный фазовый множитель. Такого рода схемы могут быть полезны в экспериментальных физических приложениях: может оказаться, что элемент, отличный от элемента Тoffoli на фазовый множитель, реализовать легче, чем сам элемент Тoffoli.

Упражнение 4.27. Пользуясь только элементами CNOT и Тoffoli, создайте квантовую схему, реализующую преобразование

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}. \quad (4.31)$$

Ниже (в гл. 7) мы воспользуемся такими «частичными циклическими перестановками».

Как можно реализовать $C^n(U)$, где U — произвольная операция на одном кубите, используя только набор известных нам элементов? Простая схема, дающая ответ на этот вопрос, изображена на рис. 4.10. Реализация проходит в три этапа с использованием небольшого числа ($n - 1$) рабочих кубитов, которые в начале и конце работы находятся в состоянии $|0\rangle$. Пусть управляющие кубиты находятся в состоянии $|c_1, c_2, \dots, c_n\rangle$ (мы работаем в вычислительном базисе). Первый этап работы схемы состоит в том, что над управляющими кубитами c_1, c_2, \dots, c_n производятся операции «обратимое AND», что дает в итоге произведение $c_1 \cdot c_2 \cdots c_n$. Для этого первый элемент в схеме проводит операцию AND над c_1 и c_2 с использованием элемента Тoffoli, в результате чего состояние первого рабочего кубита переходит в $|c_1 \cdot c_2\rangle$. Следующий элемент Тoffoli выполняет оператор над c_3 и $c_1 \cdot c_2$, так что состояние второго рабочего кубита переходит в $|c_1 \cdot c_2 \cdot c_3\rangle$. Продолжая применять таким образом элементы Тoffoli, придем к тому, что последний рабочий кубит окажется в состоянии $|c_1 \cdot c_2 \cdots c_n\rangle$. Теперь над управляемым кубитом проводится операция U (в случае, если последний рабочий кубит установлен в единицу, т.е. тогда и только тогда, когда в единицу установлены все кубиты от c_1 до c_n включительно). Наконец, на третьем этапе работы схемы первый этап повторяется в

обратном порядке, и все рабочие кубиты возвращаются в состояние $|0\rangle$). Общий итог состоит в том, что унитарный оператор U применяется к управляемому кубиту тогда и только тогда, когда управляющие кубиты c_1, \dots, c_n установлены в единицу, чего мы и хотели.

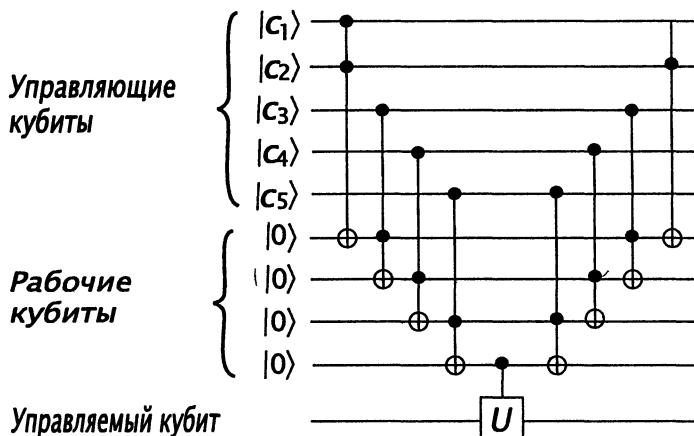


Рис. 4.10. Схема, реализующая $C^n(U)$, при $n = 5$

Упражнение 4.28. Пусть $U = V^2$, где V – унитарный оператор; постройте элемент $C^5(U)$, аналогичный использованному на рис. 4.10, без использования рабочих кубитов. Вы можете пользоваться элементами «управляемое V » и «управляемое V^\dagger ».

Упражнение 4.29. Постройте схему, использующую только элементы Тoffоли, CNOT и однокубитовые элементы, общим количеством $O(n^2)$, реализующую элемент $C^n(X)$ ($n > 3$) и не использующую рабочих кубитов.

Упражнение 4.30. Пусть U – унитарная операция на одном кубите. Постройте схему, использующую только элементы Тoffоли, CNOT и однокубитовые элементы, общим количеством $O(n^2)$, реализующую элемент $C^n(U)$ ($n > 3$) и не использующую рабочих кубитов.

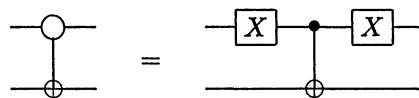


Рис. 4.11. Условная операция, в которой NOT применяется ко второму кубиту в зависимости от того, установлен ли первый кубит в нуль

До сих пор в условных операциях, которые мы рассматривали, оператор применялся к управляемому кубиту, если управляющие кубиты были установлены в единицу. Разумеется, единица в этой ситуации ничем не выделена, и

часто удобно рассматривать условные операции, в которых оператор применяется к управляемому кубиту, если управляющий кубит установлен в нуль. Пусть, например, нам нужна операция, при которой второй («управляемый») кубит изменяется, если первый («управляющий») кубит установлен в нуль. На рис. 4.11 приведено обозначение для элемента, осуществляющего такую операцию, а также реализацию этого элемента с помощью схемы, собранной из уже известных нам элементов. В дальнейшем белый кружок будет означать, что оператор применяется в случае, когда кубит установлен в нуль, а черный кружок — применение оператора в случае, если кубит установлен в единицу.

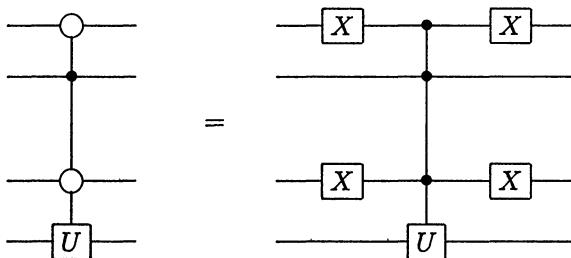


Рис. 4.12. Операция «управляемое U » и ее реализация с помощью уже известных нам элементов. Оператор U применяется к четвертому кубиту тогда и только тогда, когда первый и третий кубиты установлены в нуль, а второй — в единицу.

Более сложный пример использования этих обозначений, в котором используются три управляющих кубита, приведен на рис. 4.12. Оператор U применяется к управляемому кубиту, если первый и третий кубиты установлены в нуль, а второй — в единицу. Легко убедиться, что схема в правой части этого рисунка реализует именно эту операцию. В общем, легко перейти от схемы, в которой условия задаются в терминах равенства кубитов единице, к схеме, где условия задаются в терминах равенства кубитов нулю, путем добавления в подходящих местах элементов X , как на рис. 4.12.

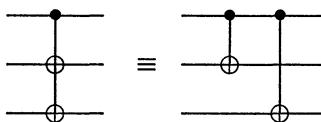


Рис. 4.13. Элемент CNOT с несколькими управляемыми кубитами

Другое соглашение, с помощью которого можно изображать управляемое NOT с несколькими управляемыми кубитами, иллюстрирует рис. 4.13. Приведенные обозначения следует понимать так: если управляющий кубит установлен в единицу, то все кубиты, помеченные знаком \oplus , меняются, — в противном случае ничего не происходит. Эти обозначения удобны, например, при построении таких классических функций как перестановки, или при кодировании и

декодировании в квантовых схемах с исправлением ошибок (см., например, гл. 10).

Упражнение 4.31 (еще несколько схемных тождеств). Условимся, что нижний индекс обозначает, на какой именно кубит действует оператор, и пусть C — операция CNOT, в которой кубит номер 1 — управляющий, а номер 2 — управляемый. Докажите следующие тождества:

$$CX_1C = X_1X_2, \quad (4.32)$$

$$CY_1C = Y_1X_2, \quad (4.33)$$

$$CZ_1C = Z_1, \quad (4.34)$$

$$CX_2C = X_2, \quad (4.35)$$

$$CY_2C = Z_1Y_2, \quad (4.36)$$

$$CZ_2C = Z_1Z_2, \quad (4.37)$$

$$R_{z,1}(\theta)C = CR_{z,1}(\theta), \quad (4.38)$$

$$R_{x,2}(\theta)C = CR_{x,2}(\theta). \quad (4.39)$$

4.4 Измерение

Последний ингредиент, используемый в квантовых схемах (иногда неявным образом), — это измерители. Будем обозначать проективное измерение в вычислительном базисе (подразд. 2.2.5) с помощью символа «измеритель», изображенного на рис. 4.14. В теории квантовых схем не принято пользоваться символами для измерений более общего вида, поскольку, как мы объясняли в гл. 2, их всегда можно реализовать с помощью композиции унитарных преобразований, использующих вспомогательные биты, и проективных измерений.

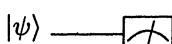


Рис. 4.14. Обозначение проективного измерения на одном кубите. В этой схеме с результатом измерения больше ничего не делается, но в общем случае его можно использовать для воздействия на поведение следующих элементов. Такое использование классической информации изображается с помощью «двойных линий» (на рисунке не показано)

Имея дело с квантовыми схемами, полезно иметь в виду два принципа, довольно очевидных, но заслуживающих вследствие своей важности явной формулировки. Первый из них состоит в том, что классические условные операции можно заменять квантовыми условными операциями:

Принцип отложенного измерения. Измерения всегда можно перенести в конец схемы; если на каком-то этапе работы схемы используются измерения, то в этом месте классические условные операции можно заменить квантовыми.

Часто квантовые измерения производятся в квантовой схеме на промежуточном этапе и результаты этих измерений подаются на вход условных квантовых элементов (см. например рис. 1.13). Однако такого рода измерения можно

всегда перенести в конец схемы. На рис. 4.15 показано как это можно сделать, заменив все классические условные операции соответствующими квантовыми. (Конечно, после этого нельзя говорить, что эта схема производит «телеportацию», поскольку никакой классической информации от Алисы к Бобу не передается, но ясно, что итоговое действие двух схем одно и то же, и это главное.)

Второй принцип еще более очевиден и удивительно полезен.

Принцип неявного измерения. Без потери общности можно считать, что все квантовые провода в схеме заканчиваются измерителями.

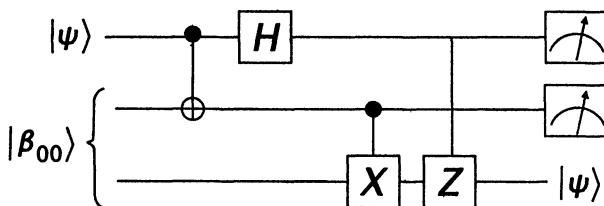


Рис. 4.15. Схема, реализующая квантовую телепортацию, в которой измерения производятся не в середине, а в конце схемы. Как и на рис. 1.13, два верхних кубита принадлежат Алисе, а нижний — Бобу

Чтобы понять, почему выполняется этот принцип, представим себе, что имеется квантовая схема, в которой участвуют лишь два кубита, и при этом в конце измеряется только первый из них. Тогда статистика измерений, производимых в этот момент, полностью определяется редуцированной матрицей плотности первого кубита. Однако, если измерить и второй кубит, то было бы весьма удивительно, если бы это измерение повлияло на статистику измерений первого кубита. Выполнив упр. 4.32, вы сможете доказать, что этого не произойдет, установив, что измерение второго кубита не влияет на редуцированную матрицу плотности первого кубита.

Важно иметь в виду, что измерения в квантовых схемах играют роль посредника между квантовым и классическим мирами; измерение обычно рассматривается как необратимая операция, разрушающая квантовую информацию и заменяющая ее на классическую. Если приложить усилия, то можно создать схему, в которой этого не будет происходить; яркими примерами являются телепортация и квантовое исправление ошибок (гл. 10). Общим у телепортации и квантового исправления ошибок является то, что в обоих случаях измерение не несет никакой информации об измеряемом квантовом состоянии. В гл. 10 будет показано, что это является общим свойством измерений: если мы хотим, чтобы измерение было обратимо, оно не должно нести информации об измеряемом квантовом состоянии!

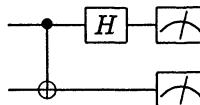
Упражнение 4.32. Пусть ρ — матрица плотности, описывающая двухкубитовую систему. Предположим, что мы производим проективное измерение второго кубита (в вычислительном базисе). Пусть $P_0 = |0\rangle\langle 0|$ и $P_1 = |1\rangle\langle 1|$ — проекторы на состояния $|0\rangle$ и $|1\rangle$ соответственно, а ρ' — матрица плотности системы

после измерения наблюдателем, не узнавшим результат измерения. Покажите, что имеет место формула

$$\rho' = P_0 \rho P_0 + P_1 \rho P_1. \quad (4.40)$$

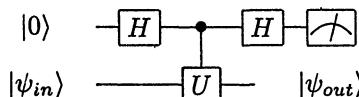
Покажите также, что редуцированная матрица плотности для первого кубита не меняется после измерения, т. е. $\text{tr}_2(\rho') = \text{tr}_2(\rho)$.

Упражнение 4.33 (измерения в базисе Белла). В модели измерений, которой мы пользовались при изучении квантовых схем, измерения проводятся только в вычислительном базисе. Однако часто возникает необходимость провести измерения в другом базисе, определенном полным набором ортонормальных состояний. Чтобы провести такое измерение, достаточно сначала перевести базис, в котором мы хотим провести измерение, в вычислительный (с помощью ортогонального преобразования), а затем измерить. Покажите, например, что схема

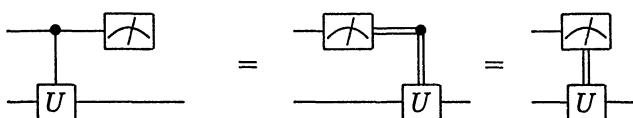


осуществляет измерение в базисе из белловских состояний. Точнее говоря, проверьте, что в результате работы этой схемы измеряются с помощью соответствующих POVM-элементов четыре проектора на белловские состояния. Каковы соответствующие измеряющие операторы?

Упражнение 4.34 (измерение оператора). Пусть имеется однокубитовый оператор U с собственными значениями ± 1 (так что U одновременно является эрмитовым и унитарным, и его можно рассматривать и как наблюдаемую, и как квантовый элемент). Предположим, мы хотим измерить наблюдаемую U , иными словами — получить результат измерения, равный одному из двух собственных значений, и при этом сделать так, чтобы состояние, в котором система окажется после измерения, совпадало с соответствующим собственным вектором. Как можно добиться этого с помощью квантовой схемы? Покажите, что приведенная ниже схема реализует измерение оператора U .



Упражнение 4.35 (измерение коммутирует с условными операциями). Из принципа отложенного измерения следует, что в случае, когда измеряется управляющий кубит, измерения коммутируют с условными элементами:



(Напомним, что двойные линии обозначают классические биты.) Докажите первое равенство. Крайняя справа схема — удобное обозначение для случая, когда результат измерения используется в качестве классического управляющего кубита.

4.5 Универсальные квантовые элементы

С помощью небольшого количества элементов (например, AND, OR, NOT) можно (см. подразд. 3.1.2) вычислить любую классическую функцию. В таких случаях говорят, что набор элементов является *универсальным* для классических вычислений. Действительно, поскольку элемент Тоффоли универсален для классических операций, с помощью квантовых схем можно выполнить все действия, реализуемые с помощью классических схем. Аналогичный вывод об универсальности верен и для квантовых вычислений, если назвать набор элементов *универсальным для квантовых вычислений* в том случае, когда любая унитарная операция может быть сколь угодно точно аппроксимирована квантовой схемой, содержащей только элементы из этого набора. Опишем три универсальные конструкции для квантовых вычислений. Эти конструкции построены одна на другой; в конечном счете получится, что любая унитарная операция может быть с произвольной точностью аппроксимирована с использованием следующих элементов: Адамара, сдвига фазы, CNOT и $\pi/8$. (Вы можете спросить, зачем включать в этот список сдвиг фазы, если его можно сконструировать из двух элементов $\pi/8$; дело в том, что сдвиг фазы естественно возникает в устойчивых к ошибкам конструкциях, описанных в гл. 10.)

Наша первая конструкция покажет, что любой унитарный оператор можно *точно* представить в виде композиции унитарных операторов, каждый из которых нетривиально действует только на подпространстве, порожденном двумя состояниями из вычислительного базиса. Вторая конструкция, объединяющая первую с результатами предыдущего подраздела, дает точное представление любого унитарного оператора в виде композиции однокубитовых операторов и элементов CNOT. Наконец, третья конструкция показывает, что однокубитовый оператор можно с произвольной точностью аппроксимировать композицией элементов Адамара, сдвига фазы и $\pi/8$; отсюда с учетом второй конструкции следует, что любой унитарный оператор можно с произвольной точностью аппроксимировать композицией элементов Адамара, сдвига фазы, CNOT и $\pi/8$.

Наши конструкции не позволяют оценить эффективность (полиномиальное или экспоненциальное количество элементов требуется для реализации данной унитарной операции?). В подразд. 4.5.4 будет показано, что существуют унитарные преобразования, для аппроксимации которых требуется экспоненциально много элементов. Разумеется, цель теории квантовых вычислений — найти интересные семейства унитарных операторов, которые *можно* выполнить эффективно.

Упражнение 4.36. Постройте квантовую схему, которая складывает два двухбитовых числа x и y по модулю 4. Иными словами, схема должна действовать по правилу $|x, y\rangle \rightarrow |x, x + y \bmod 4\rangle$.

4.5.1 Универсальность двухуровневых унитарных операторов

Рассмотрим унитарную матрицу U , действующую в d -мерном гильбертовом пространстве. В этом подразделе мы объясним, как можно разложить ее на произведение двухуровневых унитарных матриц, т. е. унитарных матриц, нетривиально действующих не более чем на двух базисных векторах. Основную идею, на которой основано это разложение, можно уяснить на примере 3×3 -матриц; итак предположим, что U имеет вид

$$U = \begin{bmatrix} a & d & g \\ b & e & h \\ c & f & j \end{bmatrix}. \quad (4.41)$$

Мы хотим найти такие двухуровневые унитарные матрицы U_1, U_2, U_3 , что

$$U_3 U_2 U_1 U = I. \quad (4.42)$$

Из этого равенства следует, что

$$U = U_1^\dagger U_2^\dagger U_3^\dagger. \quad (4.43)$$

Матрицы U_1, U_2 и U_3 , являются двухуровневыми унитарными. Нетрудно заметить, что таковы же и их обратные матрицы U_1^\dagger, U_2^\dagger и U_3^\dagger . Таким образом, если удастся доказать равенство (4.42), из этого будет следовать существование разложения матрицы U в произведение двухуровневых унитарных матриц.

Для построения U_1 воспользуемся следующей процедурой. Если $b = 0$, то положим

$$U_1 \equiv \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad (4.44)$$

а если $b \neq 0$, то

$$U_1 \equiv \begin{bmatrix} \frac{a^*}{\sqrt{|a|^2+|b|^2}} & \frac{b^*}{\sqrt{|a|^2+|b|^2}} & 0 \\ \frac{b}{\sqrt{|a|^2+|b|^2}} & \frac{-a}{\sqrt{|a|^2+|b|^2}} & 0 \\ 0 & 0 & 1 \end{bmatrix}. \quad (4.45)$$

Заметим, что в обоих случаях U_1 является двухуровневой унитарной матрицей, и что в результате ее умножения на U получим

$$\begin{bmatrix} a' & d' & g' \\ 0 & e' & h' \\ c' & f' & j' \end{bmatrix}. \quad (4.46)$$

Существенным моментом здесь служит то, что средний элемент в левом столбце равен нулю. Остальные элементы этой матрицы обозначим буквами со штрихами; их точные выражения для них нам не важны.

Теперь применим аналогичную процедуру, чтобы получить такую матрицу U_2 , что у произведения $U_2 U_1 U$ нуль стоит в левом нижнем углу. Именно, если $c' = 0$, положим

$$U_2 \equiv \begin{bmatrix} a'^* & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad (4.47)$$

а если $c' \neq 0$, то

$$U_2 \equiv \begin{bmatrix} \frac{a'^*}{\sqrt{|a'|^2 + |c'|^2}} & 0 & \frac{c'^*}{\sqrt{|a'|^2 + |c'|^2}} \\ 0 & 1 & 0 \\ \frac{c'}{\sqrt{|a'|^2 + |c'|^2}} & 0 & \frac{-a'}{\sqrt{|a'|^2 + |c'|^2}} \end{bmatrix}. \quad (4.48)$$

В каждом из этих случаев, если перемножить матрицы, получим

$$U_2 U_1 U = \begin{bmatrix} 1 & d'' & g'' \\ 0 & e'' & h'' \\ 0 & f'' & j'' \end{bmatrix}. \quad (4.49)$$

Так как матрицы U , U_1 и U_2 унитарны, то и матрица $U U_1 U_2$ унитарна, и тогда $d'' = g'' = 0$, поскольку норма первой строки должна быть равна единице. Положим, наконец,

$$U_3 \equiv \begin{bmatrix} 1 & 0 & 0 \\ 0 & e'^* & f'^* \\ 0 & h'^* & j'^* \end{bmatrix}. \quad (4.50)$$

Легко проверить, что $U_3 U_2 U_1 U = I$, так что $U = U_1^\dagger U_2^\dagger U_3^\dagger$, что и дает разложение U на произведение двухуровневых унитарных матриц.

Рассмотрим более общий случай. Предположим, что U действует на d -мерном пространстве. Тогда, действуя так же, как в 3×3 -мерном случае, можно найти такие двухуровневые матрицы U_1, \dots, U_{d-1} , что произведение $U_{d-1} U_{d-2} \dots U_1 U$ имеет единицу в верхнем левом углу и нули в остальных местах первой строки и первого столбца. Повторим эту процедуру для унитарной $(d-1) \times (d-1)$ -матрицы, полученной вычеркиванием из матрицы $U_{d-1} U_{d-2} \dots U_1 U$ первой строки и первого столбца, и т. д.; в конце концов мы придем к разложению

$$U = V_1 \dots V_k, \quad (4.51)$$

где V_i — двухуровневые унитарные матрицы и $k \leq (d-1) + (d-2) + \dots + 1 = d(d-1)/2$.

Упражнение 4.37. Разложите матрицу

$$\frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix} \quad (4.52)$$

на произведение двухуровневых унитарных матриц. (Это частный случай квантового преобразования Фурье; более подробно он будет рассмотрен в следующей главе.)

Из доказанного нами результата следует, что всякая унитарная матрица, действующая на n -кубитовой системе, может быть разложена в произведение не более чем $2^{n-1}(2^n - 1)$ двухуровневых унитарных матриц. Для конкретных унитарных матриц можно иногда найти гораздо более эффективное разложение, но, как вы сейчас докажете, существуют матрицы, которые *нельзя* разложить на произведение менее чем $d - 1$ двухуровневых унитарных матриц.

4.5.2 Универсальность набора из однокубитовых элементов и CNOT

Выше было показано, что любая унитарная матрица в d -мерном гильбертовом пространстве может быть разложена на произведение двухуровневых унитарных матриц. Теперь покажем, что однокубитовых элементов вместе с элементом CNOT достаточно, чтобы реализовать произвольную двухуровневую операцию на пространстве состояний n кубитов. Объединяя эти два результата, можно видеть, что с помощью однокубитовых и CNOT-элементов можно реализовать произвольную унитарную операцию на n кубитах, так что набор из двухкубитовых и CNOT-элементов универсален для квантовых вычислений.

Пусть U — двухуровневая унитарная матрица, действующая на n -кубитовом квантовом компьютере. Предположим, U действует нетривиально только на подпространстве, порожденном состояниями (из вычислительного базиса) $|s\rangle$ и $|t\rangle$, где $s = s_1 \dots s_n$ и $t = t_1 \dots t_n$ — двоичные разложения для s и t . Пусть \tilde{U} — нетривиальная унитарная 2×2 -подматрица матрицы U ; матрицу \tilde{U} можно рассматривать как унитарную матрицу, действующую на одном кубите.

Наша ближайшая цель — реализовать U с помощью схемы, состоящей из однокубитовых и CNOT-элементов. Для этого воспользуемся *кодами Грея*. Предположим, даны два разных двоичных числа s и t . Тогда *код Грея*, соединяющий s и t , — это последовательность двоичных чисел, начинающаяся s и заканчивающаяся t , которая обладает тем свойством, что два соседних числа в этой последовательности отличаются ровно в одной позиции. Если, например, $s = 101001$ и $t = 110011$, то код Грея выглядит как

$$\begin{array}{ccccccc} 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \end{array} \tag{4.53}$$

Пусть g_1, \dots, g_m — элементы кода Грея, соединяющего s и t , причем $g_1 = s$ и $g_m = t$. Отметим, что всегда можно найти код Грея, для которого $m \leq n + 1$, поскольку s и t могут отличаться не более чем в n местах.

Основная идея построения квантовой схемы, реализующей U , состоит в том, чтобы с помощью последовательности элементов провести преобразование $|g_1\rangle \rightarrow |g_2\rangle \rightarrow \dots \rightarrow |g_{m-1}\rangle$, затем провести операцию «управляемое \tilde{U} », у которой управляемый кубит соответствует тому единственному биту, в котором различаются g_{m-1} и g_m , и затем выполнить операции первого шага в обратном порядке $|g_{m-1}\rangle \rightarrow |g_{m-2}\rangle \rightarrow \dots \rightarrow |g_1\rangle$. Каждый из этих шагов легко выполнить с помощью операций, описанных выше в этой главе, а в результате получится реализация матрицы U .

Более подробное описание этой процедуры выглядит так. На первом шаге производится обмен состояний $|g_1\rangle$ и $|g_2\rangle$: если g_1 и g_2 различаются в i -ом бите, то применяется управляемое NOT к i -му кубиту при условии, что все остальные кубиты те же, что и остальные биты в g_1 и g_2 . Затем опять с помощью управляемой операции выполняется обмен $|g_2\rangle$ и $|g_3\rangle$ и т. д. — пока не произойдет обмен $|g_{m-2}\rangle$ и $|g_{m-1}\rangle$. В результате этих $(m - 2)$ операций имеет место перестановка

$$|g_1\rangle \rightarrow |g_{m-1}\rangle, \quad (4.54)$$

$$|g_2\rangle \rightarrow |g_1\rangle, \quad (4.55)$$

$$|g_3\rangle \rightarrow |g_2\rangle, \quad (4.56)$$

.....

$$|g_{m-1}\rangle \rightarrow |g_{m-2}\rangle, \quad (4.57)$$

а все остальные состояния из вычислительного базиса остаются неизменными. Предположим теперь, что g_{m-1} и g_m отличаются в j -ом бите. Применим управляемое \tilde{U} , для которого управляемым будет j -й кубит, при условии, что значения всех остальных кубитов — те же, что у остальных битов в g_{m-1} и g_m . Наконец, проведем обмен в обратном порядке: обменяем $|g_{m-1}\rangle$ с $|g_{m-2}\rangle$, затем $|g_{m-2}\rangle$ с $|g_{m-3}\rangle$ и т. д., пока не обменяются $|g_2\rangle$ и $|g_1\rangle$.

Данную процедуру можно проиллюстрировать на простом примере. Предположим, необходимо выполнить преобразование, имеющее вид

$$U = \begin{bmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{bmatrix}. \quad (4.58)$$

Здесь a , b , c и d — произвольные комплексные числа, обладающие тем свойством, что $\tilde{U} \equiv \begin{bmatrix} a & c \\ b & d \end{bmatrix}$ — унитарная матрица. Заметим, что U действует

нетривиально только на состояния $|000\rangle$ и $|111\rangle$. Запишем код Грэя, соединяющий 000 и 111:

A	B	C	
0	0	0	
0	0	1	
0	1	1	
1	1	1	

(4.59)

Отсюда можно получить требуемую схему (рис. 4.16). Первые два элемента переставляют состояния таким образом, что $|000\rangle$ обменивается с $|011\rangle$. Затем операция \hat{U} применяется к первому кубиту состояний $|011\rangle$ и $|111\rangle$ при условии, что второй и третий кубиты находятся в состоянии $|11\rangle$. Наконец, мы снова переставляем состояния, в результате чего $|011\rangle$ снова меняется с $|000\rangle$.

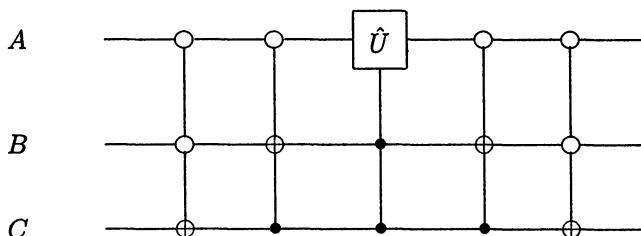


Рис. 4.16. Схема, реализующая двухуровневую унитарную операцию, заданную матрицей (4.58)

В общем случае можно сформулировать, что для реализации двухуровневого унитарного оператора требуется не более $2(n - 1)$ условных операций (чтобы обменять $|g_1\rangle$ с $|g_{m-1}\rangle$, а затем произвести обратный обмен). Каждую из этих операций можно выполнить с помощью $O(n)$ однокубитовых и CNOT-элементов; для управляемого \hat{U} также необходимо $O(n)$ элементов. Таким образом, U реализуется с помощью $O(n^2)$ однокубитовых и CNOT-элементов. В предыдущем разделе мы видели, что произвольная унитарная матрица на 2^n -мерном пространстве состояний n кубитов может быть записана как произведение $O(2^{2n}) = O(4^n)$ двухуровневых унитарных матриц. Объединяя эти результаты, получим, что любая унитарная операция на n кубитах может быть осуществлена с помощью схемы, содержащей $O(n^2 4^n)$ однокубитовых и CNOT-элементов. Ясно, что эта процедура дает не самые эффективные квантовые схемы! Тем не менее в подразд. 4.5.4 будет показано, что данная конструкция близка к оптимальной в том смысле, что существуют унитарные операции, для реализации которых необходимо экспоненциальное количество элементов. Значит, для нахождения быстрых квантовых алгоритмов требуется подход, отличный от примененного в доказательстве универсальности.

Упражнение 4.39. Найдите квантовую схему из однокубитовых и СНОТ-элементов, реализующую преобразование

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & c \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & b & 0 & 0 & 0 & 0 & d \end{bmatrix}, \quad (4.60)$$

где $\tilde{U} = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$ — произвольная унитарная 2×2 -матрица.

4.5.3 Конечный набор универсальных операций

В предыдущем подразделе было показано, что СНОТ и однокубитовые унитарные операторы образуют универсальное семейство для квантовых вычислений. К сожалению, неизвестен прямой метод, позволяющий реализовать все эти элементы устойчивым к ошибкам образом. Однако, в этом подразделе мы найдем конечный набор элементов, с помощью которого можно проводить универсальные квантовые вычисления, а в гл. 10 будет показано, как использовать квантовые коды, исправляющие ошибки, для устойчивой к ошибкам реализации этих элементов.

Аппроксимация унитарных операторов

Ясно, что с помощью конечного набора элементов невозможно *точно* реализовать произвольный унитарный оператор, поскольку множество унитарных операторов имеет мощность континуум. Тем не менее оказывается, что с помощью конечного множества можно *аппроксимировать* любую унитарную операцию. Чтобы знать, как это получается, необходимо понять, что такая аппроксимация унитарного оператора вообще. Пусть U и V — два унитарных оператора на одном и том же пространстве состояний, причем U — тот оператор, который мы хотим приближенно реализовать, а V — его приближенная реализация. Определим *ошибку* по формуле

$$E(U, V) \equiv \max_{|\psi\rangle} \|(U - V)|\psi\rangle\|, \quad (4.61)$$

где максимум берется по всем нормализованным квантовым состояниям $|\psi\rangle$ в пространстве состояний. Во вставке 4.1 будет показано, что определенная таким образом ошибка обладает следующим свойством: если $E(U, V)$ мало, то для любого начального состояния $|\psi\rangle$ всякое измерение состояния $V(|\psi\rangle)$ дает примерно ту же статистику измерений, что и измерение состояния $U(|\psi\rangle)$.

Точнее говоря, если M есть POVM-элемент в произвольном POVM и если P_U (соответственно P_V) — вероятность получения этого результата при применении U (соответственно V) к начальному состоянию $|\psi\rangle$, то

$$|P_U - P_V| \leq 2E(U, V). \quad (4.62)$$

Таким образом, если $E(U, V)$ мал, то результаты измерений имеют близкие вероятности, будь то измерение U или V . Во вставке 4.1 также показано, что если применить последовательно элементы V_1, \dots, V_m , являющиеся приближениями к элементам U_1, \dots, U_m , то ошибки накапливаются не более, чем линейно:

$$E(U_m U_{m-1} \dots U_1, V_m V_{m-1} \dots V_1) \leq \sum_{j=1}^m E(U_j, V_j). \quad (4.63)$$

Вставка 4.1. Аппроксимация квантовых схем

Пусть квантовая система первоначально находится в состоянии $|\psi\rangle$ и над ней выполняется либо унитарная операция U , либо унитарная операция V . После этого проводится измерение. Пусть M — POVM-элемент, отвечающий этому измерению и P_U (соответственно P_V) — вероятность получения соответствующего M результата измерений после выполнения операции U (соответственно V). Тогда имеем

$$|P_U - P_V| = |\langle\psi|U^\dagger MU|\psi\rangle - \langle\psi|V^\dagger MV|\psi\rangle|. \quad (4.64)$$

Положим $|\Delta\rangle \equiv (U - V)|\psi\rangle$. Простые выкладки с использованием неравенства Коши–Шварца показывают, что

$$|P_U - P_V| = |\langle\psi|U^\dagger M|\Delta\rangle| + \langle\Delta|M V|\psi\rangle \quad (4.65)$$

$$\leq |\langle\psi|U^\dagger M|\Delta\rangle| + |\langle\Delta|M V|\psi\rangle| \quad (4.66)$$

$$\leq \|\Delta\| + \|\Delta\| \quad (4.67)$$

$$\leq 2E(U, V). \quad (4.68)$$

Неравенство $|P_U - P_V| \leq 2E(U, V)$ является количественным выражением того обстоятельства, что при малой ошибке $E(U, V)$ разность вероятностей соответствующих результатов измерений также мала.

Пусть теперь мы применили последовательность операторов V_1, V_2, \dots, V_m , являющихся приближениями к операторам U_1, U_2, \dots, U_m соответственно. Тогда оказывается, что ошибка, вызываемая применением этой последовательности «несовершенных» операторов, не превосходит суммы ошибок отдельных операторов:

$$E(U_m U_{m-1} \dots U_1, V_m V_{m-1} \dots V_1) \leq \sum_{j=1}^m E(U_j, V_j). \quad (4.69)$$

Доказательство этого начнем с рассмотрения случая $m = 2$. Заметим, что для некоторого состояния $|\psi\rangle$ имеем

$$E(U_2U_1, V_2V_1) = \|(U_2U_1 - V_2V_1)|\psi\rangle\| \quad (4.70)$$

$$= \|(U_2U_1 - V_2U_1)|\psi\rangle + (V_2U_1 - V_2V_1)|\psi\rangle\|. \quad (4.71)$$

Пользуясь неравенством треугольника $\||a\rangle + |b\rangle\| \leq \||a\rangle\| + \||b\rangle\|$, получим

$$E(U_2U_1, V_2V_1) \leq \|(U_2 - V_2)U_1|\psi\rangle\| + \|V_2(U_1 - V_1)|\psi\rangle\| \quad (4.72)$$

$$\leq E(U_2, V_2) + E(U_1, V_1), \quad (4.73)$$

что и требовалось доказать. Результат для произвольного m выводится отсюда по индукции.

Неравенства (4.62) и (4.63) очень полезны. Действительно, предположим, мы хотим провести вычисления с помощью квантовой схемы, состоящей из m элементов U_1, \dots, U_m . К сожалению, все, что мы можем, — это аппроксимировать элементы U_j с помощью элементов V_j . Для того чтобы вероятности результатов измерений приближенной схемы не более чем на $\Delta > 0$ отличались от истинных вероятностей, достаточно, учитывая неравенства (4.62) и (4.63), добиться того, чтобы выполнялось неравенство $E(U_j, V_j) \leq \Delta/2m$.

Универсальность набора, состоящего из элементов Адамара, сдвига фазы, CNOT и $\pi/8$

Теперь мы, наконец, можем изучить аппроксимацию произвольных унитарных операторов с помощью конечного набора элементов. Рассмотрим два разных конечных набора, каждый из которых является универсальным. Первый из них, называемый *стандартным универсальным набором*, состоит из элементов Адамара, сдвига фазы, CNOT и $\pi/8$. В гл. 10 будут приведены конструкции устойчивых к ошибкам реализаций этих элементов; доказательство универсальности этого набора очень простое. Второй набор состоит из элементов Адамара, сдвига фазы, CNOT и Тоффоли. Упомянутые элементы также можно реализовать устойчивым способом, но доказательство универсальности и устойчивая к ошибкам реализация в этом случае более трудные.

Начнем доказательство универсальности с того, что установим, что с помощью элемента Адамара и элемента $\pi/8$ любую однокубитовую операцию можно аппроксимировать с произвольной точностью. Рассмотрим элементы T и HTH . Элемент T является с точностью до не играющего роли общего фазового множителя поворотом сферы Блоха на угол $\pi/4$ относительно оси \hat{z} , а элемент HTH — поворот той же сферы на $\pi/4$ относительно оси \hat{x} (упр. 4.14). Взяв композицию этих двух операций, получим с точностью до общей фазы соотношения

$$\exp\left(-i\frac{\pi}{8}Z\right)\exp\left(-i\frac{\pi}{8}X\right) = \left[\cos\frac{\pi}{8}I - i\sin\frac{\pi}{8}Z\right]\left[\cos\frac{\pi}{8}I - i\sin\frac{\pi}{8}X\right] \quad (4.74)$$

$$= \cos^2\frac{\pi}{8}I - i\left[\cos\frac{\pi}{8}(X+Z) + \sin\frac{\pi}{8}Y\right]\sin\frac{\pi}{8}. \quad (4.75)$$

Это — поворот блоховской сферы относительно оси, параллельной вектору $\vec{n} = (\cos\frac{\pi}{8}, \sin\frac{\pi}{8}, \cos\frac{\pi}{8})$ (обозначим соответствующий единичный вектор через \hat{n}) на угол θ , определяемый из соотношения $\cos(\theta/2) \equiv \cos^2\frac{\pi}{8}$. Значит, пользуясь только элементом Адамара и элементом $\pi/8$, можно сконструировать $R_{\hat{n}}(\theta)$. Более того, можно показать, что отношение этого угла θ к 2π иррационально; доказательство последнего факта выходит за рамки нашей книги (см. «Историю и дополнительную литературу» в конце главы).

Теперь покажем, что итерациями $R_{\hat{n}}(\theta)$, можно с произвольной точностью аппроксимировать любой поворот вида $R_{\hat{n}}(\alpha)$. Пусть нам нужна аппроксимация с точностью $\delta > 0$ и N — целое число, большее $2\pi/\delta$. Определим θ_k исходя из соотношений $\theta_k \in [0; 2\pi]$ и $\theta_k = k\theta \bmod 2\pi$. Из принципа Дирихле вытекает, что на отрезке $[1; N]$ найдутся два различных целых числа j и k , обладающих тем свойством, что $|\theta_k - \theta_j| \leq 2\pi/Nj$, так что имеем $|\theta_{k-j}| < \delta$. Поскольку $j \neq k$, и θ есть иррациональное кратное 2π , имеем $\theta_{k-j} \neq 0$. Отсюда следует, что члены последовательности $\theta_{l(k-j)}$, где l варьируется, можно расположить на интервале $[0; 2\pi)$ таким образом, чтобы соседние числа отличались друг от друга не более чем на δ . Отсюда следует, что для всякого $\varepsilon > 0$ существует такое n , что

$$E(R_{\hat{n}}(\alpha), R_{\hat{n}}(\theta)^n) < \frac{\varepsilon}{3}. \quad (4.76)$$

Упражнение 4.40. Покажите, что для любых α и β выполнено неравенство

$$E(R_{\hat{n}}(\alpha), R_{\hat{n}}(\alpha + \beta)) = |1 - \exp(i\beta/2)|, \quad (4.77)$$

и выведите отсюда (4.76).

Теперь мы можем доказать, что любая однокубитовая операция может быть с произвольной точностью аппроксимирована с помощью элементов Адамара и $\pi/8$. Простые алгебраические выкладки показывают, что для любого α имеем

$$HR_{\hat{n}}(\alpha)H = R_{\hat{m}}(\alpha), \quad (4.78)$$

где \hat{m} — единичный вектор, идущий в направлении $(\cos\frac{\pi}{8}, -\sin\frac{\pi}{8}, \cos\frac{\pi}{8})$, откуда следует, что

$$E(R_{\hat{m}}(\alpha), R_{\hat{m}}(\theta)^n) < \frac{\varepsilon}{3}. \quad (4.79)$$

Однако (с учетом упр. 4.11) всякий унитарный однокубитовый оператор U можно записать в виде

$$U = R_{\hat{n}}(\beta)R_{\hat{m}}(\gamma)R_{\hat{n}}(\delta) \quad (4.80)$$

(с точностью до несущественного общего фазового множителя). Формулы (4.76) и (4.79) вместе с неравенством (4.63) показывают, что для подходящих целых положительных чисел n_1 , n_2 и n_3 имеем

$$E(U, R_{\hat{n}}(\theta)^n H R_{\hat{n}}(\theta)^{n_2} H R_{\hat{n}}(\theta)^{n_3}) < \varepsilon. \quad (4.81)$$

Таким образом, для любого унитарного однокубитового оператора U и любого $\varepsilon > 0$ можно аппроксимировать U с ошибкой, не превосходящей ε , с помощью схемы, состоящей из элементов Адамара и $\pi/8$.

Коль скоро элементы $\pi/8$ и Адамара позволяют аппроксимировать любой однокубитовый унитарный оператор, из рассуждений в подразд. 4.5.2 вытекает, что можно аппроксимировать и любую m -элементную квантовую схему. А именно, если схема состоит из m элементов, являющихся либо CNOT, либо однокубитовыми операторами, ее можно аппроксимировать с помощью элементов Адамара, CNOT и $\pi/8$ (в дальнейшем мы увидим, что использование элемента сдвига фазы позволяет сделать это приближение устойчивым к ошибкам, но для доказательства универсальности это уточнение не является необходимым). Если ошибка не должна превосходить ε для схемы в целом, то этого можно добиться, аппроксимируя каждый однокубитовый унитарный оператор с точностью до ε/m : неравенство (4.63) показывает, что для схемы в целом ошибка будет не больше ε .

Насколько эффективна описанная процедура аппроксимации квантовых схем с помощью конечного набора элементов? Это — важный вопрос. Предположим, например, что для аппроксимации однокубитового оператора с точностью ε требуется $\Omega(2^{1/\varepsilon})$ элементов из нашего набора; тогда для аппроксимации m -элементной схемы, о которой шла речь в предыдущем абзаце, потребуется $\Omega(m2^{m/\varepsilon})$ элементов — экспоненциально больше, чем исходный размер схемы! В действительности, однако, скорость сходимости гораздо выше. Интуитивно ясно, что последовательность углов θ_k заполняет интервал $[0; 2\pi)$ более или менее равномерно, так что для аппроксимации однокубитового оператора требуется $\sim \Theta(1/\varepsilon)$ элементов. Если принять такую оценку, то число элементов, необходимое для аппроксимации m -элементной схемы, равно $\Theta(m^2/\varepsilon)$. Это — квадратичное увеличение размера схемы, что может оказаться приемлемым для многих приложений.

Замечательно, что на самом деле скорость сходимости гораздо выше. *Теорема Соловея–Китаева* (см. Приложении 3) гласит, что любой однокубитовый унитарный оператор может быть приближен с точностью ε с использованием $O(\log^c(1/\varepsilon))$ элементов из нашего конечного набора, где c — константа, примерно равная 2. Тем самым из этой теоремы следует, что для аппроксимации с точностью ε схемы, состоящей из m элементов CNOT и однокубитовых унитарных операторов, достаточно $O(m \log^c(m/\varepsilon))$ элементов из конечного набора, что дает лишь полулогарифмическое увеличение размера схемы, которое, по-видимому, приемлемо для всех приложений.

Подведем итоги. Было показано, что набор, состоящий из элементов Адамара, сдвига фазы, CNOT и $\pi/8$, универсален для квантовых вычислений в том смысле, что любую схему, состоящую из CNOT и однокубитовых унитарных операторов, можно с хорошей точностью аппроксимировать с помощью схемы, содержащей только элементы из этого набора. Более того, это приближение

может быть реализовано эффективно в том смысле, что размер схемы увеличивается в количестве раз, которое полиномиально относительно $\log(m/\varepsilon)$, где m — количество элементов в исходной схеме и ε — точность приближения.

Упражнение 4.41. В этом и двух следующих упражнениях изложена конструкция, показывающая, что семейство, состоящее из элементов Адамара, сдвига фазы, СНОТ и Тоффоли, является универсальным.

Покажите, что схема на рис. 4.17 производит над третьим (управляющим) кубитом операцию $R_z(\theta)$, где $\cos \theta = 3/5$, если результаты обоих измерений равны нулю, а в противном случае применяет к управляемому кубиту операцию Z . Проверьте, что вероятность того, что результаты обоих измерений равны нулю, равна $5/8$, и объясните, как с помощью многократного применения этой схемы и элемента $Z = S^2$ можно получить $R_z(\theta)$ с вероятностью, стремящейся к единице.

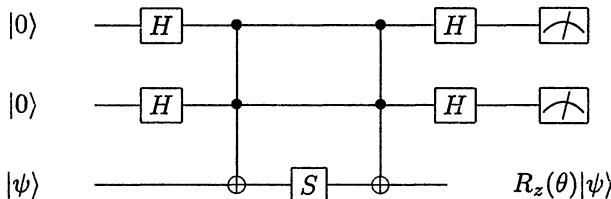


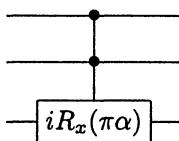
Рис. 4.17. Если результаты обоих измерений равны нулю, эта схема применяется к управляемому кубиту оператор $R_z(\theta)$, где $\cos \theta = 3/5$. Если результаты измерений другие, используется оператор Z .

Упражнение 4.42 (иррациональность θ). Пусть $\cos \theta = 3/5$. Докажите от противного, что θ несоизмеримо с 2π .

1. Пользуясь тем, что $e^{i\theta} = (3 + 4i)/5$, покажите, что если θ рационально, то существует такое целое положительное число m , что $(3 + 4i)^m = 5^m$.
2. Покажите, что $(3 + 4i)^m \equiv 3 + 4i \pmod{5}$ для всех $m > 0$, и выведите отсюда, что равенство $(3 + 4i)^m = 5^m$ невозможно.

Упражнение 4.43. Выполните из результатов двух предыдущих упражнений, что набор, состоящий из элементов Адамара, сдвига фазы, Тоффоли и СНОТ, является универсальным для квантовых вычислений.

Упражнение 4.44. Покажите, что трехкубитовый элемент G , определяемый приведенной на рисунке схемой,



является универсальным при иррациональном α .

Упражнение 4.45. Пусть U — унитарное преобразование, реализованное с помощью n -кубитовой квантовой схемы, состоящей из элементов H , S , СПОТ и Тoffоли. Покажите, что U имеет вид $2^{-k/2}M$, где k — целое число, а M — матрица размера $2^n \times 2^n$, элементы которой — комплексные числа с целыми действительной и мнимой частями. Выполните то же упражнение с элементом $\pi/8$ вместо элемента Тoffоли.

4.5.4 Трудность аппроксимации общего унитарного оператора в общем случае

Было показано, что произвольное унитарное преобразование на n кубит можно выполнить, используя ограниченный набор элементов. Всегда ли можно сделать это эффективно? Иными словами: существует ли для данного унитарного преобразования U на n кубитах, аппроксимирующая его схема, размер которой полиномиален по n ? Ответ на этот вопрос — решительное «нет»; естественно, большая часть унитарных преобразований может быть реализована только очень неэффективным образом. Чтобы понять причину этого явления, зададимся следующим вопросом: сколько требуется элементов, чтобы создать произвольное n -кубитовое состояние? Простой подсчет показывает, что, вообще говоря, требуемое количество экспоненциально. Предположим, что в нашем распоряжении имеется g разных элементов, каждый из которых действует не более чем на f входных кубитов. Числа f и g определяются используемым оборудованием и поэтому могут считаться постоянными. Пусть у нас имеется квантовая схема из t элементов, на вход которой подано состояние $|0\rangle^n$ из вычислительного базиса. Каждый элемент может перевести этот вектор в одно из не более чем $\binom{n}{f}^g = O(n^{fg})$ состояний, так что схема из t элементов может вычислить не более $O(n^{ftg})$ различных состояний.

Пусть теперь мы хотим приблизить состояние $|\psi\rangle$ с точностью до ϵ . Идея доказательства состоит в том, чтобы покрыть множество всех возможных состояний набором «кружков» радиуса ϵ (рис. 4.18), а затем показать, что количество кружков растет дважды экспоненциально по n ; сравнив с экспоненциальным количеством всевозможных состояний, которые можно получить на t элементах, получим желаемый результат. Заметим, что пространство векторов состояний n кубитов можно рассматривать как единичную $(2^{n+1}-1)$ -мерную сферу. Действительно, пусть состояние n кубит имеет амплитуды $\psi_j = X_j + iY_j$, где X_j и Y_j — действительная и мнимая части j -й амплитуды. Условие нормализации для квантовых состояний можно записать в виде $\sum_j (X_j^2 + Y_j^2) = 1$, а это и есть условие того, что точка лежит на единичной сфере в 2^{n+1} -мерном вещественном пространстве, т. е. на $(2^{n+1}-1)$ -мерной сфере. Аналогичным образом, площадь поверхности «кружка» радиуса ϵ с центром $|\psi\rangle$ примерно равна объему, ограниченному $(2^{n+1}-2)$ -мерной сферой радиуса ϵ . Пользуясь формулами $S_k(r) = 2\pi^{(k+1)/2}r^k/\Gamma((k+1)/2)$ для площади поверхности k -мерной сферы радиуса r и $V_k(r) = 2\pi^{(k+1)/2}r^{k+1}/((k+1)\Gamma((k+1)/2))$ для объема $(k+1)$ -мерного шара радиуса r , получим, что количество «кружков»,

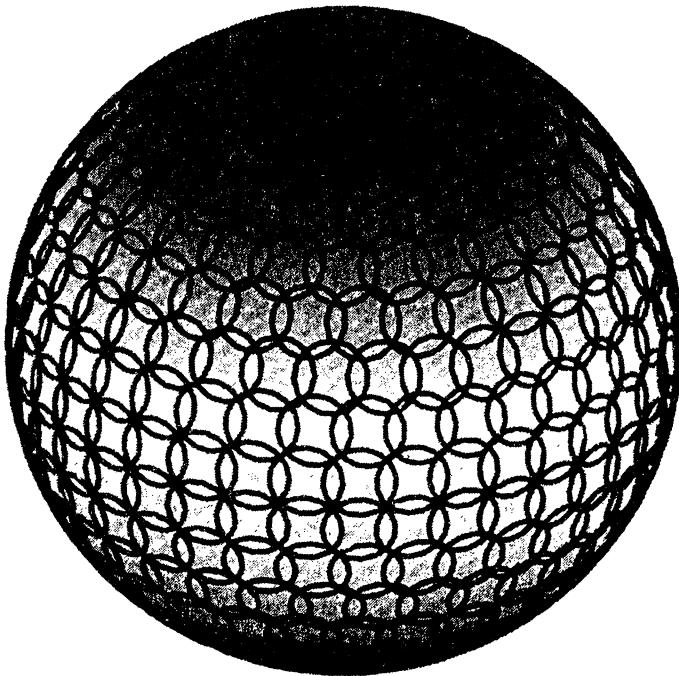


Рис. 4.18. Покрытие множества возможных состояний кружками постоянного радиуса

необходимое для покрытия всего пространства состояний, примерно равно

$$\frac{S_{2^n+1-1}(1)}{V_{2^n+1-2}(\varepsilon)} = \frac{\sqrt{\pi}\Gamma(2^n - \frac{1}{2})(2^{n+1} - 1)}{\Gamma(2^n)\varepsilon^{2^{n+1}-1}}, \quad (4.82)$$

где Γ — обычная гамма-функция. Однако $\Gamma(2^n - \frac{1}{2}) \geq \Gamma(2^n)/2^n$, так что число «кружков» не меньше чем

$$\Omega\left(\frac{1}{\varepsilon^{2^{n+1}-1}}\right). \quad (4.83)$$

Как мы помним, что с помощью m элементов можно покрыть лишь $O(n^{fgm})$ кружков, поэтому для того, чтобы можно было покрыть все «кружки» радиуса ε , необходимо выполнение условия

$$O(n^{fgm}) \geq \Omega\left(\frac{1}{\varepsilon^{2^{n+1}-1}}\right), \quad (4.84)$$

откуда следует

$$m = \Omega\left(\frac{2^n \log(1/\varepsilon)}{\log(n)}\right). \quad (4.85)$$

Значит, существуют состояния n кубитов, которые можно аппроксимировать с точностью ε с помощью не менее чем $\Omega(2^n \log(1/\varepsilon) / \log(n))$ операций. Это экспоненциально по n , и тем самым это трудно в смысле сложности вычислений (см. гл. 3). Более того, отсюда непосредственно следует, что существуют n -кубитовые унитарные операторы U , для аппроксимации которых схемой V (при условии $E(U, V) \leq \varepsilon$) требуется $\Omega(2^n \log(1/\varepsilon) / \log(n))$ элементов. В то же время из нашего доказательства универсальности и теоремы Соловея–Китаева вытекает, что любой n -кубитовый унитарный оператор U может быть аппроксимирован с точностью ε с помощью $O(n^2 4^n \log^c(n^2 4^n / c))$ элементов. Таким образом, описанная выше универсальная конструкция оптимальна с точностью «до полинома»; к сожалению, она не помогает понять, какие унитарные операции могут быть эффективно вычислены в модели квантовых схем.

4.5.5 Сложность квантовых вычислений

Гл. 3 была посвящена сложности вычислений на классических компьютерах. Неудивительно, что и применительно к квантовым компьютерам было бы интересно развить теорию сложности, которая давала бы ответ на вопрос, какие ресурсы требуются для квантовых вычислений, а также сравнить эту теорию с классической теорией сложности. Пока что в этом направлении сделаны лишь первые шаги, но эта тема, несомненно, еще принесет множество открытий будущим исследователям. Мы же ограничимся изложением только одного результата из квантовой теории сложности, а именно: установим связь между квантовым классом сложности **BQP** и классическим классом сложности **PSPACE**. Обсудим этот результат неформально; более подробное рассмотрение содержится в статье Бернштейна и Вазирани (см. раздел «История и дополнительная литература» в конце главы).

Напомним, что класс **PSPACE** был определен в гл. 3 как класс задач разрешения, которые могут быть решены на машине Тьюринга с использованием объема памяти, полиномиально зависящего от размера задачи, и без ограничений на время. Что касается **BQP**, то это — квантовый класс сложности, состоящий из задач разрешения, которые могут быть решены с ограниченной вероятностью ошибки с помощью квантовой схемы полиномиального размера. Если выражаться более формально, то язык L лежит в классе **BQP** тогда и только тогда, когда существует имеющее полиномиальный размер однородное семейство квантовых схем, которые принимают строки, принадлежащие языку, с вероятностью не менее $3/4$ и отвергают строки, ему не принадлежащие, с вероятностью также не менее $3/4$. Это означает, что на вход квантовых схем поступают двоичные строки, а в конце схемы измеряется один кубит; если в результате измерения получается 0, то строка принята, если 1, то отвергнута. Проверяя одну и ту же строку несколько раз, можно заключить, принадлежит ли она языку L , с очень высокой вероятностью правильного ответа.

Разумеется, квантовая схема имеет фиксированное число входов, и любая данная схема может решить, принадлежат ли языку L строки, длина которых ограничена сверху некоторым числом. Поэтому в определении класса **BQP**

используется целое семейство схем: для каждой длины входного слова — своя схема. При этом мы налагаем на эти схемы два дополнительных условия. Во-первых, размер схемы, которую мы применяем ко входной строке $x \in L$, должен быть ограничен сверху полиномом от длины x . Во-вторых, семейство схем должно быть *однородным* в том смысле, как данный термин употребляется в подразд. 3.1.2. Это означает следующее. Пусть дана строка x длиной n , и мы хотим построить схему, выясняющую, лежит ли она в языке L . Так вот, необходимо иметь алгоритм для построения такой схемы, точнее говоря, должна существовать машина Тьюринга, выдающая описание искомой схемы. Указанное ограничение может показаться техническим, и на практике оно почти всегда тривиальным образом выполняется, но оно ограждает нас от патологических контрпримеров, подобных описанным в подразд. 3.1.2. (У читателя может также возникнуть вопрос, о какой машине Тьюринга шла речь в этом определении — классической или квантовой; оказывается, это неважно — см. разд. «История и дополнительная литература».)

Один из наиболее значительных результатов в квантовой теории сложности состоит в том, что $\text{BQP} \subseteq \text{PSPACE}$. Поскольку ясно, что $\text{BPP} \subseteq \text{BQP}$, где BPP — классический класс сложности, состоящий из задач разрешения, которые можно решить за полиномиальное время на классической машине Тьюринга с ограниченной вероятностью ошибки, имеется цепочка включений $\text{BPP} \subseteq \text{BQP} \subseteq \text{PSPACE}$. Если бы удалось доказать, что $\text{BQP} \neq \text{BPP}$ (неформально это означает, что квантовые компьютеры эффективнее классических), тем самым было бы доказано и то, что $\text{BPP} \neq \text{PSPACE}$. Однако в данный момент неизвестно, совпадают ли классы BPP и PSPACE , и ответ на этот вопрос явился бы прорывом в теоретической информатике. Так что, если бы удалось доказать, что квантовые компьютеры эффективнее классических, это повлекло бы интересные последствия и для классической теории сложности. К сожалению, это означает и то, что доказать неравенство $\text{BPP} \neq \text{PSPACE}$ будет очень трудно.

Но почему же $\text{BQP} \subseteq \text{PSPACE}$? Вот неформальный набросок доказательства (ссылку на источник, содержащий строгое доказательство, см. в разделе «История и дополнительная литература»). Пусть имеется n -кубитовый квантовый компьютер и мы выполняем квантовое вычисление с использованием $p(n)$ элементов, где $p(n)$ — многочлен от n . Предполагая, что квантовая схема начинает работу в состоянии $|0\rangle$, объясним, как, используя лишь полиномиальную память, оценить с помощью классического компьютера вероятность того, что конечным состоянием схемы будет $|y\rangle$. Пусть в процессе вычисления использовались элементы $U_1, U_2, \dots, U_n, U_p(n)$ (в указанном порядке). Тогда вероятность того, что конечным состоянием будет $|y\rangle$, равна квадрату модуля числа

$$\langle y | U_{p(n)} \cdots U_2 U_1 | 0 \rangle, \quad (4.86)$$

и эта вероятность может быть посчитана классическим компьютером на полиномиальной памяти. Основная идея состоит в том, чтобы между каждой парой соседних сомножителей вставить соотношение полноты $\sum_x |x\rangle\langle x| = I$ и получить

$$\begin{aligned} & \langle y | U_{p(n)} \cdots U_2 U_1 | 0 \rangle \\ &= \sum_{x_1, \dots, x_{p(n)-1}} \langle y | U_{p(n)} | x_{p(n)-1} \rangle \langle x_{p(n)-1} | U_{p(n)-1} \cdots U_2 | x_1 \rangle \langle x_1 | U_1 | 0 \rangle. \end{aligned} \quad (4.87)$$

Поскольку отдельные унитарные элементы, входящие в эту сумму, — элемент Адамара, CNOT и т. п., ясно, что каждое слагаемое можно с высокой точностью вычислить с помощью классического компьютера на полиномиальной памяти; значит, и всю сумму можно вычислить, используя полиномиальную память, поскольку после прибавления очередного слагаемого к промежуточному итогу это слагаемое можно стереть. Конечно, описанный алгоритм является довольно медленным (ведь число слагаемых в сумме экспоненциально), но объем используемой памяти при этом полиномиален, так что $\text{BQP} \subseteq \text{PSPACE}$, что и требовалось доказать.

С помощью аналогичной процедуры на классическом компьютере можно моделировать произвольное квантовое вычисление, какова бы ни была его длина. Значит, класс задач, разрешимых на квантовом компьютере без ограничений на время и память, не больше, чем класс задач, разрешимых на классическом компьютере. Иными словами, квантовые компьютеры не отменяют тезис Чёрча–Тьюринга: любой алгоритм может быть выполнен на машине Тьюринга. Конечно, квантовые компьютеры могут оказаться значительно более эффективными, чем классические, что поставит под сомнение усиленный тезис Чёрча–Тьюринга, согласно которому любой алгоритм можно эффективно моделировать на вероятностной машине Тьюринга.

4.6 Модель квантовых схем вычислений

В данной книге понятие «квантовый компьютер» означает «модель вычислений, основанная на квантовых схемах», и в этой главе мы подробно обсудили квантовые схемы, основные элементы, из которых они состоят, универсальные наборы элементов, а также некоторые приложения. Прежде чем перейти к рассмотрению более сложных применений, суммируем основные положения модели квантовых схем.

- 1. Классические ресурсы.** Квантовый компьютер состоит из двух частей, классической и квантовой. В принципе классическая часть не является необходимой, но на практике некоторые задачи можно выполнить гораздо легче, если какие-то этапы вычислений реализовать классическим путем. Например, во многих схемах для квантового исправления ошибок (см. гл. 10) классические вычисления будут использоваться для повышения эффективности. Хотя в принципе любое классическое вычисление может быть выполнено на квантовом компьютере, может оказаться удобнее некоторые вычисления делать на классическом компьютере.

2. **Пространство состояний.** Квантовый компьютер работает с определенным числом кубитов (обозначим его n). Соответствующее пространство состояний является 2^n -мерным комплексным гильбертовым пространством. «Разложимые» состояния вида $|x_1, \dots, x_n\rangle$, где $x_i = 0, 1$, известны как элементы *вычислительного базиса*. Если x — число с двоичной записью x_1, \dots, x_n , то через $|x\rangle$ обозначается соответствующее состояние, принадлежащее вычислительному базису.
3. **Возможность приготовления состояний из вычислительного базиса.** Предполагается, что любое состояние $|x_1, \dots, x_n\rangle$ из вычислительного базиса можно приготовить не более чем за n шагов.
4. **Возможность выполнения квантовых элементов.** Элементы можно применять к любому нужному множеству кубитов, и можно реализовать универсальный набор элементов. Например, элемент CNOT можно применить к любой паре кубитов. Элементы Адамара, сдвига фазы, СНОТ и $\pi/8$ образуют универсальный набор элементов, с помощью которого можно аппроксимировать любую унитарную операцию, и тем самым он универсален. Существуют и другие универсальные наборы.
5. **Возможность измерения в вычислительном базисе.** В вычислительном базисе можно измерять один или несколько кубитов.

Модель квантовых схем эквивалентна многим другим моделям в том смысле, что для одинаковых задач требуется примерно одинаковый объем ресурсов. В качестве простого примера, иллюстрирующего общую идею, попытаемся выяснить, дает ли экономию ресурсов переход на трехуровневые квантовые системы взамен двухуровневых кубитов. Хотя использование трехуровневых квантовых систем (*кутритов*) и может принести небольшое преимущество, с теоретической точки зрения им можно пренебречь. Менее тривиальный пример: было показано, что «квантовая машина Тьюринга» — квантовое обобщение классической машины Тьюринга — эквивалентна как вычислительная модель квантовым схемам. Мы здесь не рассматриваем квантовые машины Тьюринга; заинтересованный читатель найдет соответствующие ссылки в разделе «История и дополнительная литература».

Несмотря на простоту и привлекательность модели квантовых схем, необходимо иметь в виду ее возможные недостатки, модификации и расширения. Так, отнюдь не самоочевидно, что обоснованы допущения относительно пространства состояний и начального состояния. В рассматриваемой модели все формулируется в терминах конечномерных пространств, но не исключено, что можно получить больше, если рассматривать системы с бесконечномерным пространством состояний. Не является необходимым и условие, что начальное состояние принадлежит вычислительному базису; мы знаем, что многие встречающиеся в природе системы «предпочитают» находиться в весьма запутанных состояниях, и, быть может, за счет этого удастся выиграть в эффективности вычислений? Не исключено, что доступ к некоторым из таких состояний позволил бы

проводить вычисления гораздо быстрее, чем тогда, когда мы начинаем работу в состоянии, принадлежащем вычислительному базису. Возможность эффективно производить запутывающие измерения в многокубитовых базисах также могла бы быть не менее полезна, чем возможность выполнять запутывающие унитарные операции. Может быть, такие измерения удастся приспособить к выполнению задач, недоступных модели квантовых схем.

Подробное рассмотрение и обоснование физики, лежащей в основе модели квантовых схем, выходит за рамки нашего обсуждения, да и за рамки современной науки. Поднимая эти вопросы, мы хотим лишь подчеркнуть важность проблемы полноты модели квантовых схем и еще раз привлечь внимание к тому важному обстоятельству, что информация — понятие физическое. Пытаясь создать модели обработки информации, не следует забывать время от времени обращаться к основным физическим законам. В нашем рассмотрении мы не выйдем за рамки квантовой модели вычислений, которая является богатой и мощной. С помощью законов квантовой механики она позволяет произвести поразительные вычисления, не имеющие аналогов в классической модели. Вопрос о том, существуют ли физически возможные вычислительные модели, более эффективные, чем квантовые схемы, мы адресуем читателю.

4.7 Моделирование квантовых систем

Возможно (...) нам недостает математической теории квантовых автоматов. (...) квантовое пространство состояний обладает гораздо большей емкостью, чем классическое: там, где в классике имеется N дискретных состояний, в квантовой теории, допускающей их суперпозицию, имеется C^N планковских ячеек. При объединении классических систем их числа состояний N_1 и N_2 перемножаются, а в квантовом варианте получается $C^{N_1 N_2}$. Эти грубые подсчеты показывают гораздо большую потенциальную сложность квантового поведения системы по сравнению с его классической имитацией.

Ю. И. Манин, 1980 [274]

Для квантовомеханического расчета молекулы метана требуется провести вычисления по методу сеток в 10^{42} точках. Если считать, что в каждой точке следует выполнить всего 10 элементарных операций, и предположить, что все вычисления производятся при сверхнизких температурах ($T = 3 \cdot 10^{-3} K$), то и при этом расчет молекулы метана потребует израсходовать энергию, производимую на Земле примерно за столетие.

Р. П. Поплавский (1975) [325] (цитируется по [274])

Можно ли смоделировать физику на универсальном компьютере? (...) физический мир — квантовомеханический, так что подлинной задачей является моделирование квантовой физики (...) полное описание квантовой механики для большой системы из R частиц (...) содержит слишком много переменных, и его невозможно смоделировать на обычном компьютере, число элементов которого пропорционально R (...) но его можно смоделировать с помощью квантового компьютера. (...) Может ли квантовая система быть вероятностно смоделирована с помощью классического (предположим, вероятностного) компьютера? (...) Если имеется в виду классический компьютер того типа, что я описал выше, то ответом, бесспорно, будет «нет».

Р. Фейнман (1982) [149]

Мы завершим эту главу рассмотрением одного из интересных и полезных приложений модели квантовых схем. Важнейшее практическое приложение компьютерных вычислений — моделирование физических систем. Например, при проектировании нового здания для обеспечения безопасности при минимальных затратах используются метод конечных элементов и моделирование. Автомобили получаются легкими, удобными, привлекательными и недорогими благодаря применению систем автоматизированного проектирования. Современное самолетостроение в большой степени основано на компьютерном аэродинамическом моделировании. Испытания ядерного оружия в основном проводятся не с помощью взрывов, а путем тщательных расчетов. Таким образом, примеров очень много по той простой причине, что моделирование, ориентированное на предсказания, имеет огромную практическую ценность. Начнем с того, что опишем различные варианты проблемы моделирования, затем представим в качестве примера квантовый алгоритм моделирования, а в заключение обсудим перспективы его применения.

4.7.1 Моделирование в действии

Главным в моделировании является решение дифференциальных уравнений, описывающих физические законы, управляющие поведением системы. В качестве примера могут быть рассмотрены закон Ньютона

$$\frac{d}{dx} \left(m \frac{dx}{dt} \right) = F, \quad (4.88)$$

уравнение Пуассона

$$-\vec{\nabla} \cdot (k \vec{\nabla} \vec{u}) = \vec{Q}, \quad (4.89)$$

волновое уравнение для электромагнитного поля

$$\vec{\nabla} \cdot \vec{\nabla} \vec{E} = \epsilon_0 \mu_0 \frac{\partial^2 \vec{E}}{\partial t^2} \quad (4.90)$$

и уравнение диффузии

$$\vec{\nabla}^2 = \frac{1}{a^2} \frac{\partial^2 \psi}{\partial t^2}. \quad (4.91)$$

Обычно дается исходное состояние системы и требуется установить, в каком состоянии она будет находиться в данный момент времени или в данной точке пространства. Для получения решения исходное состояние *приближенно описывают в числовом виде*, а затем *дискретизируют* дифференциальное уравнение (по пространству и времени) так, чтобы последовательное применение некоторой процедуры дало искомое решение. Существенно, что погрешность при такой процедуре решения ограничена — она не превышает небольшую степень числа итераций. Далее, не всякую физическую систему можно смоделировать эффективно: такому моделированию поддаются только те системы, которые могут быть эффективно описаны.

Моделирование квантовых систем на классических компьютерах возможно, но обычно оно довольно трудоемко. Поведение многих простых квантовых систем описывается уравнением Шрёдингера

$$i\hbar \frac{d}{dt} |\psi\rangle = H |\psi\rangle. \quad (4.92)$$

Нам будет удобно включить \hbar в H (до конца настоящего раздела мы будем придерживаться этого соглашения). Для типичного физически интересного гамильтониана, связанного с реальными частицами в пространстве (а не с такими абстракциями, как кубиты, с которыми мы до сих пор имели дело), это уравнение приводится к виду

$$i \frac{\partial}{\partial t} \psi(x) = \left[-\frac{1}{2m} \frac{\partial^2}{\partial x^2} + V(x) \right] \psi(x), \quad (4.93)$$

где используется так называемое координатное представление $\langle x|\psi\rangle = \psi(x)$. Это — эллиптическое уравнение, очень похожее на (4.91), так что само по себе моделирование уравнения Шрёдингера не представляет особой сложности. Так почему же трудно моделировать квантовые системы?

Главная проблема заключается в том, что количество дифференциальных уравнений, которые надо решать, экспоненциально. Для моделирования системы из одного кубита, согласно уравнению Шрёдингера, необходимо решить систему из двух дифференциальных уравнений; для двух кубитов уравнений будет четыре; а для n кубитов — 2^n . Иногда удается придумать приближение, в котором число уравнений сокращается настолько, что классическое моделирование квантовой системы становится возможным. Однако существует много физически интересных квантовых систем, для которых такое приближение неизвестно.

Упражнение 4.46 (экспоненциальный рост сложности в квантовых системах). Пусть ρ — матрица плотности, описывающая состояние n кубитов.

Покажите, что для задания матрицы ρ требуется $4^n - 1$ независимых действительных чисел.

Читатель, обладающий познаниями в физике, согласится, что существует множество важных квантовых систем, классическое моделирование которых невозможно. К ним относятся, например, модель Хаббарда, в которой фермионы взаимодействуют с гамильтонианом

$$H = \sum_{k=1}^n V_0 n_{k\uparrow} n_{k\downarrow} + \sum_{k,j - \text{соседи}, \sigma} t_0 c_{k\sigma}^* c_{j\sigma}, \quad (4.94)$$

полезная при исследовании сверхпроводимости и магнетизма; модель Изинга

$$H = \sum_{k=1}^n \vec{\sigma}_k \cdot \vec{\sigma}_{k+1} \quad (4.95)$$

и многие другие. С помощью этих моделей можно получить такие физические величины, как диэлектрическая постоянная, проводимость и магнитная восприимчивость материалов. Более сложные модели (в области квантовой электродинамики и квантовой хромодинамики) можно использовать для вычисления ряда констант, например, массы протона.

Квантовые компьютеры способны эффективно моделировать такие квантовые системы, для которых неизвестно никакой эффективной классической модели. Это возможно по той причине, что позволяет построить любую квантовую схему из универсального набора квантовых элементов. Более того, подобно тому, как существуют унитарные операторы, которые нельзя эффективно аппроксимировать, не исключено, что имеются и квантовые системы, гамильтониан которых невозможно эффективно моделировать на квантовом компьютере. Мы, конечно, полагаем, что в природе такие системы не встречаются, иначе мы смогли бы использовать их для выполнения более мощных вычислений, которые нельзя проводить с использованием модели квантовых схем.

4.7.2 Алгоритм квантового моделирования

Классическое моделирование начинается с понимания того факта, что при решении простого дифференциального уравнения, подобно $dy/dt = f(y)$, в первом порядке малости верно равенство $y(t + \Delta t) \approx y(t) + f(y)\Delta t$. В квантовом случае уравнение имеет вид $i\hbar|\psi\rangle/dt = H|\psi\rangle$, а его решение (при H , не зависящем от времени) есть

$$|\psi(t)\rangle = e^{-iHt}|\psi(0)\rangle. \quad (4.96)$$

Поскольку вычислить экспоненту от H обычно бывает крайне трудно (матрица может быть разреженной, но при этом она экспоненциально велика), в начале стоит рассмотреть приближение первого порядка $|\psi(t + \Delta t)\rangle \approx (I - iH\Delta t)|\psi(t)\rangle$. Это уже практически вычисляется, поскольку для многих гамильтонианов H

без труда можно подобрать квантовые элементы, эффективно аппроксимирующие $I - iH\Delta t$; однако такие решения первого порядка, вообще говоря, неудовлетворительны.

Эффективная аппроксимация решения уравнения (4.96) при более высоком порядке малости возможна для многих классов гамильтонианов. Например, для большинства физических систем гамильтониан можно записать в виде суммы слагаемых, отвечающих за локальные взаимодействия. Конкретнее, для системы из n частиц имеем

$$H = \sum_{k=1}^L H_k, \quad (4.97)$$

где каждый H_k действует не более чем на c системах (c — константа), а L — многочлен от n . Нередко, например, что все H_k — это либо взаимодействия двух тел (например, $X_i X_j$), либо гамильтонианы одного тела (как X_i). И в модели Хаббарда, и в модели Изинга гамильтонианы имеют именно этот вид. Такая локальность вполне осмысленна физически; для многих систем она объясняется тем, что взаимодействие быстро убывает с ростом расстояния или разности энергий. Часто имеют место также глобальные ограничения, налагаемые симметрией (например, статистикой частиц); ниже эти вопросы будут изучены подробнее. Существенным моментом является то, что, хотя e^{-iHt} подсчитать трудно, $e^{-iH_k t}$ действует на гораздо меньшей подсистеме и этот оператор легко аппроксимировать с помощью квантовых схем. Впрочем, поскольку $[H_i, H_j] \neq 0$, $e^{-iHt} \neq \prod_k e^{-iH_k t}$. Как же в таком случае использовать $e^{-iH_k t}$ для вычисления e^{-iHt} ?

Упражнение 4.47. Пусть $H = \sum_k^L H_k$; докажите, что $e^{-iHt} = e^{-iH_1 t} e^{-iH_2 t} \dots e^{-iH_k t}$, для всех t , если $[H_j, H_k] = 0$ для всех j и k .

Упражнение 4.48. Покажите, что если H_k соответствует взаимодействию не более чем с c частицами, то в формуле (4.97) число L ограничено сверху полиномом от n .

В основе алгоритмов квантового моделирования лежит следующая теорема об асимптотической аппроксимации:

Теорема 4.3 (формула Троттера). Пусть A и B — эрмитовы операторы. Покажите, что для всякого вещественного t справедлива формула

$$\lim_{n \rightarrow \infty} (e^{iAt/n} e^{iBt/n})^n = e^{i(A+B)t}. \quad (4.98)$$

Заметим, что формула (4.98) выполняется даже в том случае, когда A и B не коммутируют. Возможно, еще интереснее то обстоятельство, что эту формулу можно обобщить на тот случай, когда A и B являются образующими некоторых полугрупп, соответствующих общим преобразованиям матриц плотности. Эти образующие («форма Линдблада») будут описаны в подразд. 8.4.1, а пока ограничимся рассмотрением случая эрмитовых операторов A и B .

Доказательство. По определению,

$$e^{iAt/n} = I + \frac{1}{n}iAt + O\left(\frac{1}{n^2}\right), \quad (4.99)$$

откуда имеем

$$e^{iAt/n} e^{iBt/n} = I + \frac{1}{n}i(A+B)t + O\left(\frac{1}{n^2}\right). \quad (4.100)$$

Возведя в степень n , получим уравнение

$$(e^{iAt/n} e^{iBt/n})^n = I + \sum_{k=1}^n \binom{n}{k} \frac{1}{n^k} [i(A+B)t]^k + O\left(\frac{1}{n}\right), \quad (4.101)$$

а поскольку $\binom{n}{k} \frac{1}{n^k} = (1 + O(\frac{1}{n})) / k!$, можно записать соотношение

$$\lim_{n \rightarrow \infty} (e^{iAt/n} e^{iBt/n})^n = \lim_{n \rightarrow \infty} \frac{(i(A+B)t)^k}{k!} \left(1 + O\left(\frac{1}{n}\right)\right) + O\left(\frac{1}{n}\right) = e^{i(A+B)t}. \quad (4.102)$$

■

Различные модификации формулы Троттера дают методы для получения приближений высоких порядков, необходимых для квантового моделирования. Так, с помощью рассуждений, аналогичных приведенному выше доказательству, можно показать, что

$$e^{i(A+B)\Delta t} = e^{iA\Delta t} e^{iB\Delta t} + O(\Delta t^2). \quad (4.103)$$

Аналогичным образом имеем

$$e^{i(A+B)\Delta t} = e^{iA\Delta t/2} e^{iB\Delta t} e^{iA\Delta t/2} + O(\Delta t^3). \quad (4.104)$$

Краткое описание алгоритма квантового моделирования приведено ниже, а явный пример моделирования одномерного нерелятивистского уравнения Шрёдингера дан во вставке 4.2.

Алгоритм: квантовое моделирование

Вход: 1) гамильтониан $H = \sum_k H_k$, действующий на N -мерной системе; каждый H_k действует на небольшой подсистеме, размер которой не зависит от N ; 2) $|\psi_0\rangle$ — начальное состояние системы при $t = 0$; 3) положительное число δ (возможная ошибка); 4) время t_f — момент времени, в который мы хотим узнать состояние системы.

Выход: состояние $|\tilde{\psi}(t_f)\rangle$, такое, что $|\langle\tilde{\psi}(t_f)|e^{-iHt_f}|\psi_0\rangle|^2 \geq 1 - \delta$.

Время работы: $O(\text{poly}(1/\delta))$ операций.

Процедура: выберем представление, в котором состояние $|\tilde{\psi}\rangle$ системы из $n = \text{poly}(\log N)$ кубитов аппроксимирует нашу систему, а операторы $e^{-iH_k\Delta t}$

обладают эффективной аппроксимацией с помощью квантовых схем. Выбрать метод приближенного решения (см., в частности, формулы (4.103)–(4.105)) и Δt таким образом, чтобы ожидаемая ошибка была приемлема (и $j\Delta t = t_f$ для некоторого целого j), построить соответствующую квантовую схему $U_{\Delta t}$ (для шага итерации) и сделать следующее:

1. $|\tilde{\psi}_0\rangle \leftarrow |\psi_0\rangle; j = 0$ (инициализация)
2. $\rightarrow |\tilde{\psi}_{j+1}\rangle = U_{\Delta t}|\tilde{\psi}_j\rangle$ (шаг итерации)
3. $\rightarrow j = j + 1; \text{ goto 2 until } j\Delta t \geq t_f$ (цикл)
4. $\rightarrow |\tilde{\psi}(t_f)\rangle = |\tilde{\psi}_j\rangle$ (окончательный результат)

Упражнение 4.49 (формула Бейкера–Кэмпбелла–Хаусдорфа). Докажите, что

$$e^{(A+B)\Delta t} = e^{A\Delta t}e^{B\Delta t}e^{-\frac{1}{2}[A,B]\Delta t^2} + O(\Delta t^3), \quad (4.105)$$

а также выведите формулы (4.103) и (4.104).

Упражнение 4.50. Пусть $H = \sum_k^L H_k$, и положим

$$U_{\Delta t} = \left[e^{-iH_1\Delta t}e^{-H_2\Delta t} \dots e^{-iH_L\Delta t} \right] \left[e^{-iH_L\Delta t}e^{-H_{L-1}\Delta t} \dots e^{iH_1\Delta t} \right]. \quad (4.106)$$

a) Докажите, что $U_{\Delta t} = e^{-2iH\Delta t} + O(\Delta t^3)$.

б) С помощью результатов вставки 4.1 докажите, что при целых положительных m имеем

$$E(U_{\Delta t}^m, e^{-2miH\Delta t}) \leq m\alpha\Delta t^3 \quad (4.107)$$

для некоторой константы α .

4.7.3 Пример

Описанная процедура квантового моделирования предназначена для моделирования гамильтонианов, являющихся суммами слагаемых, соответствующих локальным взаимодействиям. Однако такое ограничение не является необходимым! Как показывает следующий пример, эффективное квантовое моделирование возможно даже для гамильтонианов, нетривиально действующих на все (или на почти все) части большей системы.

Вставка 4.2. Квантовое моделирование уравнения Шредингера.

Методы квантового моделирования и его ограничения можно продемонстрировать на следующем примере, относящемся не к абстрактной кубитовой модели, а к моделям, которыми занимаются физики. Рассмотрим одиночную частицу на прямой с одномерным потенциалом $V(x)$ и

гамильтонианом

$$H = \frac{p^2}{2m} + V(x), \quad (4.108)$$

где p — оператор импульса, а x — оператор координаты. Спектр оператора x непрерывен, и состояния $|\psi\rangle$ этой системы образуют бесконечномерное гильбертово пространство; в базисе x состояние $|\psi\rangle$ можно записать в виде

$$|\psi\rangle = \int_{-\infty}^{\infty} |x\rangle \langle x| \psi \rangle dx. \quad (4.109)$$

На практике интерес представляет только конечная часть прямой; можно считать, что она задается неравенствами $-d \leq x \leq d$. Далее, если выбрать шаг Δx достаточно коротким (достаточно малым по сравнению с наименьшей длиной волны), то выражение

$$|\tilde{\psi}\rangle = \sum_{k=-d/\Delta x}^{d/\Delta x} a_k |k\Delta x\rangle \quad (4.110)$$

будет хорошей физической аппроксимацией для $|\psi\rangle$. Это состояние можно представить с помощью $n = \lfloor \log(2d/\Delta x + 1) \rfloor$ кубитов: мы просто заменим каждое состояние $|k\Delta x\rangle$ (собственное состояние оператора x) на состояние $|k\rangle$, лежащее в вычислительном базисе для n кубитов. Отметим, что для такого моделирования достаточно только n кубитов, тогда как классически потребовалось бы 2^n комплексных чисел: за счет этого и достигается экспоненциальная экономия ресурсов.

В вычислении $|\tilde{\psi}(t)\rangle = e^{-iHt}|\tilde{\psi}(0)\rangle$ необходимо использовать одну из приближенных формул (4.103)–(4.105), поскольку, вообще говоря, $H_1 = V(x)$ не коммутирует с $H_0 = p^2/2m$. Таким образом, мы должны уметь вычислять $e^{-iH_1\Delta t}$ и $e^{-iH_0\Delta t}$. Поскольку $|\tilde{\psi}\rangle$ выражается через собственные значения оператора H_1 , оператор $e^{-iH_1\Delta t}$ является диагональным и имеет вид

$$|k\rangle \rightarrow e^{-iV(k\Delta x)\Delta t} |k\rangle. \quad (4.111)$$

Это выражение вычисляется непосредственно, поскольку можно подсчитать $V(k\Delta x)\Delta t$ (см. также задачу 4.1). Второй оператор также вычисляется легко, так как x и p сопряжены с помощью квантового преобразования Фурье: $U_{\text{FFT}} x U_{\text{FFT}}^\dagger = p$; значит, $e^{-iH_0\Delta t} = U_{\text{FFT}} e^{-ix^2\Delta t/2m} U_{\text{FFT}}^\dagger$; чтобы определить $e^{-iH_0\Delta t}$, достаточно вычислить

$$|k\rangle \rightarrow U_{\text{FFT}} e^{-ix^2/2m} U_{\text{FFT}}^\dagger |k\rangle. \quad (4.112)$$

Конструкция U_{FFT} будет обсуждена в гл. 5.

Предположим, имеется гамильтониан вида

$$H = Z_1 \otimes Z_2 \otimes \cdots \otimes Z_n, \quad (4.113)$$

действующий на n -кубитовой системе. Хотя в этом взаимодействии участвует вся система, его можно эффективно смоделировать. Для этого требуется простая квантовая схема, реализующая оператор $e^{-iH\Delta t}$ для произвольных значений Δt . Соответствующая схема (для $n = 3$) изображена на рис. 4.19. Главное здесь то, что, хотя гамильтониан действует на все кубиты, это действие является *классическим*: фазовый сдвиг системы равен $e^{-i\Delta t}$, если число кубитов четно, и $e^{i\Delta t}$, если нечетно. Поэтому смоделировать H можно так: сначала классическим способом подсчитать четность числа n (результат записывается во вспомогательном кубите), затем применить сдвиг фазы, соответствующий этой четности, затем обратить вычисление четности (чтобы стереть вспомогательный кубит). Ясно, что эта стратегия работает не только при $n = 3$, но и для произвольных значений n .

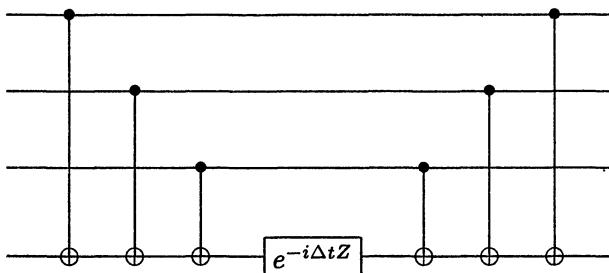


Рис. 4.19. Квантовая схема для моделирования гамильтониана $H = Z_1 \otimes Z_2 \otimes Z_3$ на промежутке времени Δt .

Обобщение этой процедуры позволяет моделировать и более сложные гамильтонианы, например, гамильтониан вида

$$H = \bigotimes_{k=1}^n \sigma_{c(k)}^k, \quad (4.114)$$

где $\sigma_{c(k)}^k$ — матрица Паули (или тождественная матрица), действующая на k -ом кубите, а $c(k) \in \{0, 1, 2, 3\}$ обозначает одну из матриц $\{I, X, Y, Z\}$. Кубиты, к которым применяется тождественное преобразование, можно не рассматривать, а операции X и Y могут быть преобразованы в операции Z с помощью однокубитовых элементов. Это сводит дело к гамильтониану вида (4.113), а его можно промоделировать, так как было объяснено выше.

Упражнение 4.51. Постройте квантовую схему, моделирующую гамильтониан

$$H = X_1 \otimes Y_2 \otimes Z_3, \quad (4.115)$$

таким образом, чтобы она выполняла унитарное преобразование $e^{-i\Delta t H}$ для любого Δt .

С помощью этой процедуры можно моделировать большой класс гамильтонианов, содержащих нелокальные слагаемые. В частности, можно моделировать гамильтонианы вида $H = \sum_{k=1}^L H_k$ при единственном условии: каждый из H_k обладает структурой тензорного произведения, а L полиномиально относительно числа частиц n . Другими словами, достаточно лишь потребовать, чтобы каждый из H_k по отдельности эффективно моделировался схемой. Например, гамильтониан $H = \sum_{k=1}^n X_k + Z^{\otimes n}$ может быть эффективно смоделирован с помощью описанного метода. Как правило, в природе таких гамильтонианов не существует, но они позволяют с другой точки зрения рассматривать квантовые компьютеры.

4.7.4 Перспективы квантового моделирования

Алгоритм квантового моделирования очень близок к классическим методам, но у него есть и фундаментальное отличие. На каждом шаге квантового алгоритма старое состояние полностью заменяется новым; без серьезных изменений в алгоритме невозможно научиться извлекать (нетривиальную) информацию из его промежуточных шагов, так как состояния являются квантовыми. Более того, для получения желаемого результата заключительное измерение должно быть тщательно выбрано, поскольку оно возмущает квантовое состояние. Конечно, алгоритм квантового моделирования можно повторять много раз, чтобы набрать статистику, но желательно, чтобы количество циклов было не более чем полиномиально. Может случиться так, что, несмотря на эффективность моделирующего алгоритма, не удается эффективно провести измерение.

Кроме того, существуют гамильтонианы, которые вообще невозможно эффективно смоделировать. Как следует из подразд. 4.5.4, имеются такие унитарные преобразования, что квантовые компьютеры не могут их эффективно аппроксимировать. Следовательно, не для всякого гамильтониана уравнение Шредингера можно эффективно решить на квантовом компьютере — иначе оказалось бы, что любое унитарное преобразование можно эффективно аппроксимировать!

Другая трудная (и очень интересная) проблема — моделирование процессов установления равновесия. Система с гамильтонианом H , находящаяся в контакте с окружающей средой при температуре T , придет, вообще говоря, к тепловому равновесию в состоянии, известном под названием *гипсовского*, $\rho_{\text{term}} = e^{-H/k_B T}/Z$, где $Z = \text{tr } e^{-H/k_B T}$ — обычная нормализация, обеспечивающая равенство $\text{tr}(\rho) = 1$. Процесс установления этого равновесия до сих пор плохо понят, хотя известны некоторые необходимые условия: окружающая среда должна быть обширной, она должна иметь состояния с энергиями, соответствующими собственным состояниям оператора H , и ее взаимодействие с системой должно быть слабым. Нахождение ρ_{term} для произвольных H и T является, как правило, экспоненциально трудной задачей, если делать это на классическом компьютере. Можно ли эффективно решить данную задачу на квантовом компьютере? Пока это неизвестно.

В то же самое время из наших обсуждений следует, что многие интересные квантовые задачи *могут* эффективно моделироваться на квантовом компьютере, даже при наличии дополнительных условий, которые не охвачены представленными здесь простыми алгоритмами. В частности, к таким условиям относится глобальная симметрия, происходящая из статистики частиц. В нашем повседневном мире мы привыкли к тому, что можно различать отдельные частицы: можно проследить траектории теннисных мячей на корте, не путая их друг с другом. Такая различимость является общей чертой классических объектов: поскольку положение классической частицы меняется непрерывно, можно узнать ее положение в любой момент и тем самым отличить ее от других частиц. В квантовой механике, однако, так не выходит: проследить точно за движением отдельной частицы невозможно. Если две частицы различны по сути (например, протон и электрон), то мы можем отличить их, измеряя, скажем, знак их заряда. Но в случае одинаковых частиц оказывается, что они принципиально неразличимы.

Неразличимость частиц налагает ограничения на вектор состояния системы, и эти ограничения проявляются двояким образом. Из экспериментов известно, что существующие в природе частицы бывают двух типов, известных под названиями «бозоны» и «фермионы». Вектор состояния системы, состоящей из бозонов, не меняется, если поменять местами две частицы, в чем и выражается их неразличимость. В фермионных системах, напротив, при перестановке двух частей вектор состояния меняется на противоположный. И те и другие системы эффективно моделируются на квантовом компьютере. Подробное объяснение того, как работают эти модели, выходит за рамки книги; достаточно сказать, что делается это довольно бесхитростно. Если начальное состояние не обладает нужной симметрией, его можно симметризовать перед началом работы модели. Операторы, участвующие в модели, могут быть построены таким образом, чтобы сохранять эту симметрию, даже с учетом членов высшего порядка. Читатель, желающий узнать подробнее о таком моделировании, может найти ссылки в разделе «История и дополнительная литература» в конце главы.

Задача 4.1 (вычислимые сдвиги фазы). Пусть m и n — целые положительные числа и $f: \{0, \dots, 2^m - 1\} \rightarrow \{0, \dots, 2^n - 1\}$ — классическая функция перехода из m -битовых чисел в n -битовые, которую можно обратимо вычислить с помощью T -элементов Тоффоли, как описано в подразд. 3.2.5. Это означает, что функция $(x, y) \rightarrow (x, y \oplus f(x))$ может быть реализована с использованием T -элементов Тоффоли. Постройте квантовую схему, с помощью $2T + n$ (или меньше) одно-, двух- и трехкубитовых элементов, которая выполняла бы унитарную операцию, заданную формулой

$$|x\rangle \rightarrow \exp\left(\frac{-2i\pi f(x)}{2^n}\right) |x\rangle. \quad (4.116)$$

Задача 4.2. Постройте схему глубиной $O(\log n)$, реализующую элемент $C^n(X)$. (Глубиной схемы называют число тактов ее работы; смысл этой задачи в том,

что при реализации $C^n(X)$ можно заставить много элементов работать параллельно.)

Задача 4.3 (альтернативная конструкция универсальности). Пусть U — унитарная матрица, действующая на n кубитах, $H \equiv i \ln(U)$. Покажите, что

1. матрица H эрмитова и ее собственные значения лежат в интервале $[0; 2\pi]$;
2. H можно записать в виде

$$H = \sum_g h_g g, \quad (4.117)$$

где h_g — действительные числа и g пробегает все возможные n -кратные тензорные произведения матриц Паули $\{I, X, Y, Z\}$;

3. можно реализовать унитарную операцию $\exp(-ih_g g \Delta)$ с использованием $O(n)$ одно- и двухкубитовых операций, если $\Delta = 1/k$, где k — целое положительное число;
4. формула

$$\exp(-iH\Delta) = \prod_g \exp(-ih_g g \Delta) + O(4^n \Delta^2); \quad (4.118)$$

справедлива (подразумевается, что матрицы g берутся в каком-то фиксированном порядке);

5. справедлива формула

$$U = \left[\prod_g \exp(-ih_g g \Delta) \right]^k + O(4^n \Delta). \quad (4.119)$$

6. можно аппроксимировать U с точностью $\varepsilon > 0$, используя $O(n16^n/\varepsilon)$ одно- и двухкубитовых унитарных операций.

Задача 4.4 (минимальная конструкция Тоффоли (задача для исследования)).

1. Какое наименьшее количество двухкубитовых элементов требуется для реализации элемента Тоффоли?
2. Какое наименьшее количество однокубитовых элементов и СНОТ необходимо для реализации элемента Тоффоли?
3. Какое должно быть наименьшее количество однокубитовых элементов и элементов «управляемое Z » для реализации элемента Тоффоли?

Задача 4.5 (задача для исследования). Постройте такую последовательность n -кубитовых гамильтонианов $\{H_n\}$, чтобы для моделирования H_n требовалось суперполиномиальное количество операций.

Задача 4.6 (универсальность с предварительным запутыванием).

СNOT и однокубитовые элементы образуют универсальный набор квантовых логических элементов. Покажите, что альтернативный универсальный набор можно составить из однокубитовых унитарных операторов, измерений пары кубитов в базисе Белла и возможности приготавливать произвольные (запутанные) четырехкубитовые состояния.

Краткое содержание главы

- **Универсальность.** Произвольная n -кубитовая унитарная операция может быть реализована (точно) с помощью однокубитовых элементов и CNOT.
- **Универсальность конечного семейства.** Элементы Адамара, сдвига фазы, CNOT и $\pi/8$ образуют *универсальный* для квантовых вычислений набор в том смысле, что произвольная n -кубитовая унитарная операция может быть аппроксимирована с произвольной точностью $\epsilon > 0$ с помощью схемы, использующей только элементы из этого набора. Если заменить элемент $\pi/8$ элементом Тоффоли, то также получится универсальный набор.
- **Не каждая унитарная операция может быть эффективно реализована.** Существуют n -кубитовые унитарные операции, для аппроксимации которых с точностью ϵ требуется не менее $\Omega(2^n \log(1/\epsilon) / \log(n))$ элементов из любого данного конечного набора.
- **Моделирование.** Для гамильтониана $H = \sum_k H_k$, являющегося суммой полиномиального количества слагаемых H_k , каждое из которых может быть эффективно реализовано с помощью квантовой схемы, на квантовом компьютере можно эффективно моделировать эволюцию e^{-iHt} и аппроксимировать $|\psi\rangle = e^{-iHt}|\psi(0)\rangle$, при условии что дано $|\psi(0)\rangle$.

История и дополнительная литература

Конструкция элементов, о которых шла речь в этой главе, взята из многочисленных источников. Из статьи Баренко, Беннета, Клива и др.[24] взяты многие конструкции элементов, а также доказательство универсальности набора, состоящего из однокубитовых и CNOT-элементов. Другой полезный источник идей — статья Бекмана, Чари, Девабхактуни и Прескилла [33]. Доступное и по-

следовательное введение принадлежит ДиВинченцо [125]. То обстоятельство, что измерения можно перенести в конец схемы, было отмечено Гриффитсом и Ниу [163].

Доказательство универсальности двухуровневых элементов принадлежит Реку, Цайлингеру, Бернштейну и Бертани [345]. Универсальность набора из однокубитовых элементов и СНОТ была доказана ДиВинченцо [124]. Универсальный элемент G (упр. 4.44) иногда называют элементом Дойча [118]. Дойч, Баренко и Экерт [115], а также Ллойд [253] независимо показали, что почти любой двухкубитовый элемент универсален. То, что ошибка, накапливающаяся при применении последовательности элементов, не превосходит суммы ошибок каждого из них, доказана в работе Бернштейна и Вазирани [75]. Универсальность набора элементов, на котором здесь было сосредоточено внимание, состоящего из элементов Адамара, сдвига фазы, СНОТ и $\pi/8$ — была обнаружена Бойкином, Мором, Пулвером и др. [62]; в этой работе содержится также доказательство того, что число θ , определенное соотношением $\cos(\theta/2) \equiv \cos^2(\pi/8)$, является иррациональным кратным 2π . Оценка, сделанная в подразд. 4.5.4, основана на работе Нилла [223]; в этой статье содержится гораздо более подробное исследование трудности аппроксимации произвольных унитарных операторов с помощью квантовых схем. В частности, Нилл получил более точные и общие оценки; кроме того, он рассматривает случай, когда семейство элементов, используемых для аппроксимации, непрерывно.

Вычислительная модель, основанная на квантовых схемах, введена Дойчем [118]; ее дальнейшую разработку выполнил Яо [425], который показал, что модель квантовых схем эквивалентна модели, основанной на квантовых машинах Тьюринга. Последние были введены в 1980 г. Бениоффом [45]; далее их теорию развили Дойч [117] и Яо [425], а современное определение было дано Бернштейном и Вазирани [75]. В последних двух статьях сделаны первые шаги в направлении теории квантовой вычислительной сложности, аналогичной обычной теории сложности. В частности, включение $BQP \subseteq PSPACE$ и даже некоторое его усиление получены Бернштейном и Вазирани. Нилл и Лафламм [217] обнаружили интересные связи между квантовой и классической вычислительной сложностью. В числе других работ по квантовой вычислительной сложности следует отметить статьи Адлемана, Демарре и Хуанга [4] и Ватроуза [411]. Последняя содержит интригующие свидетельства в пользу того, что квантовые компьютеры эффективнее классических в «системах интерактивных доказательств» (interactive proof systems).

То обстоятельство, что квантовые компьютеры могут моделировать квантовые системы более эффективно, чем это могли бы сделать классические компьютеры, было отмечено Маниным [274] в 1980 г.; независимо от него эту идею более детально развил Фейнман [149]. Более подробные исследования были предприняты Абрамсон и Ллойдом [12], Богосяном и Тейлором [74], Сорнборгером и Стюартом [369], Виснером [417] и Залкой [430]. Формула Троттера [386] была также доказана Черновым [84], а ее более простая форма (с унитарными операторами) была известна гораздо раньше и восходит к временам Софуса Ли. Формула Бейкера–Кэмпбелла–Хаусдорффа с точностью до третьего по-

рядка (согласно нашей нумерации формула (4.104)) была приведена в работе Сорнборгера и Стюарта [369]. Абрамс и Ллойд [12] разработали процедуру для моделирования фермионных систем многих тел на квантовом компьютере. Терхел и ДиВинченцо изучили проблему моделирования перехода системы в равновесное гиббсовское состояние [384]. Метод моделирования уравнения Шредингера, описанный во вставке 4.2, принадлежит Залке [430] и Виснеру [417].

Упражнение 4.25 было предложено Вандерспеном; оно связано с работой Чая и Вильчека [110]. Авторы упр. 4.45—Бойкин, Мор, Пулвер и др. [62]. Задача 4.2 принадлежит Готтесману, а 4.6 — Готтесману и Чуангу [161].

Предположение о том, что использование начальных состояний, не принадлежащих вычислительному базису, может давать дополнительные возможности по сравнению с моделью квантовых схем (см. разд. 4.6), было сделано Готтесманом и Нильсеном.

Глава 5

КВАНТОВОЕ ПРЕОБРАЗОВАНИЕ ФУРЬЕ И ЕГО ПРИЛОЖЕНИЯ

*Будь на квантах компьютеры эти,¹
Захотят их все воры на свете.
Наши цифры поймут,
нашу почту прочтут,
Но мы квантовым крипто ответим!*

Дж. и П. Шор

*Нашу почту читать будут скоро
На компьютере квантовом воры,
Но утешься: сперва
Разлагать 22
Научиться должны их приборы!*

Ф. Штрассен

Программирование — это такое же искусство, как сочинение стихов или музыки.

Д. Кнут

Наиболее ярким открытием в теории квантовых вычислений является на сегодняшний день то, что квантовые компьютеры оказались способны эффективно решать задачи, с которыми не могут справиться классические компьютеры. Например, для разложения на простые множители n -битового целого числа с помощью лучшего из известных на момент написания книги классических алгоритмов (так называемого *теоретико-числового решета*) необходимо $\exp(\Theta(n^{1/3} \log^{2/3} n))$ операций. Это количество экспоненциально по размеру числа, так что задача факторизации целого числа считается не имеющей эффективного решения на классическом компьютере: уже для чисел, выражаемых не слишком большим количеством цифр, найти разложение за разумное время немыслимо. А вот квантовый алгоритм может выполнить эту задачу за $O(n^2 \log n \log \log n)$ операций, так что квантовый компьютер может выполнять разложение чисел экспоненциально быстрее, чем классический. Этот ре-

¹ Перевод этого и следующего стихотворного эпиграфа принадлежит В. Н. Панову. — Прим. ред

зультат важен и сам по себе, но интересен вопрос, который возникает в связи с этим : какие еще трудные для классических компьютеров задачи можно эффективно решить на квантовом компьютере?

В этой главе будет рассмотрено *квантовое преобразование Фурье*, являющееся основой для квантовой факторизации и многих других интересных квантовых алгоритмов. Квантовое преобразование Фурье, которому посвящен разд. 5.1,— это эффективный квантовый алгоритм для выполнения преобразования Фурье квантовомеханических амплитуд. Оно не ускоряет вычисление преобразования Фурье классических данных, но позволяет при определенных условиях найти хорошие приближения для собственных чисел унитарного оператора (*задача определения собственного числа*); об этом речь пойдет в разд 5.2. Это позволит решить несколько других интересных задач, включая задачи *нахождения порядка и факторизации* (разд. 5.3). Определение собственного числа в сочетании с квантовым алгоритмом поиска приводит к решению *задачи перечисления* (подсчета решений в задаче поиска — см. следующую главу). В завершающем главу разд. 5.4 обсуждается, как с помощью квантового преобразования Фурье можно решить *задачу о скрытой подгруппе* — обобщение задач определения собственного числа и нахождения порядка, частным случаем которой является задача о *дискретном логарифме*, — еще одна задача, считающаяся трудной для классического компьютера.

5.1 Квантовое преобразование Фурье

Хорошая идея имеет обыкновение становиться со временем проще и при этом может использоваться для решения задач, отличных от тех, ради которых она была придумана.

Р. Тарьян

Один из наиболее удачных способов решения задачи в математике или информатике — преобразовать эту задачу в другую, решение которой уже известно. Среди такого рода преобразований имеется несколько используемых столь часто и в столь разнообразных ситуациях, что сами эти преобразования стали предметом изучения. Основное открытие в теории квантовых вычислений — это то, что некоторые из этих преобразований на квантовом компьютере вычисляются гораздо быстрее, чем на классическом, и именно благодаря этому стало возможно строить быстрые алгоритмы для квантовых компьютеров.

Один из примеров таких преобразований — *дискретное преобразование Фурье*. В обычных математических обозначениях входом для преобразования Фурье является вектор с комплексными компонентами x_0, \dots, x_{N-1} , где длина N фиксирована. На выходе получаются преобразованные данные, а именно вектор с комплексными компонентами y_0, \dots, y_{N-1} , определенный по формуле

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i j k / N}. \quad (5.1)$$

Квантовое преобразование Фурье — это в точности то же преобразование, но немного по-другому записанное. В ортонормальном базисе $|0\rangle, \dots, |N-1\rangle$ квантовое преобразование Фурье определяется как линейный оператор, действующий на базисных состояниях по формуле

$$|j\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j k / N} |k\rangle. \quad (5.2)$$

Аналогичным образом действие этого оператора на произвольном состоянии можно записать в виде

$$\sum_{j=0}^{N-1} x_j |j\rangle \longrightarrow \sum_{k=0}^{N-1} y_k |k\rangle, \quad (5.3)$$

где амплитуды y_k — дискретные преобразования Фурье амплитуд x_j . Хотя это и не очевидно из определения, этот оператор является унитарным и тем самым может быть реализован на квантовом компьютере. Мы докажем унитарность преобразования Фурье, построив вычисляющую его квантовую схему, которая, естественно, будет унитарна. Унитарность преобразования Фурье нетрудно доказать и непосредственно:

Упражнение 5.1. Приведите прямое доказательство того, что линейное преобразование, заданное формулой (5.2), унитарно.

Упражнение 5.2. Вычислите в явном виде преобразование Фурье n -кубитового состояния $|00\dots 0\rangle$.

В дальнейшем будем считать, что $N = 2^n$, где n — целое число, и что базис $|0\rangle, \dots, |2^n - 1\rangle$ есть вычислительный базис для n -кубитового квантового компьютера. Удобно записывать состояние $|j\rangle$ в виде двоичного числа $j = j_1 j_2 \dots j_n$. Это означает, что $j = j_1 2^{n-1} + j_2 2^{n-2} + \dots + j_n 2^0$. Можно также пользоваться обозначением $0.j_1 j_2 \dots j_m$ для записи двоичных дробей $j_1/2 + j_2/4 + \dots + j_m/2^{m-l+1}$.

С помощью небольших алгебраических манипуляций можно представить квантовое преобразование Фурье в виде произведения

$$|j_1, \dots, j_n\rangle \rightarrow \frac{(|0\rangle + e^{2\pi i 0 \cdot j_n} |1\rangle) (|0\rangle + e^{2\pi i 0 \cdot j_{n-1} j_n} |1\rangle) \dots (|0\rangle + e^{2\pi i 0 \cdot j_1 j_2 \dots j_n} |1\rangle)}{2^{n/2}}. \quad (5.4)$$

Это представление настолько полезно, что порой его рассматривают как определение квантового преобразования Фурье. Ниже будет объяснено, что данное представление позволяет построить квантовую схему, эффективно вычисляющую преобразование Фурье, и это доказывает унитарность такого преобразования. Указанное представление позволяет понять алгоритмы, основанные на квантовом преобразовании Фурье. В качестве полезного побочного продукта будет получено (в упражнениях) классическое быстрое преобразование Фурье.

Эквивалентность формулы (5.4) и определения (5.2) устанавливается с помощью элементарной алгебры:

$$|j\rangle \rightarrow \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi i j k / 2^n} |k\rangle \quad (5.5)$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^1 \dots \sum_{k_n=0}^1 e^{2\pi i j (\sum_{l=1}^n k_l 2^{-l})} |k_1 \dots k_n\rangle \quad (5.6)$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^1 \dots \sum_{k_n=0}^1 \bigotimes_{l=1}^n e^{2\pi i j k_l 2^{-l}} |k_l\rangle \quad (5.7)$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^n \left[\sum_{k_l=0}^1 e^{2\pi i j k_l 2^{-l}} |k_l\rangle \right] \quad (5.8)$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^n \left[|0\rangle + e^{2\pi i j 2^{-l}} |1\rangle \right] \quad (5.9)$$

$$= \frac{\left(|0\rangle + e^{2\pi i 0 \cdot j_n} |1\rangle \right) \left(|0\rangle + e^{2\pi i 0 \cdot j_{n-1} j_n} |1\rangle \right) \dots \left(|0\rangle + e^{2\pi i 0 \cdot j_1 j_2 \dots j_n} |1\rangle \right)}{2^{n/2}}. \quad (5.10)$$

Представление преобразования Фурье в виде (5.4) дает возможность легко построить схему, которая эффективно его вычисляет. Эта схема изображена на рис. 5.1. Через R_k обозначено унитарное преобразование

$$R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i / 2^k} \end{bmatrix}. \quad (5.11)$$

Чтобы убедиться, что изображенная на рисунке схема действительно вычисляет квантовое преобразование Фурье, посмотрим, что происходит со входным состоянием $|j_1 \dots j_n\rangle$. Применяя элемент Адамара к первому биту, получим состояние

$$\frac{1}{2^{1/2}} \left(|0\rangle + e^{2\pi i 0 \cdot j_1} |1\rangle \right) |j_2 \dots j_n\rangle, \quad (5.12)$$

поскольку $e^{2\pi i 0 \cdot j_1} = -1$ при $j_1 = 1$ и $+1$ в противном случае. Применяя управляемое R_2 , имеем

$$\frac{1}{2^{1/2}} \left(|0\rangle + e^{2\pi i 0 \cdot j_1 j_2} |1\rangle \right) |j_2 \dots j_n\rangle. \quad (5.13)$$

Далее будем применять управляемое R_3 , управляемое R_4 , и т.д. до R_n , добавляя на каждом шаге по биту к фазе первого из векторов $|1\rangle$. По завершении этой процедуры придем к состоянию

$$\frac{1}{2^{1/2}} \left(|0\rangle + e^{2\pi i 0 \cdot j_1 j_2 \dots j_n} |1\rangle \right) |j_2 \dots j_n\rangle. \quad (5.14)$$

Теперь используем ту же процедуру для второго кубита. Элемент Адамара переводит в состояние

$$\frac{1}{2^{2/2}} \left(|0\rangle + e^{2\pi i 0 \cdot j_1 j_2 \dots j_n} |1\rangle \right) \left(|0\rangle + e^{2\pi i 0 \cdot j_2} |1\rangle \right) |j_3 \dots j_n\rangle, \quad (5.15)$$

а применение управляемых R_2, \dots, R_{n-1} даст состояние вида

$$\frac{1}{2^{2/2}} \left(|0\rangle + e^{2\pi i 0 \cdot j_1 j_2 \dots j_n} |1\rangle \right) \left(|0\rangle + e^{2\pi i 0 \cdot j_2 \dots j_n} |1\rangle \right) \dots \left(|0\rangle + e^{2\pi i 0 \cdot j_n} |1\rangle \right) |j_3 \dots j_n\rangle. \quad (5.16)$$

Продолжая выполнять те же действия для остальных кубитов, придем в конце концов к состоянию

$$\frac{1}{2^{2/2}} \left(|0\rangle + e^{2\pi i 0 \cdot j_1 j_2 \dots j_n} |1\rangle \right) \left(|0\rangle + e^{2\pi i 0 \cdot j_2 \dots j_n} |1\rangle \right) \dots \left(|0\rangle + e^{2\pi i 0 \cdot j_n} |1\rangle \right). \quad (5.17)$$

Теперь с помощью операций обмена (см. подразд. 1.3.4), не показанных для простоты на рис. 5.1, обратим порядок кубитов. После этого получим состояние

$$\frac{1}{2^{n/2}} \left(|0\rangle + e^{2\pi i 0 \cdot j_n} |1\rangle \right) \left(|0\rangle + e^{2\pi i 0 \cdot j_{n-1} \dots j_n} |1\rangle \right) \dots \left(|0\rangle + e^{2\pi i 0 \cdot j_1 j_2 \dots j_n} |1\rangle \right). \quad (5.18)$$

Если сравнить данный результат с формулой (5.4), то окажется, что мы произвели квантовое преобразование Фурье, что и требовалось! Наша конструкция доказывает также унитарность квантового преобразования Фурье (поскольку каждый из использованных элементов унитарен). Явный пример схемы, осуществляющей квантовое преобразование Фурье на трех кубитах, приведен во вставке 5.1.

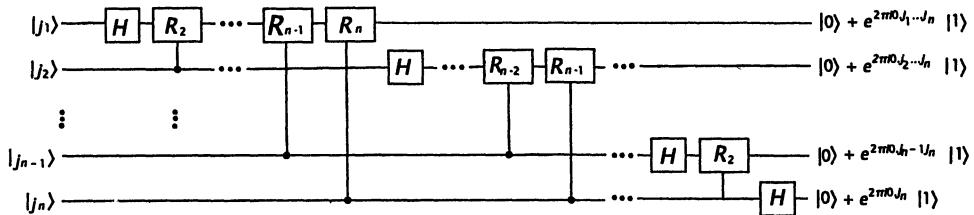
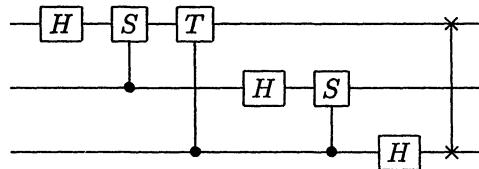


Рис. 5.1. Эффективная схема, вычисляющая квантовое преобразование Фурье. Эта схема легко получается из представления квантового преобразования Фурье в виде произведения (5.4). На рисунке не отражены операции обмена в конце схемы, обращающие порядок следования кубитов, а также нормализующие множители $1/\sqrt{2}$ в выходных состояниях.

Сколько элементов используется в нашей схеме? Сначала мы применяем элемент Адамара и $(n - 1)$ условный фазовый сдвиг к первому кубиту — всего n элементов. Затем мы применяем элемент Адамара и $(n - 2)$ условных фазовых сдвига ко второму кубиту — итого $(n + (n - 1))$ элементов. Продолжив вычисление, получим, что используются $n + (n - 1) + \dots + 1 = n(n + 1)/2$ элементов и элементы, необходимые для обращения порядка кубитов. Для выполнения последней задачи требуется не более $n/2$ обменов, а для каждого обмена нужно три элемента CNOT. Следовательно, такая схема дает алгоритм для выполнения квантового преобразования Фурье, работающий за время $\Theta(n^2)$.

Вставка 5.1. Трехкубитовое квантовое преобразование Фурье

Возможно, стоит рассмотреть конкретный пример схемы, осуществляющей квантовое преобразование Фурье на трех кубитах.



Напомним, что S и T – элементы сдвига фазы $\pi/8$. В матричном виде преобразование Фурье в этом случае можно записать следующим образом (положив $\omega = e^{2\pi i/8} = \sqrt{i}$):

$$\frac{1}{\sqrt{8}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega^1 & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{bmatrix}. \quad (5.19)$$

Стоит сравнить это с классическим случаем: лучшие известные классические алгоритмы для вычисления дискретного преобразования Фурье 2^n -компонентного вектора, такие, как *быстрое преобразование Фурье* (FFT), используют $\Theta(n2^n)$ элементов. Таким образом, для выполнения преобразования Фурье на классическом компьютере необходимо экспоненциально больше операций, чем для решения той же задачи на квантовом компьютере.

На первый взгляд это выглядит потрясающее, поскольку преобразование Фурье является ключевым шагом во многих прикладных задачах обработки данных. Например, при компьютерном распознавании речи первый шаг в распознавании фонемы состоит в том, что к оцифрованному звуку применяется именно преобразование Фурье. Может быть, стоит применить квантовое преобразование Фурье для ускорения этих вычислений? К сожалению, неизвестно никакого способа это сделать: проблема в том, что в квантовом компьютере непосредственно измерить амплитуды невозможно, так что не существует способа найти амплитуды состояния, полученного преобразованием Фурье из исходного. Более того, нет, вообще говоря, и способа приготовить исходное состояние (то, к которому мы хотим применить квантовое преобразование Фурье) в нужном виде. Так что найти применения квантовому преобразованию Фурье – задача более деликатная, чем можно было бы предположить. В этой и следующей главах мы приведем примеры нескольких алгоритмов, основанных на более тонком применении квантового преобразования Фурье.

Упражнение 5.3 (классическое быстрое преобразование Фурье).

Предположим, требуется получить на классическом компьютере преобразование Фурье вектора с 2^n комплексными компонентами. Проверьте, что при непосредственном применении формулы (5.1) для этого потребуется $\Theta(2^{2n})$ элементарных арифметических операций. Найдите способ (основанный на формуле (5.4)) сократить число таких операций до $\Theta(n2^n)$.

Упражнение 5.4. Разложите элемент «управляемое R_k » в композицию однокубитовых и СНОТ-элементов.**Упражнение 5.5.** Постройте квантовую схему, реализующую обратное квантовое преобразование Фурье.**Упражнение 5.6 (приближенное квантовое преобразование Фурье).** Очевидно, что в схеме, реализующей квантовое преобразование Фурье, применяются элементы экспоненциальной (в зависимости от числа кубитов) точности. На самом деле, однако, ни в какой квантовой схеме полиномиального размера такая точность не требуется. Пусть, например, U — идеальное квантовое преобразование Фурье на n кубит и V — преобразование, которое получится, если элементы «управляемое R_k » реализованы с точностью $\Delta = 1/p(n)$, где $p(n)$ — многочлен. Покажите, что ошибка $E(U, V) \equiv \max_{|\psi\rangle} \|(U - V)(|\psi\rangle)\|$ имеет порядок $\Theta(n^2/p(n))$ и тем самым полиномиальной точности в каждом элементе достаточно, чтобы гарантировать полиномиальную точность схемы в целом.

5.2 Определение собственного числа

Преобразование Фурье играет ключевую роль в процедуре, известной под названием *определение собственного числа*, которая в свою очередь является ключом ко многим квантовым алгоритмам. Предположим, что унитарный оператор U имеет собственный вектор $|u\rangle$ с собственным числом $e^{2\pi i\varphi}$, где значение φ неизвестно.

Цель процедуры определения собственного числа — найти оценку для φ . Мы получим такую оценку в предположении, что нам доступны *черные ящики* (называемые также *оракулами*), способные приготовить состояние $|u\rangle$ и выполнить операцию «управляемое U^{2^j} » для целого неотрицательного j .

Поскольку используются черные ящики, определение собственного числа не является само по себе настоящим квантовым алгоритмом: его нужно представлять как «подпрограмму» (или «модуль»), которая в сочетании с другими подпрограммами может решать интересные вычислительные задачи. В конкретных приложениях процедуры определения собственного числа будем действовать именно так: описывать, как можно осуществить операции, выполняемые черными ящиками, и затем использовать определение собственного числа для решения действительно интересных задач. В данный момент, однако, содержимым черных ящиков мы интересоваться не будем.

В процедуре квантового определения собственного числа используются два регистра. Первый содержит t кубитов, изначально находящихся в состоянии $|0\rangle$. Выбор значения t зависит от двух факторов: требуемой точности приближенного значения φ и необходимой вероятности успешного выполнения процедуры. Зависимость t от этих параметров будет ясна из последующего анализа.

Второй регистр содержит столько кубитов, сколько нужно для того, чтобы записать в него $|u\rangle$, и его начальное состояние есть $|u\rangle$. Определение собственного числа проводится в два этапа. В начале применяется схема, изображенная на рис. 5.2. Начинается работа этой схемы с того, что к каждому биту первого регистра применяется элемент Адамара, а затем ко второму регистру – управляемые варианты операции U , возведенной в степень, равные последовательным степеням двойки. Легко видеть, что конечное состояние первого регистра равно

$$\begin{aligned} \frac{1}{2^{t/2}} & \left(|0\rangle + 2^{2\pi i 2^{t-1}\varphi} |1\rangle \right) \left(|0\rangle + e^{2\pi i 2^{t-1}\varphi} |1\rangle \right) \dots \left(|0\rangle + e^{2\pi i 2^0\varphi} |1\rangle \right) = \\ & = \frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} e^{2\pi i \varphi k} |k\rangle. \end{aligned} \quad (5.20)$$

Про второй регистр мы здесь не упоминаем, поскольку на протяжении всего вычисления он остается в состоянии $|u\rangle$.

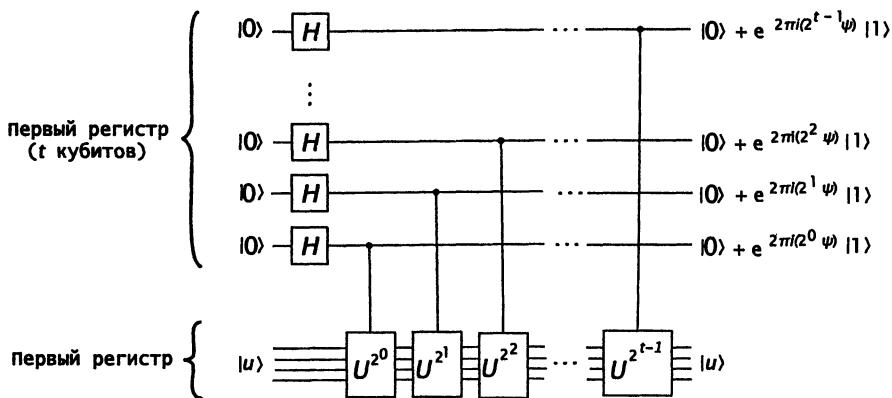


Рис. 5.2. Первый этап процедуры определения собственного числа. В правой части опущены нормирующие множители $1/\sqrt{2}$

Упражнение 5.7. Вы лучше поймете, как работает схема на рис. 5.2, если покажете, что изображенная на нем последовательность управляемых U переводит состояние $|j\rangle|u\rangle$ в $|j\rangle|U^j u\rangle$. (Отметим, что это верно и в том случае, если $|u\rangle$ не является собственным вектором U .)

Второй этап процедуры определения собственного числа состоит в том, что к первому регистру применяют *обратное* квантовое преобразование Фурье. Чтобы это сделать, надо обратить схему для квантового преобразования Фурье

из предыдущего раздела (упр. 5.5), и это достигается за $\Theta(t^2)$ шагов. Третий и заключительный этап — найти состояние первого регистра с помощью измерения в вычислительном базисе. Покажем, что при этом получается очень хорошая оценка для φ . Общая схема процедуры представлена на рис. 5.3.

Чтобы понять, почему процедура определения собственного числа работает, предположим, что φ можно точно записать с использованием t битов: $\varphi = 0.\varphi_1 \dots \varphi_t$. Тогда состояние (5.20), получаемое в конце первого этапа работы процедуры, можно переписать в виде

$$\frac{1}{2^{t/2}} \left(|0\rangle + e^{2\pi i 0 \varphi_t} |1\rangle \right) \left(|0\rangle + e^{2\pi i 0 \varphi_{t-1} \varphi_t} |1\rangle \right) \dots \left(|0\rangle + e^{2\pi i 0 \varphi_1 \varphi_2 \dots \varphi_t} |1\rangle \right). \quad (5.21)$$

На втором этапе определения собственного числа применим обратное преобразование Фурье. Если теперь сравнить (5.21) с формулой (5.4) для преобразования Фурье, то на втором этапе получим состояние $|\varphi_1 \dots \varphi_t\rangle$; теперь измерение в вычислительном базисе дает точное значение φ !

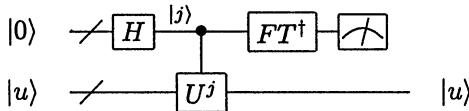


Рис. 5.3. Общая схема процедуры определения собственного числа. Верхние t кубитов (символ $<</>>$ обозначает, как обычно, набор проводов) образуют первый регистр, нижние кубиты (в количестве, необходимом для того, чтобы применить U) — второй регистр $|u\rangle$ — это собственный вектор оператора U с собственным числом $e^{2\pi i \varphi}$. Результат измерения — приближенное значение для φ с точностью 2^{-A} , где $A = t - \left\lceil \log \left(2 + \frac{1}{2\varepsilon} \right) \right\rceil$, и с вероятностью успеха не менее $(1 - \varepsilon)$.

Итак, процедура определения собственного числа позволяет оценить фазу φ собственного числа унитарного оператора U при условии, что дан соответствующий собственный вектор $|u\rangle$. Существенной частью процедуры является возможность применить обратное преобразование Фурье

$$\frac{1}{2^{t/2}} \sum_{j=0}^{2^t-1} e^{2\pi i \varphi j} |j\rangle |u\rangle \rightarrow |\tilde{\varphi}\rangle |u\rangle, \quad (5.22)$$

где $|\tilde{\varphi}\rangle$ — состояние, дающее хорошую оценку для φ при измерении.

5.2.1 Оценка скорости работы и вероятности ошибки

Приведенный выше анализ относится к идеальному случаю, когда φ может быть точно записано в виде t -битовой двоичной дроби. Что будет, если это условие не выполнено? Оказывается, описанная нами процедура с высокой вероятностью даст хорошее приближение для φ (на что и указывали обозначения в (5.22)). Доказательство этого утверждения требует известной аккуратности.

Пусть b — такое целое число из интервала $[0; 2^t - 1]$, что $b/2^t = 0.b_1 \dots b_t$ есть t -битовое приближение для φ снизу. Это означает, что разность $\delta \equiv \varphi - b/2^t$

удовлетворяет условию $0 \leq \delta \leq 2^{-t}$. Наша цель — показать, что в результате измерения в конце процедуры получится результат, близкий к b , что и дает с высокой вероятностью хорошую оценку для φ .

Применяя обратное преобразование Фурье к состоянию (5.20), получим состояние

$$\frac{1}{2^t} \sum_{k,l=0}^{2^t-1} e^{\frac{-2\pi i k l}{2^t}} e^{2\pi i \varphi k} |l\rangle. \quad (5.23)$$

Пусть α_l — амплитуда $|(b+l) \bmod 2^t\rangle$:

$$\alpha_l \equiv \frac{1}{2^t} \sum_{k=0}^{2^t-1} \left(e^{2\pi(\varphi-(b+l)/2^t)} \right)^k. \quad (5.24)$$

Это — сумма геометрической прогрессии, так что имеем

$$\alpha_l = \frac{1}{2^t} \left(\frac{1 - e^{2\pi i (2^t \varphi - (b+l))}}{2 - e^{2\pi i (\varphi - (b+l)/2^t)}} \right), \quad (5.25)$$

$$= \frac{1}{2^t} \left(\frac{1 - e^{2\pi i (2^t \delta - l)}}{1 - e^{2\pi i (\delta - l/2^t)}} \right). \quad (5.26)$$

Предположим, что результат заключительного измерения есть m . Оценим вероятность получения такого значения m , что $|m - b| > e$, где e — положительное число, характеризующее допустимую ошибку. Вероятность наблюдения такого m равна

$$p(|m - b| > e) = \sum_{-2^{t-1} < l \leq -(e+1)} |\alpha_l|^2 + \sum_{e+1 \leq l \leq 2^{t-1}} |\alpha_l|^2. \quad (5.27)$$

Однако для любого действительного θ имеем $|1 - \exp(i\theta)| \leq 2$, откуда

$$|\alpha_l| \leq \frac{2}{2^t |1 - e^{2\pi i (\delta - l/2^t)}|}. \quad (5.28)$$

Из элементарной геометрии или анализа следует, что $|1 - \exp(i\theta)| \geq 2|\theta|/\pi$ при $-\pi \leq \theta \leq \pi$. Однако при $-2^{t-1} < l \leq 2^{t-1}$ имеем $-\pi \leq 2\pi(\delta - l/2^t) \leq \pi$. Тогда можно записать

$$|\alpha_l| \leq \frac{1}{2^{t+1}(\delta - l/2^t)}. \quad (5.29)$$

Сопоставив (5.27) и (5.29), получим

$$p(|m - b| > e) \leq \frac{1}{4} \left[\sum_{l=-2^{t-1}+1}^{-(e+1)} \frac{1}{(l - 2^t \delta)^2} + \sum_{l=e+1}^{2^{t-1}} \frac{1}{(l - 2^t \delta)^2} \right]. \quad (5.30)$$

Поскольку $0 \leq 2^t \delta \leq 1$, имеем

$$p(|m - b| > e) \leq \frac{1}{4} \left[\sum_{l=-2^{t-1}+1}^{-(e+1)} \frac{1}{l^2} + \sum_{l=e+1}^{2^{t-1}} \frac{1}{(l-1)^2} \right] \quad (5.31)$$

$$\leq \frac{1}{2} \sum_{l=e}^{2^{t-1}-1} \frac{1}{l^2} \quad (5.32)$$

$$\leq \frac{1}{2} \int_{e-1}^{2^{t-1}-1} dl \frac{1}{l^2} \quad (5.33)$$

$$= \frac{1}{2(e-1)}. \quad (5.34)$$

Предположим теперь, что надо аппроксимировать φ с точностью 2^{-n} , т. е. что $e = 2^{t-n} - 1$. Если мы будем в процедуре определения собственного числа использовать $t = n+p$ кубитов, то из (5.34) следует, что вероятность получения приближения с такой точностью равна как минимум $1 - 1/2(2^p - 2)$. Тогда для того, чтобы с вероятностью не менее $1 - \varepsilon$ получить значение φ с точностью 2^{-n} , выберем

$$t = n + \left\lceil \log \left(2 + \frac{1}{2\varepsilon} \right) \right\rceil. \quad (5.35)$$

Чтобы можно было воспользоваться процедурой определения собственного числа, необходимо уметь приготавливать состояние $|u\rangle$ — собственный вектор оператора U . Как быть, если приготовить такое состояние мы не можем? Предположим, что вместо $|u\rangle$ мы подготовили какое-то состояние $|\psi\rangle$. Разложение $|\psi\rangle$ по собственным векторам оператора U имеет вид $|\psi\rangle = \sum_u c_u |u\rangle$. Пусть собственному вектору $|u\rangle$ соответствует собственное число $e^{2\pi i \varphi_u}$. Интуитивно ясно, что в результате работы процедуры определения собственного числа получится состояние, близкое к $\sum_u |\widetilde{\varphi_u}\rangle |u\rangle$, где $|\widetilde{\varphi_u}\rangle$ — хорошее приближенное значение для фазы φ_u . Следовательно, можно ожидать, что результат считывания первого регистра даст хорошее приближение к φ_u , где u выбирается случайно с вероятностью $|c_u|^2$. (Строгое проведение этого рассуждения — предмет упражнения 5.8.) Описанный прием позволяет обойтись без приготовления (возможно, неизвестного) собственного вектора за счет добавления фактора случайности в работу алгоритма.

Упражнение 5.8. Пусть процедура определения собственного числа переводит состояние $|0\rangle |u\rangle$ в состояние $|\widetilde{\psi_u}\rangle |u\rangle$, так что $|0\rangle (\sum_u c_u |u\rangle)$ переводится в $\sum_u c_u |\widetilde{\psi_u}\rangle |u\rangle$. Покажите, что если t выбрано в соответствии с (5.35), то вероятность измерения φ_u с точностью 2^{-n} не менее $|c_u|^2(1 - \varepsilon)$.

Чем интересна процедура определения собственного числа? Она представляет интерес и сама по себе, поскольку решает нетривиальную и физически интересную задачу: как оценить собственное число, соответствующее данному собственному вектору унитарного оператора. Реальная польза от этой процедуры, однако, состоит в том, что другие интересные задачи могут, как мы уви-

дим в следующих разделах, быть сведены к определению собственного числа. Запишем еще раз процедуру в целом.

Алгоритм: квантовое определение собственного числа

- Вход:** 1) черный ящик, выполняющий операции «управляемое U^j » для целых j ; 2) $|u\rangle$ — собственный вектор оператора U с собственным числом $e^{2\pi i \varphi_u}$; 3) $t = n + \left\lceil \log \left(2 + \frac{1}{2\varepsilon} \right) \right\rceil$ кубитов в состоянии $|0\rangle$.

Выход: число $\widetilde{\varphi_u}$, являющееся n -битовой аппроксимацией к φ_u .

Время выполнения: $O(t^2)$ операций и одно обращение к черному ящику, выполняющему операцию «управляемое U^j ». Вероятность успеха не менее $1 - \varepsilon$.

Процедура:

1. $|0\rangle|u\rangle$ Начальное состояние
2. $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle|u\rangle$ Создание суперпозиции
3. $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle U^j |u\rangle$ Обращение к черному ящику
 $= \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} e^{2\pi ij\varphi_u} |j\rangle|u\rangle$ Результат работы черного ящика
4. $\rightarrow |\varphi_u\rangle|u\rangle$ Быстрое преобразование Фурье
5. $\rightarrow \widetilde{\varphi_u}$ Измерение первого регистра

Упражнение 5.9. Пусть U — унитарное преобразование с собственными числами ± 1 , действующее на состояние $|\psi\rangle$. Пользуясь процедурой определения собственного числа, постройте квантовую схему, переводящую $|\psi\rangle$ в одно из двух собственных подпространств² для U и при этом информирующую (классическим образом), в какое из этих подпространств мы попали. Сравните полученный результат с упр. 4.34.

5.3 Приложения: нахождение порядка и факторизация

С помощью процедуры определения собственного числа можно решить множество задач. Рассмотрим две наиболее интересные из них: *задачу нахождения порядка* и *задачу факторизации целого числа*. На самом деле эти две задачи эквивалентны, так что в подразд. 5.3.1 мы приведем квантовый алгоритм, решающий задачу нахождения порядка, а затем в подразд. 5.3.2 объясним, как, умев находить порядок, можно разлагать числа на простые множители.

Для понимания квантовых алгоритмов факторизации и нахождения порядка требуются некоторые знания из теории чисел. Весь необходимый материал собран в Приложении 4. Описание алгоритмов в двух следующих подразделах концентрируется на квантовых аспектах задачи, и для его понимания достаточно начальных знаний арифметики остатков по модулю n . Подробные до-

² Соответствующих собственным числам 1 или -1 — *Прим. перев*

казательства используемых нами теоретико-числовых результатов собраны в Приложении 4.

Быстрые квантовые алгоритмы для нахождения порядка и факторизации интересны по меньшей мере по трем причинам. Во-первых (и в основном, по нашему мнению), наличие этих алгоритмов является свидетельством того, что квантовые компьютеры по сути своей более эффективны, чем классические, что ставит под серьезное сомнение усиленный тезис Чёрча–Тьюринга. Во-вторых, обе задачи достаточно интересны сами по себе, чтобы любой новый алгоритм для их решения, будь то классический или квантовый, представлял интерес. В-третьих (и с практической точки зрения это главное), эффективные алгоритмы для нахождения порядка и факторизации могут быть использованы для взлома крипtosистемы RSA с открытым ключом (см. Приложение 5).

5.3.1 Нахождение порядка

Если x и N – взаимно простые целые числа, причем $x < N$, то *порядком* x по модулю N называют наименьшее целое положительное число r , обладающее тем свойством, что $x^r \equiv 1 \pmod{N}$. Задача нахождения порядка состоит в том, что требуется определить этот порядок для данных x и N . Считается, что для классического компьютера эта задача трудна в том смысле, что неизвестен решающий ее алгоритм, количество операций которого полиномиально по L , где $L = \lceil \log N \rceil$ – число битов, необходимое для задания N . В этом подразделе мы объясним, как с помощью определения собственного числа построить эффективный квантовый алгоритм для нахождения порядка.

Упражнение 5.10. Покажите, что порядок числа $x = 5$ по модулю $N = 21$ равен 6.

Упражнение 5.11. Покажите, что порядок числа x удовлетворяет условию $r \leq N$.

Квантовый алгоритм для нахождения порядка представляет собой просто процедуру определения собственного числа, примененную к унитарному оператору

$$U|y\rangle \equiv |xy \pmod{N}\rangle, \quad (5.36)$$

где $y \in \{0, 1\}^L$. (Отметим, что здесь и ниже мы полагаем, что $xy \pmod{N} = y$, если $N \leq y \leq 2^L - 1$, так что U нетривиально действует только при $0 \leq y \leq N - 1$.) Простое вычисление показывает, что состояния, определенные по формулам

$$|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[\frac{-2\pi i sk}{r}\right] |x^k \pmod{N}\rangle \quad (5.37)$$

при $0 \leq s \leq r - 1$, являются собственными для U , так как

$$U|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[\frac{-2\pi i sk}{r}\right] |x^{k+1} \bmod N\rangle \quad (5.38)$$

$$= \exp\left[\frac{2\pi i s}{r}\right] |u_s\rangle. \quad (5.39)$$

С помощью процедуры определения собственного числа можно найти с высокой точностью соответствующие собственные числа $\exp(2\pi i s/r)$, откуда после небольшой дополнительной работы можно вычислить и r .

Упражнение 5.12. Покажите, что оператор U унитарен. (Указание: числа x и N взаимно простые, так что у него есть обратный по модулю N .)

Чтобы можно было применить процедуру определения собственного числа, необходимо выполнить два важных требования: в нашем распоряжении должны быть эффективные способы реализации операций «управляемое U^{2^j} » для произвольного целого j и мы должны уметь эффективно приготавливать состояние $|u_s\rangle$ с нетривиальным собственным числом или хотя бы суперпозицию таких состояний. Первому требованию удается удовлетворить благодаря процедуре, известной под названием *возвведение в степень по модулю N* , с помощью которой можно реализовать всю последовательность используемых при определении собственного числа операций «управляемое U^{2^j} », затратив на это $O(L^3)$ элементов. Как это делается, описано во вставке 5.2.

Вставка 5.2. Возвведение в степень по модулю N

Как можно вычислить последовательность операций «контролируемое U^{2^j} », используемых при определении собственного числа в алгоритме нахождения порядка? Необходимо вычислить преобразование

$$|z\rangle|y\rangle \rightarrow |z\rangle U^{z_t 2^{t-1}} \dots U^{z_1 2^0}|y\rangle \quad (5.40)$$

$$= |z\rangle x^{z_t 2^{t-1}} \times \dots \times x^{z_1 2^0} y \pmod{N} \quad (5.41)$$

$$= |z\rangle|x^z y \pmod{N}\rangle. \quad (5.42)$$

Как можно видеть, вычисление этой последовательности операций «управляемое U^{2^j} » равносильно умножению содержимого второго регистра на степень $x^z \pmod{N}$, где z — содержимое первого регистра. Эту процедуру легко реализовать, используя обратимые вычисления. Идея состоит в том, чтобы сначала обратимо вычислить $x^z \pmod{N}$ в третьем регистре, а затем обратимо умножить содержимое второго регистра на $x^z \pmod{N}$, после чего восстановить исходное состояние третьего регистра с

помощью обращения вычислений. Алгоритм включает два этапа. Сначала, последовательно возводя в квадрат по модулю N , мы находим $x^{2^j} \pmod{N}$ для всех j , не превосходящих $t-1$. У нас $t = 2L+1+\lceil \log(2+1/(2\epsilon)) \rceil = O(L)$, так что для этого требуется $t-1 = O(L)$ возведений в квадрат, каждое за $O(L^2)$ операций (подразумевается, что мы возводим в квадрат путем умножения столбиком), поэтому общее количество операций на первом этапе есть $O(L^3)$. Второй этап алгоритма основан на том, что, как было отмечено,

$$x^z \pmod{N} = \left(x^{z_t 2^{t-1}} \pmod{N} \right) \left(x^{z_{t-1} 2^{t-2}} \pmod{N} \right) \dots \left(x^{z_1 2^0} \pmod{N} \right). \quad (5.43)$$

Проведя $t-1$ умножение по модулю N , каждое за $O(L^2)$ операций, получим, что произведение можно вычислить с использованием $O(L^3)$ элементов. Для наших целей такой производительности достаточно, но имеются и более эффективные алгоритмы, основанные на быстрых алгоритмах умножения (см. раздел «История и дополнительная литература» в конце главы). Теперь с помощью метода из подразд. 3.5, легко построить обратимую схему из $O(L^3)$ элементов с t - и L -битовым регистрами, которая переводит состояние (z, y) в $(z, x^z y \pmod{N})$; эту схему можно переделать в квантовую схему, использующую $O(L^3)$ регистров и вычисляющую преобразование $|x\rangle|y\rangle \rightarrow |z\rangle|x^z y \pmod{N}\rangle$.

Второе требование более изощренное: ведь чтобы приготовить $|u_s\rangle$, необходимо заранее знать r , о чём и речи быть не может. К счастью, одно остроумное наблюдение позволяет обойти эту проблему. Заметим, что

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle. \quad (5.44)$$

При определении собственного числа используем $t = 2L + 1 + \left\lceil \log \left(2 + \frac{1}{2\epsilon} \right) \right\rceil$ кубитов в первом регистре (в соответствии с обозначениями на рис. 5.3) и приготавливаем второй регистр в состоянии $|1\rangle$, что тривиально. Тогда для каждого s из интервала $[0; r-1]$ найдем оценку фазы собственного числа $\varphi \approx s/r$ с точностью 2^{-2L-1} и вероятностью успеха не менее $(1-\epsilon)/r$. Общая схема работы алгоритма нахождения порядка изображена на рис. 5.4.

Упражнение 5.13. Выведите формулу (5.44). Докажите, что на самом деле

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{2\pi sk/r} |u_s\rangle = |x^k \pmod{N}\rangle. \quad (5.45)$$

(Указание: $\sum_{s=0}^{r-1} \exp(-2\pi i sk/r) = r\delta_{k0}$.)

Упражнение 5.14. Квантовое состояние, получаемое в алгоритме нахождения порядка до применения обратного преобразования Фурье, имеет вид

$$|\psi\rangle = \sum_{j=0}^{2^t-1} |j\rangle U^j |1\rangle = \sum_{j=0}^{2^t-1} |j\rangle |x^j \bmod N\rangle, \quad (5.46)$$

если начальное состояние второго регистра $|1\rangle$. Покажите, что получится то же состояние, если U^j заменить на другое унитарное преобразование:

$$V|j\rangle|k\rangle = |j\rangle|k + x^j \bmod N\rangle, \quad (5.47)$$

и если начальным состоянием второго регистра был $|0\rangle$. Объясните также, как сконструировать V с использованием $O(L^3)$ элементов.

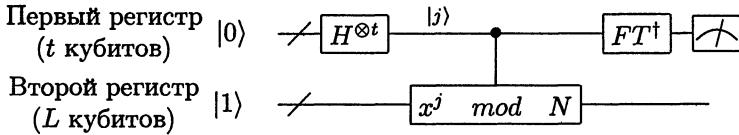


Рис. 5.4. Квантовая схема для алгоритма нахождения порядка. На рисунке кубиты второго регистра установлены в состояние $|1\rangle$, но если применить метод упр. 5.14, то их можно установить и в состояние $|0\rangle$. Если использовать результаты подразд. 5.3.2, то эту схему можно применить и для факторизации.

Разложение в непрерывную дробь

Сведение задачи вычисления порядка к определению собственного числа будет завершено, когда мы опишем, как находить искомое число r , исходя из числа $\varphi \approx s/r$, являющегося результатом работы процедуры определения собственного числа. Нам известно число φ только с точностью 2^{-2L-1} , но также известно, что это *рациональное* число — отношение двух целых, величина которых ограничена сверху, поэтому если мы сможем вычислить ближайшее к φ число с такими свойствами, то мы найдем и r .

Замечательным образом существует алгоритм, эффективно решающий эту задачу; он известен под названием *алгоритма цепных дробей*. Пример того, как он работает, приведен во вставке 5.3. Объяснение того, почему этот алгоритм отвечает нашим целям, дает следующая ниже теорема, доказательство которой приведено в Приложении 4.

Теорема 5.1. Пусть r/s — такое рациональное число, что

$$\left| \frac{s}{r} - \varphi \right| \leq \frac{1}{2r^2}. \quad (5.48)$$

Тогда s/r является подходящей дробью для φ и тем самым может быть вычислена за $O(L^3)$ операций с помощью алгоритма разложения в цепную дробь.

Поскольку φ является приближением для s/r с точностью 2^{-2L-1} , то $|s/r - \varphi| \leq 2^{-2L-1} \leq 1/2r^2$, так как $r \leq N \leq 2^L$. Таким образом, теорема в нашем случае применима.

Алгоритм цепных дробей эффективно вычисляет такие взаимно-простые числа s' и r' , так что $s'/r' = s/r$. Число r' является нашим кандидатом на то, чтобы быть порядком x . Можно проверить, действительно ли это порядок, вычислив $x^{r'} \bmod N$ и посмотрев, получится ли 1. Если получилась 1, то r' является порядком x по модулю N .

Как же все-таки найти порядок?

В каких случаях алгоритм нахождения порядка может дать неверный результат? Для этого имеется две возможности. Во-первых, определение собственного числа может выдать плохое приближение для s/r . Такое случается с вероятностью, не превосходящей ϵ , и эту вероятность можно сделать сколь угодно малой за счет несущественного увеличения размеров схемы. Более серьезная проблема состоит в том, что у s и r может быть общий множитель, и в этом случае разложение в цепную дробь даст не само число r , а число r' , являющееся его делителем. Однако существует не менее трех способов обойти эту проблему.

Возможно, самый простой способ — заметить, что для случайно выбранного $s \in [0; r-1]$ весьма вероятно, что s будет взаимно просто с r , а в этом случае алгоритм цепных дробей выдаст r . Чтобы понять, почему это так, укажем, что, согласно задаче 4.1 количество простых чисел, меньших r , не менее $r/2 \log r$, и тем самым вероятность того, что s просто (и тем самым взаимно просто с r), не менее, чем $1/2 \log r > 1/2 \log N$. Таким образом, повторив алгоритм $2 \log N$ раз, можно с высокой вероятностью измерить такую фазу s/r , что s и r взаимно просты, и тогда алгоритм цепных дробей выдаст r , что и требовалось.

Вставка 5.3. Алгоритм цепных дробей

Идея алгоритма цепных дробей состоит в том, чтобы представить действительные числа с помощью целых, используя выражения вида

$$[a_0, \dots, a_M] \equiv a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_M}}}}, \quad (5.49)$$

где a_0, \dots, a_M — целые положительные числа. (Применительно к квантовым вычислениям удобно считать, что $a_0 = 0$.) Определим m -ую ($0 \leq m \leq M$) подходящую дробь как $[a_0, \dots, a_m]$. Алгоритм цепных дробей — это алгоритм для нахождения разложения произвольного действительного числа в цепную дробь. Рассмотрим пример. Пусть мы хотим представить в виде цепной дроби число $31/13$. Первый шаг — выделить в дроби $31/13$ целую часть:

$$\frac{31}{13} = 2 + \frac{5}{13}. \quad (5.50)$$

Обратив дробную часть, получим

$$\frac{31}{13} = 2 + \frac{1}{\frac{13}{5}}. \quad (5.51)$$

Теперь применим ту же операцию (выделение целой части и обращение дробной) к $13/5$:

$$\frac{31}{13} = 2 + \frac{1}{2 + \frac{3}{5}} = 2 + \frac{1}{2 + \frac{1}{\frac{5}{3}}}. \quad (5.52)$$

Далее выделим целую часть и обратим дробную у $5/3$:

$$\frac{31}{13} = 2 + \frac{1}{2 + \frac{1}{1 + \frac{2}{3}}} = 2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{\frac{3}{2}}}}. \quad (5.53)$$

На этом разложение в цепную дробь завершается, поскольку

$$\frac{3}{2} = 1 + \frac{1}{2} \quad (5.54)$$

может быть записано с единицей в числителе, и обращать дробную часть уже незачем; окончательно разложение $31/13$ в цепную дробь имеет вид

$$\frac{31}{13} = 2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}}. \quad (5.55)$$

Ясно, что алгоритм цепных дробей завершается за конечное число шагов для любого рационального числа, так как последовательность числителей ($31, 5, 3, 2, 1$ в приведенном здесь примере) является строго убывающей. Насколько быстро заканчивается этот алгоритм? Оказывается, что если $\varphi = s/r$ — рациональное число, причем s и r являются L — битовыми целыми числами, то разложение φ в цепную дробь можно провести за $O(L^3)$ операций: $O(L)$ операций для выделения целой части и обращения дробной, каждая из которых использует $O(L^2)$ операций для выполнения арифметических действий.

Второй способ состоит в том, чтобы заметить, что если $r' \neq r$, то r' обязательно будет делителем r (кроме случая, когда $s = 0$, но вероятность этого равна $1/r \leq 1/2$, причем с помощью повторений эту вероятность можно быстро уменьшить). Заменим a на $a' \equiv a^{r'} \pmod{N}$. Тогда порядок a' будет равен r/r' . Повторим алгоритм и попытаемся посчитать порядок a' ; если все получится, то мы будем знать и порядок a , поскольку $r = r' \times r/r'$. Если не получится,

то в нашем распоряжении будет число r'' , являющееся делителем r/r' , и мы попробуем найти порядок числа $a'' \equiv (a')^{r''} \pmod{N}$. Будем продолжать эту процедуру, пока порядок a не будет найден. Нам может потребоваться не более чем $\log r = O(L)$ итераций, поскольку каждая итерация уменьшает порядок очередного a'' · по крайней мере вдвое.

Третий способ лучше первых двух в том отношении, что в нем используется $O(1)$ попыток, а не $O(L)$. Необходимо дважды повторить процедуру определения собственного числа с последующим разложением в цепную дробь; обозначим найденные при этом числа как $r'_1 = r/q'_1$ (первая попытка) и $r'_2 = r/q'_2$ (вторая попытка). Если q'_1 и q'_2 взаимно просты, то r будет равно наименьшему общему кратному r'_1 и r'_2 ; вероятность же того, что q'_1 и q'_2 не взаимно просты, равна

$$1 - \sum_q p(q|q'_1)p(q|q'_2), \quad (5.56)$$

где сумма берется по всем простым числам q , и $p(x|y)$ — вероятность того, что x делит y . Ясно, что вероятность того, что q делит q'_1 , не превосходит $1/q$, и то же верно для $p(q|q'_2)$. Следовательно, вероятность того, что q'_1 и q'_2 взаимно просты, не меньше, чем

$$1 - \sum_q p(q|q'_1)p(q|q'_2) \geq 1 - \sum_q \frac{1}{q^2}. \quad (5.57)$$

Правую часть можно оценить снизу многими разными способами; например простой способ, представленный в упр. 5.16, дает

$$1 - \sum_q p(q|q'_1)p(q|q'_2) \geq \frac{1}{4}, \quad (5.58)$$

так что вероятность нахождения правильного значения r не менее $1/4$.

Упражнение 5.15. Покажите, что наименьшее общее кратное целых положительных чисел x и y равно $xy/\text{НОД}(x, y)$ и тем самым может быть вычислено за $O(L^2)$ операций, если x и y — L -битовые числа.

Упражнение 5.16. Докажите, что для всех $x \geq 2$ имеем $\int_x^{x+1} 1/y^2 dy \geq 2/3x^2$. Покажите, что

$$\sum_q \frac{1}{q^2} \leq \frac{3}{2} \int_2^\infty \frac{1}{y^2} dy = \frac{3}{4}, \quad (5.59)$$

т. е. выполнено неравенство (5.58).

Сколько ресурсов требуется описанному здесь алгоритму? Для преобразования Адамара необходимо $O(L)$ элементов, а для обратного преобразования Фурье — $O(L^2)$. Основные затраты идут на возведение в степень по модулю N : для этого нужно $O(L^3)$ элементов; для разложения в непрерывную дробь также необходимо $O(L^3)$ элементов, так что для нахождения r' требуется $O(L^3)$ элементов. Если воспользоваться третьим методом для нахождения r по r' , то

всю эту процедуру следует повторить постоянное число раз, поэтому затраты на нахождение r также равны $O(L^3)$. Ниже следует описание алгоритма в целом.

Квантовое нахождение порядка

Вход: 1) черный ящик $U_{x,N}$, выполняющий преобразования $|j\rangle|k\rangle \rightarrow |j\rangle|x^j k \bmod N\rangle$ для x , являющихся взаимно простыми с L -битовым целым числом N ; 2) $t = 2L + 1 + \left\lceil \log \left(2 + \frac{1}{2\varepsilon} \right) \right\rceil$ кубит в состоянии $|0\rangle$; 3) L кубитов в состоянии $|1\rangle$.

Выход: наименьшее целое $r > 0$, обладающее тем свойством, что $x^r \equiv 1 \pmod{N}$.

Время выполнения: $O(L^3)$ операций; вероятность успеха $\Omega(1)$.

Процедура:

1. $|0\rangle|1\rangle$ Начальное состояние
2. $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle|1\rangle$ Создать суперпозицию
3. $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle|x^j \bmod N\rangle$ Применить $U_{x,N}$
 $\approx \frac{1}{\sqrt{r2^t}} \sum_{s=0}^{r-1} \sum_{j=0}^{2^t-1} e^{2\pi i s j / r} |j\rangle|u_s\rangle$
4. $\rightarrow \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\widetilde{s/r}\rangle|u_s\rangle$ Применить обратное преобразование
Фурье к первому регистру
5. $\rightarrow \widetilde{s/r}$ Измерить первый регистр
6. $\rightarrow r$ Применить алгоритм цепных дробей

5.3.2 Факторизация

Проблема отличения простых чисел от составных и разложение составных чисел на простые множители является одной из наиболее важных и нужных во всей арифметике. [...] Дело чести для ученых — всячески приветствовать и поддерживать любую помочь в решении этой красавой и знаменитой проблемы.

К. Фридрих Гаусс (цитируется по Д. Кнуту)

Дано составное число N ; произведением каких простых чисел оно является? Так формулируется задача разложения на множители (*задача факторизации*), и оказывается, что она эквивалентна изученной нами задаче нахождения порядка в том смысле, что быстрый алгоритм для нахождения порядка легко

переделать в быстрый алгоритм для факторизации. В этом подразделе мы объясним, как свести факторизацию к нахождению порядка, и приведем простой пример.

Сведение факторизации к нахождению порядка проводится в два шага. На первом шаге показано, что можно найти нетривиальный делитель числа N , если только можно найти нетривиальное решение $x \neq \pm 1 \pmod{N}$ уравнения $x^2 = 1 \pmod{N}$. На втором шаге доказывается, что случайно выбранное число y , взаимно простое с N , с большой вероятностью будет иметь четный порядок r , причем такой, что $y^{r/2} \neq \pm 1 \pmod{N}$. Эти два шага оформлены в виде двух теорем, доказательства которых можно найти в разд. А4.3 Приложения 4.

Теорема 5.2. Пусть N — L -битовое составное число, а x — решение уравнения $x^2 = 1 \pmod{N}$, лежащее в интервале $[1; N]$ и удовлетворяющее условию $x \neq \pm 1 \pmod{N}$ (мы будем называть такие решения нетривиальными). Тогда хотя бы одно из чисел $\text{НОД}(x - 1, N)$ и $\text{НОД}(x + 1, N)$ является нетривиальным делителем числа N , и этот делитель можно вычислить за $O(L^3)$ операций.

Теорема 5.3. Пусть $N = p_1^{\alpha_1} \dots p_m^{\alpha_m}$ — разложение на простые множители нечетного составного целого положительного числа, а x — случайно выбранное целое число, взаимно-простое с N и удовлетворяющее условиям $1 \leq x \leq N - 1$ (случайный выбор таков, что все эти числа равновероятны). Тогда

$$p(r \text{ четно и } x^{r/2} \neq -1 \pmod{N}) \geq 1 - \frac{1}{2^m}. \quad (5.60)$$

Если объединить теоремы 5.2 и 5.3, то получим алгоритм, который с высокой вероятностью выдает нетривиальный делитель любого составного числа N . Все шаги алгоритма могут быть эффективно реализованы на классическом компьютере, за исключением (насколько нам известно в настоящее время) «подпрограммы» для нахождения порядка. Повторяя эту процедуру, получим разложение числа N . Приведем этот алгоритм.

Алгоритм: сведение факторизации к нахождению порядка

Вход: составное число N .

Выход: нетривиальный делитель числа N .

Время выполнения: $O((\log N)^3)$ операций; вероятность успеха $\Omega(1)$.

Процедура:

1. Если N четно, выдать делитель 2.
2. Выяснить, не выполнено ли равенство $N = a^b$ для некоторых целых чисел $a \geq 1$ и $b \geq 2$; если да, то выдать делитель a (для выполнения этого шага воспользоваться классическим алгоритмом — см. упр. 5.17).

3. Выбрать случайным образом число x из интервала $[1; N - 1]$. Если $\text{НОД}(x, N) > 1$, выдать делитель $\text{НОД}(x, N)$.
4. С помощью алгоритма нахождения порядка найти число r , являющееся порядком x по модулю N .
5. Если r четно и $x^{r/2} \neq -1 \pmod{N}$, вычислить $\text{НОД}(x^{r/2} - 1, N)$ и $\text{НОД}(x^{r/2} + 1, N)$ и проверить, не является ли одно из этих чисел нетривиальным делителем N ; если да, выдать его, если нет, то выполнение алгоритма завершается безуспешно.

На шагах 1 и 2 либо алгоритм выдает делитель, либо мы убеждаемся, что N — нечетное число, имеющее более одного простого делителя. Эти два шага можно выполнить за $O(1)$ и $O(L^2)$ операций соответственно. На шаге 3 алгоритм либо выдает делитель, либо порождает случайный элемент x множества $\{0, 1, 2, \dots, N - 1\}$. На шаге 4 с помощью алгоритма нахождения порядка отыскивается число r — порядок x по модулю N . Шаг 5 завершает алгоритм, поскольку теорема 5.3 гарантирует, что с вероятностью не менее $1/2$ число r будет четным, и при этом $x^{r/2} \neq -1 \pmod{N}$, а в соответствии с теоремой 5.3 либо $\text{НОД}(x^{r/2} - 1, N)$, либо $\text{НОД}(x^{r/2} + 1, N)$ будет нетривиальным делителем числа N . Пример, иллюстрирующий работу алгоритма с использованием подпрограммы нахождения порядка, приведен во вставке 5.4.

Упражнение 5.17. Пусть число N записывается L битами. Цель этого упражнения — найти эффективный классический алгоритм, выясняющий, верно ли, что $N = a^b$ для некоторых целых чисел $a \geq 1$ и $b \geq 2$. Это можно сделать следующим образом:

1. Покажите, что $b \leq L$ (если b существует).
2. Покажите, что не более чем за $O(L^2)$ операций можно вычислить $y = \log_2 N$, $x = y/b$ (где $b \leq L$) и найти два целых числа u_1 и u_2 , ближайших к 2^x .
3. Покажите, что не более чем за $O(L^2)$ операций можно вычислить u_1^b и u_2^b (пользуйтесь возведением в квадрат) и проверить, не равно ли одно из этих чисел числу N .
4. Объединяя два предыдущих результата, покажите, что за $O(L^3)$ операций можно выяснить, верно ли, что $N = a^b$ для целых a и b .

Упражнение 5.18 (разложение числа 91). Пусть мы хотим разложить на множители число $N = 91$. Убедитесь, что на шагах 1 и 2 алгоритм не останавливается. На шаге 3 предположим, что мы выбрали $x = 4$ (это число взаимно просто с 91). Вычислите r — порядок x по модулю N и покажите, что $x^{r/2} \pmod{91} = 64 \neq -1 \pmod{91}$, так что алгоритм успешно завершается и выдает $\text{НОД}(64 - 1, 19) = 7$.

Вряд ли это самый эффективный из известных вам способов разложения числа 91 на множители. И действительно, если выполнять вычисления на классическом компьютере, этот способ ничего не даст, так как неизвестен хороший классический алгоритм нахождения порядка.

Упражнение 5.19. Покажите, что $N = 15$ — наименьшее число, для которого при разложении на множители по описанному алгоритму требуется нахождение порядка (т. е. наименьшее составное число, не являющееся ни четным, ни степенью меньшего числа).

Вставка 5.4. Квантовомеханическое разложение числа 15

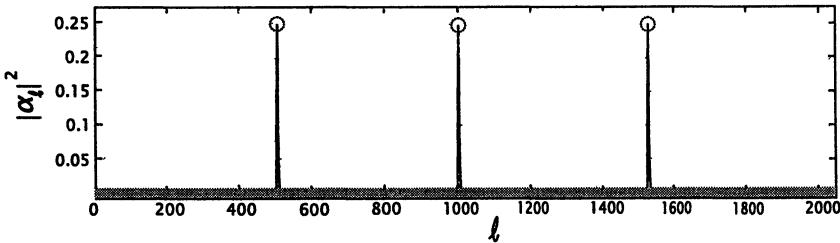
Использование нахождения порядка, определения собственного числа и разложения в цепную дробь в квантовом алгоритме факторизации можно проиллюстрировать на примере числа $N = 15$. В начале выберем случайное число, взаимно простое с N ; предположим, мы выбрали $x = 7$. Теперь вычислим r — порядок x по модулю N — с помощью квантового алгоритма: начнем с состояния $|0\rangle|0\rangle$ и создадим состояние

$$\frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} |k\rangle|0\rangle = \frac{1}{\sqrt{2^t}} [|0\rangle + |1\rangle + |2\rangle + \dots + |2^t-1\rangle] |0\rangle, \quad (5.61)$$

применяя $t = 11$ преобразований Адамара к первому регистру. При выборе этого значения t вероятность ошибки, обозначаемая ε , не будет превышать $1/4$. Затем вычислим $f(k) = x^k \pmod{N}$ и оставим результат во втором регистре:

$$\begin{aligned} & \frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} |k\rangle|x^k \pmod{N}\rangle \\ &= \frac{1}{\sqrt{2^t}} [|0\rangle|1\rangle + |1\rangle|7\rangle + |2\rangle|4\rangle|3\rangle|13\rangle + |4\rangle|13\rangle + |4\rangle|1\rangle + |5\rangle|7\rangle + |6\rangle|4\rangle + \dots]. \end{aligned} \quad (5.62)$$

Теперь применим обратное преобразование Фурье FT^\dagger к первому регистру и измерим его. Один из возможных способов изучить распределение результатов — вычислить редуцированную матрицу плотности для первого регистра, применить к ней FT^\dagger и найти статистику измерений. Однако поскольку никаких дальнейших операций со вторым регистром произойдет не будет, вместо этого можно применить принцип неявного измерения (разд. 4.4) и принять, что второй регистр измеряется, причем получается случайный результат: 1, 7, 4 или 13. Пусть вышло 4 (подошел бы и любой другой результат); это означает, что на вход оператору FT^\dagger подается $\sqrt{\frac{4}{2^t}} (|2\rangle + |6\rangle + |10\rangle + |14\rangle + \dots)$. Применив FT^\dagger , получим некоторое состояние $\sum_l \alpha_l |l\rangle$ (на рисунке показано распределение вероятностей для $2^t = 2048$).



Таким образом, заключительное измерение дает 0, 512, 1024 или 1536 (каждый результат — с вероятностью $1/4$). Пусть мы получили $l = 1536$; разложив в цепную дробь, имеем $1536/2048 = 1/(1 + (1/3))$, так что $3/4$ является подходящей дробью в разложении, откуда $r = 4$ является порядком числа $x = 7$. Удачным образом оказывается, что r четно, и более того, $x^{r/2} \bmod N = 7^2 \bmod 15 = 4 \neq -1 \pmod{15}$, так что алгоритм успешно сработал: вычисляя наибольшие общие делители $\text{НОД}(x^2 - 1, 15) = 3$ и $\text{НОД}(x^2 + 1, 15) = 5$, получим, что $15 = 3 \times 5$.

5.4 Общие приложения квантового преобразования Фурье

Основные приложения квантового преобразования Фурье, описанные выше, — определение собственного числа и нахождение порядка. Какие еще задачи можно решить таким образом? В этом разделе мы сформулируем общую задачу, известную как *задача о скрытой подгруппе*, и опишем эффективный квантовый алгоритм ее решения. Эта задача, включающая все известные «экспоненциально быстрые» приложения квантового преобразования Фурье, может рассматриваться как обобщение задачи о нахождении неизвестного периода периодической функции в ситуации, когда область определения и множество значений функции очень сложные. Чтобы представить эту задачу в более доступной форме, начнем изложение с двух частных приложений: нахождения периода (у одномерной функции) и вычисления дискретного логарифма, а затем вернемся к общей задаче о скрытой подгруппе. Материал в этом разделе представлен более сжато, чем в начальных разделах главы, а это означает, что читатель, желающий вникнуть во все детали, должен будет приложить больше усилий.

5.4.1 Нахождение периода

Рассмотрим следующую задачу. Пусть f — периодическая функция, значения которой 0 и 1, удовлетворяющая условию $f(x+r) = f(x)$ для некоторого неизвестного r , $(0 < r < 2^k)$, где $x, r \in \{0, 1, 2, \dots\}$. Если дан квантовый черный ящик U , выполняющий унитарную операцию $U|x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$ (здесь \oplus —

сложение по модулю 2), то сколько обращений к этому черному ящику и прочих операций следует сделать для нахождения r ? Заметим, что на практике U действует на конечном множестве, размер которого определяется точностью, с которой надо определить r . Приведем квантовый алгоритм, находящий r за один запрос и $O(L^2)$ других операций.

Алгоритм: нахождение периода

Вход: 1) черный ящик, выполняющий операцию $U|x\rangle|y\rangle \rightarrow |x\rangle|y\oplus f(x)\rangle$; 2) регистр, в который будут записываться значения функции, его кубиты установлены в состояние $|0\rangle$; 3) $t = O(L + \log(1/\varepsilon))$ кубитов в состоянии $|0\rangle$.

Выход: наименьшее целое $r > 0$, для которого верно тождество $f(x+r) = f(x)$.

Время выполнения: одно использование U и $O(L^2)$ операций; вероятность успеха $\Omega(1)$.

Процедура:

1. $|0\rangle|0\rangle$ Начальное состояние
2. $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |x\rangle|0\rangle$ Создать суперпозицию
3. $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |x\rangle|f(x)\rangle$ Применить U
 $\approx \frac{1}{\sqrt{r2^t}} \sum_{\ell=0}^{r-1} \sum_{x=0}^{2^t-1} e^{2\pi i \ell x / r} |x\rangle|\hat{f}(\ell)\rangle$
4. $\rightarrow \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} |\tilde{\ell}/r\rangle|\hat{f}(\ell)\rangle$ Применить обратное преобразование Фурье к первому регистру
5. $\tilde{\ell}/r$ Измерить первый регистр
6. $\rightarrow r$ Применить алгоритм цепных дробей

Основным в этом алгоритме, основанном на определении собственного числа и очень похожем на квантовый алгоритм нахождения порядка, является шаг 3, на котором мы вводим состояние

$$|\hat{f}(\ell)\rangle \equiv \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{-2\pi i \ell x / r} |f(x)\rangle, \quad (5.63)$$

являющееся преобразованием Фурье от $|f(x)\rangle$. Тождество, использованное в шаге 3, основано на равенстве

$$|f(x)\rangle = \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} e^{2\pi i \ell x / r} |\hat{f}(\ell)\rangle, \quad (5.64)$$

которое легко проверить, если заметить, что сумма $\sum_{\ell=0}^{r-1} e^{2\pi i \ell x / r}$ равна r , если x делится на r , и нулю в противном случае. Знак приближенного равенства на

шаге 3 стоит потому, что, вообще говоря, 2^t не обязано делиться на r (эта возможность учитывается процедурой определения собственного числа). С учетом формулы (5.22) применение обратного преобразования Фурье к первому регистру на шаге 4 дает оценку фазы ℓ/r , где ℓ выбирается случайно. Число r находится на последнем шаге с помощью цепных дробей.

Вставка 5.5. Инвариантность преобразования Фурье относительно сдвигов

Преобразование Фурье (5.1) обладает интересным и полезным свойством, известным как *инвариантность относительно сдвигов*. Запишем квантовое преобразование Фурье в виде

$$\sum_{h \in H} \alpha_h |h\rangle \rightarrow \sum_{g \in G} \tilde{\alpha}_g |g\rangle, \quad (5.65)$$

где $\tilde{\alpha}_g = \sum_{h \in H} \alpha_h \exp(2\pi i gh/|G|)$, H — подмножество в G , а G — множество индексов, нумерующих состояния из некоторого ортонормального базиса в гильбертовом пространстве (например, для n -кубитовой системы G может быть множеством чисел от 0 до $2^n - 1$), а $|G|$ — число элементов в G . Предположим, мы применили к начальному состоянию унитарный оператор U_k , действующий по формуле

$$U_k |g\rangle = |g + k\rangle, \quad (5.66)$$

а затем — преобразование Фурье. Полученный результат

$$U_k \sum_{h \in H} \alpha_h |h\rangle = \sum_{h \in H} \alpha_h |h + k\rangle \rightarrow \sum_{g \in G} e^{2\pi i gk/|G|} \tilde{\alpha}_g |g\rangle \quad (5.67)$$

обладает тем свойством, что абсолютные величины амплитуд состояний $|g\rangle$ не меняются, каким бы ни было k : $|\exp(2\pi i gk/|G|)\tilde{\alpha}_g| = |\tilde{\alpha}_g|$.

На языке теории групп G — это группа, H — ее подгруппа, а утверждение состоит в том, что если функция f постоянна на смежных классах по H , то и ее преобразование Фурье инвариантно относительно H .

Почему же этот алгоритм работает? Можно, например, рассмотреть (5.63) как преобразование Фурье функции $|f(x)\rangle$ на множестве $\{0, 1, \dots, 2^\ell - 1\}$ (см. упр. 5.20); это преобразование Фурье обладает интересным свойством, называемым *инвариантностью относительно сдвигов*, описанным во вставке 5.5. Другой способ понять, на чем основан этот алгоритм, — заметить, что алгоритм нахождения порядка определяет период функции $f(k) = x^k \bmod N$, так что не удивительно, что аналогичным методом можно найти период и произвольной функции. Еще один способ — заметить, что черный ящик U естественным образом реализуется с помощью унитарного оператора, собственные числа ко-

торого как раз равны $|\hat{f}(\ell)\rangle$ (см. упр. 5.21), так что можно применить процедуру определения собственного числа из разд. 5.2.

Упражнение 5.20. Пусть $f(x+r) = f(x)$ и $0 \leq x < N$, где N — целое кратное числа r . Вычислите

$$\hat{f}(\ell) \equiv \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{-2\pi i \ell x / N} f(x) \quad (5.68)$$

и сравните свой результат с (5.65). Вам понадобится тот факт, что

$$\sum_{k \in \{0, r, 2r, \dots, N-r\}} e^{2\pi i k \ell / N} = \begin{cases} \sqrt{N/r} & \text{если } \ell \text{ делится на } N/r \\ 0 & \text{иначе.} \end{cases} \quad (5.69)$$

Упражнение 5.21 (нахождение периода и определение собственного числа). Пусть дан унитарный оператор U_y , осуществляющий преобразование $U_y|f(x)\rangle = |f(x+y)\rangle$ для описанной выше периодической функции.

- Покажите, что собственными векторами этого оператора являются $|\tilde{f}(l)\rangle$ и найдите их собственные числа.
- Покажите, что в предположении, что дано $|f(x_0)\rangle$ для некоторого x_0 , с помощью оператора U_y можно реализовать черный ящик, который можно использовать для нахождения периода.

5.4.2 Дискретный логарифм

Задача нахождения периода, которую мы только что рассмотрели, проста в том отношении, что функция отображала целые числа в целые числа. Что происходит с более сложными функциями? Рассмотрим функцию $f(x_1, x_2) = a^{sx_1+x_2} \bmod N$ (переменные — целые числа), и пусть r — порядок x по модулю N . Эта функция периодическая, поскольку $f(x_1 + l, x_2 - ls) = f(x_1, x_2)$ для целых l , но здесь периоды — это пары целых чисел $(l, -ls)$. Эта функция производит странное впечатление, но она очень полезна в криптографии, поскольку нахождение s позволяет решить задачу, известную как *задача о дискретном логарифме*: даны a и $b = a^s$; чему равно s ? Ниже приводится квантовый алгоритм, решающий эту задачу за одно обращение к черному ящику U , осуществляющему унитарное преобразование $U|x_1\rangle|x_2\rangle|y\rangle = |x_1\rangle|x_2\rangle|y \oplus f(x)\rangle$ (где \oplus — побитовое сложение по модулю 2) и $O(\lceil \log r \rceil^2)$ других операций. Мы предполагаем, что число r (порядок a по модулю N) уже найдено с помощью алгоритма нахождения порядка.

Алгоритм: дискретный логарифм

Вход: 1) черный ящик, осуществляющий операцию $U|x_1\rangle|x_2\rangle|y\rangle = |x_1\rangle|x_2\rangle|y \oplus f(x_1, x_2)\rangle$, где $f(x_1, x_2) = b^{x_1}a^{x_2}$; 2) регистр для значений функции, кубиты

которого установлены в состояние $|0\rangle$; 3) два $t = O(\lceil \log r \rceil + \log(1/\varepsilon))$ -кубитовых регистра, установленных в $|0\rangle$.

Выход: Наименьшее положительное число s , для которого верно равенство $a^s = b$.

Время выполнения: одно обращение к U плюс $O(\lceil \log r \rceil^2)$ операций. Вероятность успеха $\Omega(1)$.

Процедура:

1. $|0\rangle|0\rangle|0\rangle$ Начальное состояние
2. $\rightarrow \frac{1}{2^t} \sum_{x_1=0}^{2^t-1} \sum_{x_2=0}^{2^t-1} |x_1\rangle|x_2\rangle|0\rangle$ Создать суперпозицию
3. $\rightarrow \frac{1}{2^t} \sum_{x_1=0}^{2^t-1} \sum_{x_2=0}^{2^t-1} |x_1\rangle|x_2\rangle|f(x_1, x_2)\rangle$ Применить U
 $\approx \frac{1}{2^t\sqrt{r}} \sum_{\ell_2=0}^{r-1} \sum_{x_1=0}^{2^t-1} \sum_{x_2=0}^{2^t-1} e^{2\pi i(s\ell_2 x_1 + \ell_2 x_2)/r} |x_1\rangle|x_2\rangle|\hat{f}(s\ell_2, \ell_2)\rangle$
 $= \frac{1}{2^t\sqrt{r}} \sum_{\ell_2=0}^{r-1} \left[\sum_{x_1=0}^{2^t-1} e^{2\pi i(s\ell_2 x_1)/r} |x_1\rangle \right] \left[\sum_{x_2=0}^{2^t-1} e^{2\pi i(\ell_2 x_2)/r} |x_2\rangle \right] |\hat{f}(s\ell_2, \ell_2)\rangle$
4. $\rightarrow \frac{1}{\sqrt{r}} \sum_{\ell_2=0}^{r-1} |\widetilde{s\ell_2/r}\rangle|\widetilde{\ell_2/r}\rangle|\hat{f}(s\ell_2, \ell_2)\rangle$ Применить обратное преобразование Фурье к двум первым регистрам
5. $\rightarrow (\widetilde{s\ell_2/r}, \widetilde{\ell_2/r})$ Измерить два первых регистра
6. $\rightarrow s$ Применить обобщенный алгоритм цепных дробей

Опять основным является шаг 3, на котором вводится состояние

$$|\hat{f}(\ell_1, \ell_2)\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{-2\pi i \ell_2 j / r} |f(0, j)\rangle, \quad (5.70)$$

являющееся преобразованием Фурье от $|f(x_1, x_2)\rangle$ (см. упр. 5.22). В этом равенстве значения ℓ_1 и ℓ_2 должны удовлетворять условию

$$\sum_{k=0}^{r-1} e^{2\pi i k (\ell_1/s - \ell_2) / r} = r. \quad (5.71)$$

Иными словами, амплитуда $|\hat{f}(\ell_1, \ell_2)\rangle$ близка к нулю. Обобщенное разложение в цепную дробь, используемое на последнем шаге для нахождения s , аналогично процедурам из подразд. 5.3.1; его построение оставим читателю в качестве простого упражнения.

Упражнение 5.22. Покажите, что

$$|\hat{f}(\ell_1, \ell_2)\rangle = \sum_{x_1=0}^{r-1} \sum_{x_2=0}^{r-1} e^{-2\pi i (\ell_1 x_1 + \ell_2 x_2) / r} |f(x_1, x_2)\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{-2\pi i \ell_2 j / r} |f(0, j)\rangle, \quad (5.72)$$

и что это выражение отлично от нуля только тогда, когда $\ell_1/s - \ell_2$ — целое число, делящееся на r .

Упражнение 5.23. Вычислите

$$\frac{1}{r} \sum_{\ell_1=0}^{r-1} \sum_{\ell_2=0}^{r-1} e^{-2\pi i (\ell_1 x_1 + \ell_2 x_2)/r} |\hat{f}(\ell_1, \ell_2)\rangle \quad (5.73)$$

с использованием (5.70) и покажите, что ответ равен $f(x_1, x_2)$.

Упражнение 5.24. Разработайте алгоритм обобщенных цепных дробей, используемый на шаге 6 алгоритма дискретного логарифмирования для восстановления s по приближенным значениям для $s\ell_2/r$ и ℓ_2/r .

Упражнение 5.25. Постройте квантовую схему, реализующую черный ящик U , используемый в квантовом алгоритме дискретного логарифмирования: этот оператор зависит от параметров a и b , и он выполняет унитарное преобразование $|x_1\rangle|x_2\rangle|y\rangle \rightarrow |x_1\rangle|x_2\rangle|y \oplus b^{x_1}a^{x_2}\rangle$. Сколько элементарных операций для этого нужно?

5.4.3 Задача о скрытой подгруппе

Теперь общий принцип должен быть ясен: если дана периодическая функция (при этом периодичность может быть достаточно сложной), то часто можно воспользоваться квантовым алгоритмом для эффективного нахождения периода. Важно, однако, отметить, что *не все* периоды могут быть найдены. Задача, являющаяся широким обобщением всех задач такого рода, может быть коротко сформулирована в терминах теории групп (см. краткий обзор в Приложении 2) следующим образом:

Пусть f — функция из конечно порожденной группы G в конечное множество X , постоянная на смежных классах по некоторой подгруппе K и принимающая различные значения на разных смежных классах. Пусть дан квантовый черный ящик, выполняющий унитарное преобразование $U|g\rangle|h\rangle = |g\rangle|h \oplus f(g)\rangle$, где $g \in G$, $h \in H$ и \oplus — некоторая подходящая бинарная операция на X . Найти множество образующих группы K .

Задача нахождения порядка и периода, дискретное логарифмирование и многие другие задачи — частные случаи этой задачи, называемой *задачей о скрытой подгруппе*; некоторые другие интересные частные случаи представлены на рис. 5.5.

Если G — *конечная абелева группа*, то квантовый компьютер может решить задачу о скрытой подгруппе за полиномиальное по $\log |G|$ количество операций, воспользовавшись одним обращением к черному ящику, с помощью алгоритма, очень похожего на другие алгоритмы, рассматриваемые в этом разделе. (На самом деле аналогичный метод работает и для конечно порожденных абелевых групп, но мы ограничимся конечным случаем.) Предложим читателю подробно описать алгоритм в качестве упражнения: после объяснения основной идеи,

сделать это будет легко³. Многие детали в нашем алгоритме практически не будут отличаться от предыдущих алгоритмов, поскольку конечные абелевы группы изоморфны произведениям аддитивных групп остатков. Это означает, что определено квантовое преобразование Фурье функции f на группе G (см. разд. A2.3) и это преобразование по-прежнему может быть выполнено эффективно. Первый нетривиальный шаг алгоритма — провести преобразование Фурье (обобщающее операцию Адамара) и создать суперпозицию по элементам группы; затем с помощью черного ящика для f это состояние преобразуется в следующее:

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |f(g)\rangle. \quad (5.74)$$

Как и раньше, теперь наша цель — переписать $|f(g)\rangle$ в базисе Фурье. Начнем с того, что напишем формулу

$$|f(g)\rangle = \frac{1}{\sqrt{|G|}} \sum_{\ell=0}^{|G|-1} e^{2\pi i \ell g / |G|} |\hat{f}(\ell)\rangle, \quad (5.75)$$

где $\exp(-2\pi i \ell g / |G|)$ — значение в точке $g \in G$ представления (см. упр. A2.13) группы G , под номером ℓ (преобразование Фурье переводит функции на группе в функции на множестве ее неприводимых представлений — см. упр. A2.23). Теперь заметим, что это выражение можно упростить, поскольку f постоянна на смежных классах и принимает на разных классах разные значения; получим, что

$$|\hat{f}(\ell)\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} e^{-2\pi i \ell g / |G|} |f(g)\rangle \quad (5.76)$$

имеет амплитуду, близкую к нулю, для всех ℓ , кроме тех, которые удовлетворяют условию

$$\sum_{h \in K} e^{-2\pi i \ell h / |G|} = |K|. \quad (5.77)$$

Если можно определить ℓ , то с помощью линейных ограничений, налагаемых этим условием, можно найти элементы группы K , а так как K абелева, это позволит в конечном счете найти множество образующих для всей скрытой подгруппы, т. е. решить нашу задачу.

Жизнь, однако, не столь проста. Важной причиной этого, почему эффективны алгоритмы нахождения порядка и дискретного логарифмирования, является то обстоятельство, что возможно применение цепных дробей для восстановления ℓ из $\ell / |G|$. Эти задачи таковы, что с высокой вероятностью ℓ и $|G|$ будут взаимно просты. В общем случае, однако, это не обязательно быть верным: $|G|$ может быть составным числом со многими делителями, и у нас нет никакой информации априори относительно ℓ .

³ Читатель должен иметь в виду, что изложение в этом разделе крайне неформально — *Прим. ред.*

Название	G	X	K	Функция
Задача Дойча	$\{0, 1\}, \oplus$	$\{0, 1\}$	$\{0\}$ или $\{0, 1\}$	$K = \{0, 1\} : \begin{cases} f(x) = 0 \\ f(x) = 1 \end{cases}$ $K = \{0\} : \begin{cases} f(x) = x \\ f(x) = 1 - x \end{cases}$
Задача Саймона	$\{0, 1\}^n, \oplus$	Произвольное конечное множество	$\{0, s\}$ $s \in \{0, 1\}^n$	$f(x \oplus s) = f(x)$
Нахождение периода	$\mathbf{Z}, +$	Произвольное конечное множество	$\{0, r, 2r, \dots\}$ $r \in G$	$f(x + r) = f(x)$
Нахождение порядка	$\mathbf{Z}, +$	$\{a^j\}$ $j \in \mathbf{Z}_r$ $a^r = 1$	$\{0, r, 2r, \dots\}$ $r \in G$	$f(x) = a^x$ $f(x + r) = f(x)$
Дискретный логарифм	$\mathbf{Z}_r \times \mathbf{Z}_r$ + (mod r)	$\{a^j\}$ $j \in \mathbf{Z}_r$ $a^r = 1$	$(\ell, -\ell s)$ $\ell, s \in \mathbf{Z}_r$	$f(x_1, x_2) = a^{kx_1+x_2}$ $f(x_1 + \ell, x_2 - \ell s)$ $= f(x_1, x_2)$
Порядок перестановки	$\mathbf{Z}_{2^m} \times \mathbf{Z}_{2^n}$ + (mod 2^m)	\mathbf{Z}_{2^n}	$\{0, r, 2r, \dots\}$ $r \in X$	$f(x, y) = \pi^x(y)$ $f(x + r, y) = f(x, y)$ $\pi = \text{перестановка множества } X$
Скрытая линейная функция	$\mathbf{Z} \times \mathbf{Z}, +$	\mathbf{Z}_N	$(\ell, -\ell s)$ $\ell, s \in X$	$f(x_1, x_2)$ $= \pi(sx_1 + x_2 \bmod N)$ $\pi = \text{перестановка множества } X$
Абелев стабилизатор	(H, X) $H = \text{произвольная абелева группа}$	Произвольное конечное множество	$\{s \in H \mid f(s, x) = x, \forall x \in X\}$	$f(gh, x) = f(g, f(h, x))$ $f(gs, x) = f(g, x)$

Рис. 5.5. Частные случаи задачи о скрытой подгруппе. Функция f отображает группу G в конечное множество X ; известно, что она постоянна на смежных классах по подгруппе $K \subseteq G$. В этой таблице \mathbf{Z}_N обозначает множество $\{0, 1, \dots, N - 1\}$, а \mathbf{Z} — множество целых чисел. Задача состоит в том, чтобы найти подгруппу K (или ее множество образующих), если задан черный ящик для f .

Однако эта проблема разрешима: как отмечалось выше, всякая конечная абелева группа является произведением циклических групп, порядки которых являются степенями простых чисел, т. е. $G = \mathbf{Z}_{p_1} \times \mathbf{Z}_{p_2} \times \dots \times \mathbf{Z}_{p_M}$, где p_i — степени простых чисел, а \mathbf{Z}_{p_i} — группа, состоящая из элементов $\{0, 1, \dots, p_i - 1\}$ с групповой операцией — сложением по модулю p_i . Тогда можно переписать фазу из формулы (5.75) в виде

$$e^{2\pi i \ell g / |G|} = \prod_{i=1}^M e^{2\pi i \ell'_i g_i / p_i}, \quad (5.78)$$

где $g_i \in \mathbf{Z}_{p_i}$. Определение собственного числа дает ℓ'_i , исходя из этого можно найти ℓ , а тем самым и элемент подгруппы K , как было описано выше, т. е. решить задачу о скрытой подгруппе.

Упражнение 5.26. Пусть K является такой подгруппой в G , для которой разложение G в произведение циклических групп индуцирует аналогичное разложение и для K . С помощью формулы (5.77) покажите, что определив ℓ'_i , можно найти элемент из соответствующей циклической подгруппы $K_{p_i} \subseteq K$.

Упражнение 5.27. Конечно, разложение произвольной конечной абелевой группы G на произведение циклических групп, порядки которых равны степеням простых чисел, является трудной задачей (не менее трудной, чем, например, факторизация). Но и здесь квантовые алгоритмы приходят на помощь: покажите, как с помощью алгоритмов этой главы можно эффективно найти разложение группы G .

Упражнение 5.28. Выпишите подробное описание квантового алгоритма, решающего задачу о скрытой подгруппе для конечных абелевых групп; оцените время работы и вероятность успеха.

Упражнение 5.29. Постройте квантовые алгоритмы, решающие задачи Дойча и Саймона из таблицы на рис. 5.5, руководствуясь решением задачи о скрытой подгруппе.

5.4.4 Возможны ли другие квантовые алгоритмы?

Один из наиболее интересных аспектов задачи о скрытой подгруппе состоит в том, что возможно решение и более сложных задач путем рассмотрения различных групп G и функции f . Мы описали решение задачи только для абелевых групп. Как обстоят дела с *неабелевыми* группами, которые довольно интересны (см. Приложение 2 по поводу преобразования Фурье на неабелевых группах)? Например, задача об *изоморфизме графов* состоит в том, станут ли два данных графа одинаковыми после какой-нибудь из перестановок вершин (см. подразд. 3.2.3). Эти перестановки можно рассматривать как элементы симметрической группы S_n , и существуют алгоритмы для вычисления быстрого преобразования Фурье на таких группах. Однако квантовый алгоритм, эффективно решający задачу об изоморфизме графов, пока неизвестен.

Хотя квантовые алгоритмы для решения более общих случаев задачи о скрытой подгруппе пока не найдены, полезным оказывается уже наличие общего подхода, поскольку он позволяет ставить вопросы о том, как выйти за его пределы. Слабо верится, что все быстрые квантовые алгоритмы, которые будут когда-либо открыты, окажутся лишь частными случаями решения задачи о скрытой подгруппе. Если считать, что решение задачи о скрытой подгруппе основано на инвариантности преобразования Фурье, то, возможно, в поисках новых алгоритмов стоило бы исследовать другие преобразования, обладающие другими свойствами инвариантности. Рассуждая в ином направлении, можно спросить: какие трудные задачи о скрытой подгруппе можно решить, если разрешается воспользоваться некоторым произвольным (но заданным независимо от задачи) квантовым состоянием? В конце концов в гл. 4 мы выяснили, что большинство квантовых состояний обладает тем свойством, что построить их — экспоненциально трудная задача. Такое состояние могло бы стать полезным ресурсом (воистину «квантовым оракулом»!), если бы существовали квантовые алгоритмы, которые могли его использовать для решения трудных задач.

Задача о скрытой подгруппе демонстрирует также важное ограничение, за пределы которого квантовые алгоритмы, дающие экспоненциальное ускорение по сравнению со своими (известными на данный момент) классическими аналогами, не выходят: эта задача имеет следующий вид: «нам заранее известно, что $F(X)$ обладает таким-то свойством; охарактеризуйте его». Возможно, это звучит разочаровывающе, но в конце следующей главы мы покажем, что при решении задач без таких дополнительных условий квантовые компьютеры *не могут* дать экспоненциального ускорения по сравнению с классическими; лучшее возможное ускорение полиномиально⁴. В то же время, это обстоятельство указывает, для задач какого рода квантовые компьютеры могут быть полезны: задним числом оказывается, что задача о скрытой подгруппе — естественный кандидат на применение квантовых вычислений. А какие еще имеются естественные задачи такого рода? Подумайте!

Задача 5.1. Постройте квантовую схему, вычисляющую квантовое преобразование Фурье

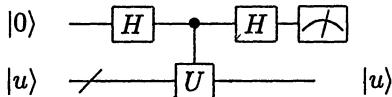
$$|j\rangle \longrightarrow \frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} e^{2\pi i j k / p} |k\rangle, \quad (5.79)$$

где p — простое число.

Задача 5.2 (измеряемое квантовое преобразование Фурье). Предположим, что квантовое преобразование Фурье производится на последнем шаге квантового вычисления, а затем выполняется измерение в вычислительном базисе. Покажите, что эту комбинацию квантового преобразования Фурье и измерения можно реализовать с помощью схемы, состоящей только из однокубитовых элементов и измерителей, с классическими условными операциями. (Используйте результаты обсуждения в разд. 4.4.)

⁴ Здесь имеются в виду только алгоритмы, применимые к функциям, заданным оракулами (или черными ящиками) — Прим. ред.

Задача 5.3 (алгоритм Китаева). Рассмотрим квантовую схему



здесь $|u\rangle$ — собственный вектор оператора U с собственным числом $e^{2\pi i\varphi}$. Покажите, что верхний кубит дает при измерении $|0\rangle$ с вероятностью $p \equiv \cos^2(\pi\varphi)$. Поскольку состояние $|u\rangle$ не меняется в результате работы схемы, им можно воспользоваться повторно; покажите, что если заменить U на U^k , где k — подходящее целое число, то, повторяя это вычисление нужное число раз, можно найти с произвольной точностью p , а значит и φ . Это — еще один способ определения собственного числа.

Задача 5.4. Приведенная нами оценка $O(L^3)$ для трудоемкости алгоритма факторизации не является точной. Покажите, что можно осуществить факторизацию за $O(L^2 \log L \log \log L)$ операций.

Задача 5.5 (неабелева задача о скрытой подгруппе (для исследования)). Пусть f — функция из конечной группы G в произвольное конечное множество X , о которой известно, что она постоянна на левых смежных классах по некоторой подгруппе $K \subseteq G$, причем на разных смежных классах она принимает разные значения. Начните с состояния

$$\frac{1}{\sqrt{|G|^m}} \sum_{g_1, \dots, g_m} |g_1, \dots, g_m\rangle |f(g_1), \dots, f(g_m)\rangle \quad (5.80)$$

и покажите, что при $m = 4 \log |G| + 2$ подгруппа K может быть однозначно восстановлена с вероятностью, не меньшей $1 - 1/|G|$. Обратите внимание на то, что G не предполагается абелевой и не имеется в виду проводить преобразование Фурье.

Этот результат показывает, что, используя $O(\log |G|)$ обращений к оракулу, можно получить результат, в котором чистые состояния, соответствующие различным возможным скрытым подгруппам, почти ортогональны. Тем не менее неизвестно, существует ли POVM, позволяющий найти скрытую подгруппу эффективно (т. е. за $\text{poly}(\log |G|)$ операций) исходя из этого конечного состояния.

Задача 5.6 (сложение с помощью преобразования Фурье). Пусть требуется построить квантовую схему, выполняющую вычисление $|x\rangle \rightarrow |x+y \bmod 2^n\rangle$, где y — фиксированная константа и $0 \leq x < 2^n$. Покажите, что при $y = 1$ это можно эффективно сделать следующим образом: провести квантовое преобразование Фурье, применить однокубитовые сдвиги фазы, а затем выполнить обратное преобразование Фурье. Для каких еще значений y такой метод эффективен? Сколько при этом требуется операций?

Краткое содержание главы

- При $N = 2^n$ квантовое преобразование Фурье

$$|j\rangle = |j_1, \dots, j_n\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i \frac{jk}{N}} |k\rangle \quad (5.81)$$

может быть записано в виде

$$\begin{aligned} |j\rangle &\rightarrow \frac{1}{2^{n/2}} (|0\rangle + e^{2\pi i 0 \cdot j_n} |1\rangle) (|0\rangle + e^{2\pi i 0 \cdot j_{n-1} j_n} |1\rangle) \dots \\ &\quad \times (|0\rangle + e^{2\pi i 0 \cdot j_1 j_2 \dots j_n} |1\rangle) \end{aligned} \quad (5.82)$$

и реализовано с помощью $\Theta(n^2)$ элементов.

- **Определение собственного числа.** Пусть $|u\rangle$ — собственный вектор оператора U с собственным числом $e^{2\pi i \varphi}$. Процедура определения собственного числа (см. рис. 5.3), начиная с состояния $|0\rangle^{\otimes t}|u\rangle$, может эффективно найти состояние $|\tilde{\varphi}\rangle|u\rangle$, где $\tilde{\varphi}$ с вероятностью не менее $(1 - \varepsilon)$ аппроксимирует φ с точностью $2^{-t + \lceil \log(2 + \frac{1}{2\varepsilon}) \rceil}$; все это верно в предположении, что возможно эффективно реализовывать оператор U^{2^k} для целых k .
- **Нахождение порядка.** Порядок числа x по модулю N — это наименьшее целое положительное число r , для которого $x^r \bmod N = 1$. Это число можно найти за $O(L^3)$ операций с помощью квантовой процедуры определения собственного числа, если x и N — L -битовые целые числа.
- **Факторизация:** Простые сомножители L -битового целого числа N могут быть найдены за $O(L^3)$ операций путем сведения этой задачи к нахождению порядка случайного числа x , взаимно простого с N .
- **Задача о скрытой подгруппе:** Все известные быстрые квантовые алгоритмы можно рассматривать как частные случаи следующей задачи. Пусть f — функция из конечно порожденной группы G в конечное множество X , обладающая тем свойством, что она постоянна на смежных классах по некоторой подгруппе $K \subset G$ и принимает разные значения на разных смежных классах. Дан квантовый черный ящик, выполняющий унитарное преобразование $U|g\rangle|h\rangle = |g\rangle|h \oplus f(g)\rangle$, где $g \in G$, $h \in X$. Найдите множество образующих для K .

История и дополнительная литература

Можно дать более общее определение преобразования Фурье, чем то, которым мы пользовались в этой главе. Общее преобразование Фурье определено на множестве последовательностей комплексных чисел $\{\alpha_g\}$, где индекс g пробегает элементы некоторой группы G . В этой главе в качестве G выступала аддитивная группа целых чисел по модулю 2^n , часто обозначаемая через Z_{2^n} . Дойч [117] показал, что на квантовом компьютере можно эффективно реализовать преобразование Фурье на группе Z_2^n — это не что иное, как преобразование Адамара. Шор [354] сделал важное открытие: для некоторых специальных значений m на квантовых компьютерах можно эффективно выполнить преобразование Фурье на группе Z_m . Вдохновленные этим результатом, Копперсмит [100], Дойч (не опубликовано) и Клив (не опубликовано) построили простые квантовые схемы для вычисления квантового преобразования Фурье на Z_2^n , которыми мы воспользовались в этой главе. Клив, Экерт, Макиавелло и Моска [80], также Гриффитс и Ниу [163] независимо открыли формулу произведения (5.4); следует отметить, что этот результат был гораздо раньше известен Даниэльсону и Ланцшу. Упрощенное доказательство, начинаяющееся с формулы (5.5), было предложено Зоу. Гриффитсу и Ниу [163] принадлежит измеряемое преобразование Фурье из задачи 5.2.

Преобразование Фурье на Z_{2^n} было обобщено до преобразования Фурье на произвольной конечной абелевой группе Китаевым [211]; он также предложил процедуру определения собственного числа в виде, изложенном в задаче 5.3. Клив, Экерт, Макиавелло и Моска [80] объединили некоторые элементы техники Шора и Китаева в изящную картину, на которой основан разд. 5.2. Подробное описание процедуры определения собственного числа можно найти в диссертации Моски [294].

Шор предложил квантовый алгоритм нахождения порядка в основополагающей работе 1994 г. [354] и заметил, что задачи факторизации и дискретного логарифмирования можно свести к нахождению порядка. Заключительная статья, содержащая подробное обсуждение и библиографию, была опубликована в 1997 г. [357]. В этой статье содержится также обсуждение остроумных алгоритмов умножения, с помощью которых алгоритм Шора можно сделать более быстрым, чем в нашем изложении, где умножение проводилось довольно простыми методами. При использовании этих ускоренных методов умножения трудоемкость разложения n -битового числа равна $O(n^2 \log n \log \log n)$, как и было отмечено во введении к главе. В 1995 г. Китаев [211] разработал алгоритм для нахождения стабилизатора общей абелевой группы и показал, что его частными случаями являются задачи о дискретном логарифме и факторизации. Кроме того, алгоритм Китаева содержал ряд идей, отсутствовавших у Шора. Описание алгоритма факторизации сделли Экерт и Йожа [139]; см. также Ди Винченцо [123]. Обсуждение цепных дробей основано на гл. 10 книги Харди и Райта [195]. Во время работы над книгой наиболее эффективным клас-

сическим алгоритмом факторизации был метод теоретико-числового решета. Он описан в сборнике под редакцией А. К.Ленстры и Х. У. Ленстры (мл.) [250].

Обобщение квантовых алгоритмов для решения задачи о скрытой подгруппе рассматривалось многими авторами. Исторически Саймон был первым, кто заметил, что квантовый компьютер может найти скрытый период функции, удовлетворяющей условию $f(x \oplus s) = f(x)$ [359, 360]. В действительности Шор сделал свое открытие, обобщив результат Саймона и применив преобразование Фурье на Z_N вместо использовавшихся Саймоном преобразований Адамара (преобразования Фурье на Z_2^k). Затем Боне и Липтон обнаружили связь с задачей о скрытой подгруппе и описали квантовый алгоритм, решающий задачу о скрытой линейной функции [61]. Йожа был первым, кто дал унифицированное описание алгоритмов Дойча–Йожи, Саймона и Шора в терминах задачи о скрытой подгруппе. Работа Экерта и Йожи пояснила роль абелева и неабелева быстрых преобразований Фурье в ускорении квантовых алгоритмов [140]. Наше описание задачи о скрытой подгруппе в разд. 5.4 соответствует работе Москки и Эккера [279, 294]. Клив показал, что задача нахождения порядка перестановки нуждается в экспоненциальном количестве запросов при ее решении на классическом вероятностном компьютере с ограниченными ошибками [91]. Попытки обобщить метод решения задачи о скрытой подгруппе за пределы абелевых групп были предприняты Эттингером и Хёйером [136], Рётелером и Бетом [337], Пюшлем, Рётелером и Бетом [326], Билзом, который также описал конструкцию квантового преобразования Фурье на симметрической группе [25], а также Эттингером, Хёйером и Книллом [137]. На данный момент эти результаты показывают, что *существует* квантовый алгоритм, решающий неабелеву задачу о скрытой подгруппе с использованием $O(\log |G|)$ обращений к оракулу, но неизвестно, можно ли его реализовать за полиномиальное время.

Глава 6

КВАНТОВЫЕ АЛГОРИТМЫ ПОИСКА

Представьте, что у вас есть карта с большим количеством городов, а вы хотите найти кратчайший маршрут, проходящий через все эти города. Простой алгоритм заключается в переборе всех возможных путей, проходящих через все города, и сравнении каждого из них с кратчайшим из уже рассмотренных путей. Если имеется N возможных маршрутов, то с помощью классического компьютера, очевидно, кратчайший можно найти таким методом за $O(N)$ операций. В высшей степени удивительно, что существует *квантовый алгоритм поиска*, называемый иногда *алгоритмом Гровера*, который позволяет существенно ускорить этот метод поиска — до $O(\sqrt{N})$ операций. Более того, квантовый алгоритм поиска является *общим* в том смысле, что может быть применен не только для поиска кратчайшего пути, но и для ускорения многих (хотя и не всех) классических алгоритмов, использующих перебор.

В этой главе рассматривается квантовый алгоритм поиска. Основной алгоритм изложен в разд. 6.1. В разд. 6.2 мы выведем алгоритм другим способом — с использованием алгоритма моделирования квантовой системы, описанного в разд. 4.7. Также будут описаны три важных применения этого алгоритма: квантовое перечисление (разд. 6.3), ускорение решения **NP**-полных задач (разд. 6.4) и поиск по неструктурированной базе данных (разд. 6.5). Априори можно было бы надеяться на дальнейшее улучшение квантового алгоритма поиска, чтобы он работал быстрее, чем за $O(\sqrt{N})$ операций, но, как мы покажем в разд. 6.6, это невозможно. В разд. 6.7 будет доказано, что данный предел быстродействия относится к большинству неструктурированных задач.

6.1 Квантовый алгоритм поиска

Начнем с формулирования схемы алгоритма поиска в терминах *оракула* — по аналогии с подразд. 3.1.1. Это позволит провести общее описание процедуры поиска и геометрического способа визуализации ее действия, а также увидеть, как она выполняется.

6.1.1 Оракул

Допустим, мы хотим провести поиск в пространстве поиска из N элементов. Вместо того чтобы искать непосредственно среди элементов, сосредоточимся на *номерах* этих элементов, т. е. числах в диапазоне от 0 до ($N - 1$). Для удобства будем считать, что $N = 2^n$, поэтому номер можно хранить в ячейке

из n бит, и что задача поиска имеет ровно M решений, где $1 \leq M \leq N$. Задачу поиска удобно представлять функцией f , аргументом которой является целое число x в диапазоне от 0 до $(N - 1)$. По определению, $f(x) = 1$, если x является решением задачи поиска, $f(x) = 0$ в противном случае.

Будем считать, что имеется квантовый *оракул* — черный ящик, внутреннее устройство которого мы обсудим позже (впрочем, на данной стадии это нас не интересует), — он может *распознавать* решения задачи поиска. Сигнал распознавания подается с помощью *кубита оракула*. Точнее говоря, оракул представляет собой унитарный оператор O , определенный действием на вычислительный базис следующим образом:

$$|x\rangle|q\rangle \xrightarrow{O} |x\rangle|q \oplus f(x)\rangle, \quad (6.1)$$

где $|x\rangle$ — индексный регистр, символом « \oplus » обозначено сложение по модулю 2, а кубит оракула $|q\rangle$ меняет значение, если $f(x) = 1$, и сохраняет его в противном случае. Можно проверить, является ли x решением нашей задачи поиска, приготовив состояние $|x\rangle|0\rangle$, подействовав на него оракулом и проверив, перешел ли кубит оракула в состояние $|1\rangle$.

В квантовом алгоритме поиска полезно применять оракул к кубиту оракула, находящемуся изначально в состоянии $(|0\rangle - |1\rangle)/\sqrt{2}$, как это сделано в алгоритме Дойча–Йожа (см. подразд. 1.4.4). Если x не является решением задачи поиска, действие оракула на состояние $|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$ не изменит последнее. В то же время, если x — решение задачи поиска, то состояния $|0\rangle$ и $|1\rangle$ в результате применения оракула перейдут друг в друга, и конечное состояние будет иметь вид $-|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$. Таким образом, действие оракула можно представить следующим выражением:

$$|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \xrightarrow{O} (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right). \quad (6.2)$$

Обратите внимание на то, что состояние кубита оракула не меняется. Оказывается, оно остается равным $(|0\rangle - |1\rangle)/\sqrt{2}$ на протяжении всей работы квантового алгоритма поиска, следовательно, в дальнейшем обсуждении алгоритма его можно не учитывать, что несколько упростит наше описание.

С учетом этого соглашения запишем действие оракула таким образом:

$$|x\rangle \xrightarrow{O} (-1)^{f(x)} |x\rangle. \quad (6.3)$$

Будем говорить, что оракул *помечает* решения задачи поиска, если он сдвигает фазу этих решений. Оказывается, для получения ответа в задаче поиска из N элементов с M решениями на квантовом компьютере необходимо применить оракул $O(\sqrt{N/M})$ раз.

Это обсуждение оракула без объяснения принципа его действия достаточно абстрактно и даже, возможно, загадочно. Создается впечатление, что оракул заранее *знает* ответ в задаче поиска; тогда непонятно, какой смысл в квантовом алгоритме поиска, основанном на сведениях, полученных от такого оракула. Ответ прост: существует разница между *нахождением* решения задачи

поиска и способностью *распознать* его; ключевой момент заключается в том, что бывают ситуации, в которых для распознавания решения не обязательно уметь его *находить*.

Простым примером, иллюстрирующим сказанное выше, является задача факторизации. Представьте себе, что имеется большое число m , о котором известно, что оно является произведением двух простых чисел p и q — схожая ситуация возникает при попытке взломать RSA-криптосистему с открытым ключом (см. Приложение 5). Очевидный путь для вычисления p и q на классическом компьютере заключается в *поиске* среди всех чисел от 2 до $m^{1/2}$ наименьшего из двух делителей числа m . Другими словами, мы должны попробовать последовательно разделить m на все числа в диапазоне от 2 до $m^{1/2}$, пока не найдем меньший из двух простых делителей числа m . Другой простой делитель после этого может быть получен делением числа m на найденный меньший делитель. Очевидно, что в алгоритме, основанном на поиске, для нахождения делителя на классическом компьютере требуется порядка $m^{1/2}$ операций деления.

С помощью квантового алгоритма поиска данный процесс можно ускорить. По определению, действие оракула на входном состоянии $|x\rangle$ заключается в делении с остатком числа m на x , проверке, равен ли остаток нулю, и изменении значения кубита оракула в этом случае. Применение квантового алгоритма поиска вместе с оракулом приводит к нахождению меньшего из двух простых делителей с большой вероятностью. Однако чтобы заставить указанный алгоритм работать, необходимо создать эффективную схему, реализующую этот оракул. Решение задачи представляет собой упражнение из области обратимых вычислений. Начнем с определения такой функции $f(x)$, что $f(x) \equiv 1$, когда x делит m , и $f(x) \equiv 0$ в противном случае; значение $f(x)$ показывает, удалось ли выполнить деление без остатка. Используя методы обратимых вычислений, обсуждавшиеся в подразд. 3.2.5, построим следующую классическую обратимую схему. Она переводит (X, q) (во входном регистре установлено значение X , в однокубитовом выходном регистре — q) в $(x, q \oplus f(x))$. Эта схема представляет собой простую модификацию обычной (необратимой) классической схемы для проверки делимости. Размер такой же (с точностью до умножения на двойку), как у классической необратимой схемы, поэтому упомянутые обе эти схемы примерно равнозначны. Кроме того, из классической обратимой схемы можно легко получить квантовую: она будет переводить состояние $|x\rangle|q\rangle$ в $|x\rangle|q \oplus f(x)\rangle$, как и требуется для оракула. Ключевой момент состоит в том, что *даже без нахождения простых делителей числа m можно построить в явном виде оракул, который распознает решение задачи поиска, когда оно ему предъявлено*. С помощью этого оракула и квантового алгоритма поиска можно провести поиск в диапазоне от 2 до $m^{1/2}$, используя $Q(m^{1/4})$ обращений к оракулу. Таким образом, необходимо выполнить пробное деление порядка $m^{1/4}$ раз вместо $m^{1/2}$ раз, как в случае использования классического алгоритма.

Разложение на простые множители — интересный умозрительный, но отнюдь не практический пример: существуют классические алгоритмы, которые работают гораздо быстрее, чем простой перебор всех возможных чисел с про-

веркой, являются ли они делителями числа m . Тем не менее он иллюстрирует общую идею применения квантового алгоритма поиска: классический алгоритм, использующий метод поиска, можно ускорить с помощью квантового поиска. Далее в этой главе мы исследуем сценарии, в которых квантовый алгоритм поиска является единственным инструментом для ускорения решения NP-полных задач.

6.1.2 Процедура

Схема действия алгоритма поиска показана на рис. 6.1. Алгоритм надлежащим образом использует одиночный n -кубитовый регистр. Детали внутреннего устройства оракула, включая возможную потребность в дополнительных рабочих кубитах, не являются важными для описания самого алгоритма. Цель алгоритма — найти решение задачи поиска с минимально возможным числом обращений к оракулу.

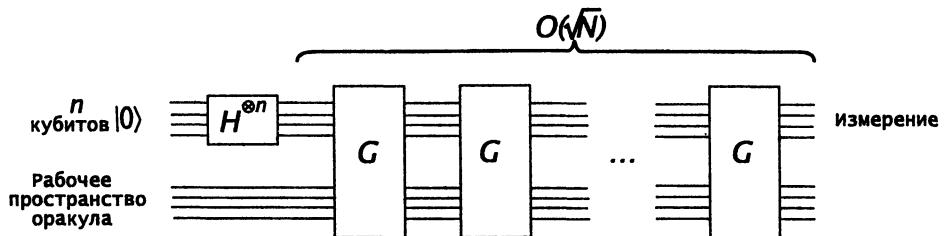


Рис. 6.1. Схема квантового алгоритма поиска. Оракул может использовать рабочие кубиты для своих целей, однако для анализа квантового алгоритма поиска рассматривается только n -кубитовый регистр

В начале алгоритма компьютер находится в состоянии $|0\rangle^{\otimes n}$. С помощью преобразования Адамара компьютер переводится в состояние

$$|\psi\rangle = \frac{1}{N^{1/2}} \sum_{x=0}^{N-1} |x\rangle. \quad (6.4)$$

Дальше в квантовом алгоритме поиска последовательно применяется квантовая подпрограмма, называемая *итерацией* (или *оператором*) Гровера (будем обозначать ее буквой « G »). Итерация Гровера, квантовая схема которой изображена на рис. 6.2, может быть разбита на четыре шага:

1. применение оракула O ,
2. применение преобразования Адамара $H^{\otimes n}$,
3. применение к регистру условного сдвига фазы — каждое состояние вычислительного базиса, за исключением $|0\rangle$, приобретает фазовый сдвиг -1 :

$$|x\rangle \rightarrow -(-1)^{\delta_{x0}} |x\rangle, \quad (6.5)$$

4. применение преобразования Адамара $H^{\otimes n}$.

Упражнение 6.1. Покажите, что унитарный оператор, соответствующий фазовому сдвигу в итерации Гровера, имеет вид $2|0\rangle\langle 0| - I$.

Каждая операция в итерации Гровера может быть эффективно реализована на квантовом компьютере. Шаги 2 и 4 (преобразования Адамара) требуют по $n = \log N$ операций каждый. Шаг 3 (условный фазовый сдвиг) может быть реализован с использованием методов, описанных в разд. 4.3, для этого необходимо $O(n)$ элементов. Затраты на обращение к оракулу зависят от конкретного приложения, а пока просто заметим, что при итерации Гровера требуется лишь одно обращение к оракулу. Заметим, что объединение шагов 2, 3 и 4 записывается следующим образом:

$$H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} = 2|\psi\rangle\langle\psi| - I, \quad (6.6)$$

где $|\psi\rangle$ — суперпозиция взятых с равными весами состояний (формула (6.4)). Таким образом, итерация Гровера G может быть записана в виде $G = (2|\psi\rangle\langle\psi| - I)O$.

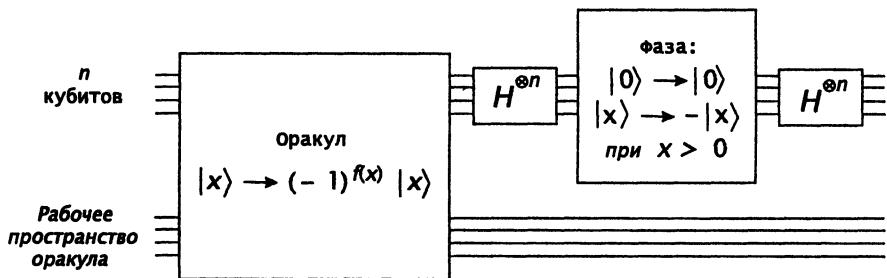


Рис. 6.2. Схема итерации Гровера G .

Упражнение 6.2. Покажите, что применение операции $(2|\psi\rangle\langle\psi| - I)$ к состоянию $\sum_k \alpha_k |k\rangle$ дает результат

$$\sum_k [-\alpha_k + 2\langle\alpha\rangle] |k\rangle, \quad (6.7)$$

где $\langle\alpha\rangle \equiv \sum_k \alpha_k / N$ — среднее значение α . Поэтому операцию $2|\psi\rangle\langle\psi| - I$ иногда называют *инверсией относительно среднего*.

6.1.3 Геометрическая интерпретация

Что делает итерация Гровера? Выше было указано, что $G = (2|\psi\rangle\langle\psi| - I)O$. Покажем, что итерацию Гровера можно рассматривать как *поворот* в двумерном пространстве, порождаемом начальным вектором $|\psi\rangle$ и состоянием, являющимся суперпозицией решений задачи поиска с равными весами. Убедимся

в этом. Введем обозначения \sum'_x для суммы по всем x , которые представляют собой решения задачи поиска, и \sum''_x для суммы по всем x , которые не являются решениями задачи поиска. Определим нормированные состояния следующим образом:

$$|\alpha\rangle \equiv \frac{1}{\sqrt{N-M}} \sum''_x |x\rangle, \quad (6.8)$$

$$|\beta\rangle \equiv \frac{1}{\sqrt{M}} \sum'_x |x\rangle. \quad (6.9)$$

Простые алгебраические вычисления показывают, что начальное состояние $|\psi\rangle$ можно переписать в виде

$$|\psi\rangle = \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle, \quad (6.10)$$

т. е. начальное состояние квантового компьютера лежит в пространстве, порожденном векторами $|\alpha\rangle$ и $|\beta\rangle$.

Действие оператора G можно представить себе следующим образом. Оракул O производит отражение относительно вектора $|\alpha\rangle$ в плоскости, задаваемой векторами $|\alpha\rangle$ и $|\beta\rangle$. Это означает, что $O(a|\alpha\rangle + b|\beta\rangle) = a|\alpha\rangle - b|\beta\rangle$. Аналогично, оператор $2|\psi\rangle\langle\psi| - I$ также производит отражение в плоскости, задаваемой векторами $|\alpha\rangle$ и $|\beta\rangle$, относительно вектора $|\psi\rangle$. А композиция двух отражений представляет собой поворот! Таким образом, для любого k состояние $G^k|\psi\rangle$ остается в пространстве, натянутом на векторы $|\alpha\rangle$ и $|\beta\rangle$. Отсюда можно получить угол поворота. Пусть $\cos(\theta/2) = \sqrt{(N-M)/N}$, так что $|\psi\rangle = \cos(\theta/2)|\alpha\rangle + \sin(\theta/2)|\beta\rangle$. Как показано на рис. 6.3, после выполнения двух отражений, композиция которых равна повороту G , вектор $|\psi\rangle$ переходит в

$$G|\psi\rangle = \cos \frac{3\theta}{2} |\alpha\rangle + \sin \frac{3\theta}{2} |\beta\rangle, \quad (6.11)$$

так что угол поворота действительно равен θ . Ясно, что после k -кратного применения оператора G состояние $|\psi\rangle$ переходит в следующее:

$$G^k|\psi\rangle = \cos \left(\frac{2k+1}{2}\theta \right) |\alpha\rangle + \sin \left(\frac{2k+1}{2}\theta \right) |\beta\rangle. \quad (6.12)$$

Таким образом, можно сказать, что G представляет собой поворот на угол θ в двумерном пространстве, натянутом на векторы $|\alpha\rangle$ и $|\beta\rangle$. Повторное применение итерации Гровера поворачивает вектор состояния еще ближе к вектору $|\beta\rangle$. Когда вектор $G^k|\psi\rangle$ будет достаточно близок к вектору $|\beta\rangle$, измерение в вычислительном базисе даст с высокой вероятностью одно из слагаемых, образующих вектор $|\beta\rangle$, т. е. решение задачи поиска! Пример, иллюстрирующий алгоритм поиска при $N = 4$, показан на вставке 6.1.

Упражнение 6.3. Покажите, что в базисе, состоящем из векторов $|\alpha\rangle$ и $|\beta\rangle$, итерацию Гровера можно записать следующим образом:

$$G = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}, \quad (6.13)$$

где θ — действительное число в диапазоне от 0 до $\pi/2$ (для простоты будем считать, что $M \leq N/2$; вскоре мы снимем это ограничение), выбранное таким образом, что

$$\sin \theta = \frac{2\sqrt{M(N-M)}}{N}. \quad (6.14)$$

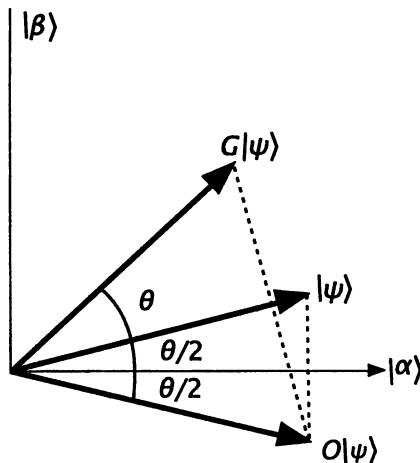


Рис. 6.3. Однократное действие итерации Гровера G вектор состояния поворачивается на угол θ в сторону суперпозиции $|\beta\rangle$ всех решений задачи поиска. В начальный момент вектор состояния отклонен на угол $\theta/2$ от вектора $|\alpha\rangle$ (состояния, ортогонального состоянию $|\beta\rangle$). Оракул O отражает состояние относительно вектора $|\alpha\rangle$, затем оператор $2|\psi\rangle\langle\psi| - I$ отражает его относительно вектора $|\psi\rangle$. Здесь векторы $|\alpha\rangle$ и $|\beta\rangle$ для наглядности изображены немного длиннее, чем должны быть (все векторы должны иметь единичную длину). После многократного применения итерации Гровера вектор состояния оказывается близко к вектору $|\beta\rangle$, после чего наблюдение в вычислительном базисе дает с большой вероятностью решение задачи поиска. Алгоритм обладает замечательной эффективностью, поскольку θ ведет себя как $\Omega(\sqrt{M/N})$, т. е. требуется порядка $O(\sqrt{N/M})$ итераций, чтобы повернуть вектор состояния в положение, близкое к вектору $|\beta\rangle$.

6.1.4 Эффективность

Какое количество итераций Гровера необходимо выполнить, чтобы повернуть вектор $|\psi\rangle$ близко к вектору $|\beta\rangle$? Начальное состояние системы задается вектором $|\psi\rangle = \sqrt{(N-M)/N}|\alpha\rangle + \sqrt{M/N}|\beta\rangle$, поэтому после поворота на угол $\arccos \sqrt{M/N}$ вектор состояния переходит в $|\beta\rangle$. Обозначим через $CI(x)$ целое число, ближайшее к действительному числу x ; будем считать, что половина всегда округляется в меньшую сторону, т. е. $CI(3.5) = 3$. Тогда, повторив итерацию Гровера

$$R = CI\left(\frac{\arccos \sqrt{M/N}}{\theta}\right) \quad (6.15)$$

раз, мы уменьшим угол между образом вектора $|\psi\rangle$ и вектором $|\beta\rangle$ до величины, меньшей $\theta/2$, причем $\theta/2 \leq \pi/4$. Измерение, проведенное над этим состоянием в вычислительном базисе, даст решение задачи поиска с вероятностью не менее $1/2$. На самом деле, для специально выбранных значений M и N можно достичь гораздо большей вероятности успеха. Например, когда $M \ll N$, получим $\theta \approx \sin \theta \approx 2\sqrt{M/N}$, т. е. отличие по углу на конечной стадии не превышает $\theta/2 \approx \sqrt{M/N}$, что приводит к вероятности ошибки, не превышающей M/N . Обратите внимание, что R зависит от числа решений M , а не от того, чему они равны, поэтому, если известно число M , можно применить описанным выше образом квантовый алгоритм поиска. В разд. 6.3 мы объясним, как применять алгоритм поиска даже при неизвестном значении M .

Выражение (6.15) полезно для точного определения числа вызовов оракула при квантовом поиске. Однако удобно было бы иметь более простое выражение, передающее в общих чертах поведение величины R . Предположим пока, что $M \leq N/2$, тогда

$$\frac{\theta}{2} \geq \sin \frac{\theta}{2} = \sqrt{\frac{M}{N}}, \quad (6.16)$$

откуда следует верхняя оценка числа итераций:

$$R \leq \left[\frac{\pi}{4} \sqrt{\frac{N}{M}} \right]. \quad (6.17)$$

Таким образом, чтобы получить решение задачи поиска с высокой вероятностью, необходимо выполнить $R = O(\sqrt{N/M})$ итераций Гровера (а следовательно, и обращений к оракулу); т. е. мы имеем квадратичное улучшение по сравнению с классической оценкой $O(N/M)$. Квантовый алгоритм поиска описывается ниже (рассмотрен случай $M = 1$).

Алгоритм: квантовый поиск

Вход: 1) черный ящик с оракулом O , который выполняет преобразование $O|x\rangle|q\rangle = |x\rangle|q \oplus f(x)\rangle$, где $f(x) = 0$ при $0 \leq x < 2^n$ за исключением $x = x_0$, для которого $f(x_0) = 1$; 2) $(n+1)$ кубит в состоянии $|0\rangle$.

Выход: x_0 .

Время выполнения: $O(\sqrt{2^n})$ операций. Вероятность успеха $O(1)$.

Процедура:

- | | |
|--|--|
| 1. $ 0\rangle^{\otimes n} 0\rangle$
2. $\rightarrow \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} x\rangle \left[\frac{ 0\rangle - 1\rangle}{\sqrt{2}} \right]$ | Начальное состояние

Применить $H^{\otimes n}$ к первым n кубитам и HX к последнему кубиту |
| 3. $\rightarrow [(2 \psi\rangle\langle\psi - I)O]^{\otimes R} \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} x\rangle \left[\frac{ 0\rangle - 1\rangle}{\sqrt{2}} \right]$
$\approx x_0\rangle \left[\frac{ 0\rangle - 1\rangle}{\sqrt{2}} \right]$ | Применить итерацию Гровера R примерно $[\pi\sqrt{2^n}/4]$ раз
Измерить первые n кубитов |
| 4. $\rightarrow x_0$ | |

Упражнение 6.4. Выпишите в явном виде шаги квантового алгоритма поиска, аналогичные приведенным выше, но для случая M решений ($1 < M < N/2$).

Что происходит, когда более половины элементов являются решениями задачи поиска, т. е. когда $M \geq N/2$? Из выражения $\theta = \arcsin(2\sqrt{M(N-M)}/N)$ (сравните с формулой (6.14)) можно заметить, что угол θ уменьшается, когда M меняется от $N/2$ до N . Из этого следует, что количество итераций в алгоритме поиска *растет* с увеличением M (при $M \geq N/2$). Интуитивно представляется, что это неподходящее свойство для алгоритма поиска: казалось бы, решения проще найти, когда их число растет. Существуют, по крайней мере, два способа обойти эту проблему. Если заранее известно, что M больше, чем $N/2$, то можно просто выбрать случайным образом элемент из пространства поиска, а затем с использованием оракула проверить, является ли он решением задачи поиска. Вероятность успеха такого подхода не менее половины, и требуется одно обращение к оракулу. Неудобство этого способа заключается в том, что мы можем не знать заранее величину M .

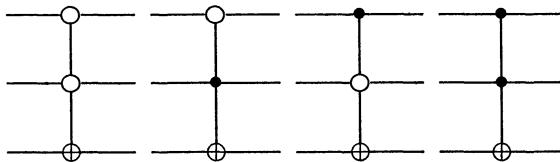
В том случае, когда неизвестно, выполняется ли условие $M \geq N/2$, можно использовать другой подход. Он интересен сам по себе, и для него существует полезное применение — он упрощает анализ квантового алгоритма для вычисления количества решений задачи поиска (см. разд. 6.3). Основная идея заключается в удвоении количества элементов в пространстве поиска путем добавления к пространству поиска N дополнительных элементов, ни один из которых не является решением. В результате в новом пространстве решениями будет являться менее половины элементов. Это осуществляется за счет добавления одного кубита $|q\rangle$ к переменной, нумерующей элементы пространства поиска, из-за чего количество элементов, среди которых ведется поиск, удваивается и становится равным $2N$. После этого строится новый *расширенный* оракул O' , который помечает элемент только в том случае, если он является решением задачи поиска, а дополнительный бит равен нулю. В упражнении 6.5 предлагается объяснить, как оракул O' может быть построен с использованием одного обращения к оракулу O . Для новой задачи поиска имеется только M решений из $2N$ элементов, и мы увидим, что при запуске алгоритма поиска с новым оракулом O' потребуется самое большое $R = (\pi/4)\sqrt{2N/M}$ обращений к оракулу O' , а, следовательно, для решения задачи поиска необходимо $O(\sqrt{N/M})$ обращений к оракулу O .

Упражнение 6.5. Покажите, что расширенный оракул O' может быть построен с помощью однократно использованного оракула O и применяемых к дополнительному кубиту $|q\rangle$ базисных квантовых элементов.

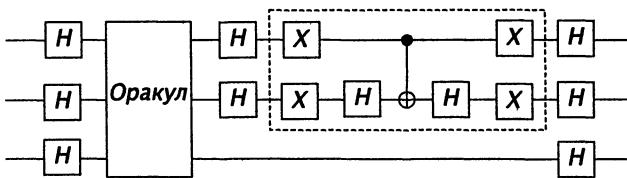
Квантовый алгоритм поиска имеет много применений, некоторые из них будут описаны в последующих разделах. Квантовый алгоритм поиска очень полезен, поскольку мы не делаем предположений о какой-либо конкретной структуре решаемой задачи поиска. В этом большое преимущество формулирования задачи в терминах оракула, представляющего собой черный ящик, и мы будем использовать этот подход везде, где это окажется удобным в оставшейся части

Вставка 6.1. Квантовый поиск: двухбитовый пример

Приведем пример, иллюстрирующий работу квантового алгоритма поиска на пространстве поиска с $N = 4$. Оракул, для которого $f(x) = 0$ при всех x , кроме такого $x = x_0$, что $f(x_0) = 1$, может задаваться одной из четырех схем



соответствующих $x_0 = 0, 1, 2, 3$ (слева направо), при этом два верхних кубита содержат запрос x , а нижний — ответ оракула. Квантовая схема, которая выполняет начальные преобразования Адамара и одну итерацию Гровера, имеет вид



В начальный момент два верхних кубита приготавливаются в состоянии $|0\rangle$, а нижний — в состоянии $|1\rangle$. Элементы, находящиеся внутри пунктирной рамки, выполняют операцию условного фазового сдвига $2|00\rangle\langle 00| - I$. Сколько раз следует повторить операцию G , чтобы получить x_0 ? Из уравнения (6.15), используя условие $M = 1$, найдем, что требуется меньше одной итерации. Это следует из того, что $\theta = \pi/3$, согласно формуле (6.14), и в этом особом случае необходима *точно одна* итерация, чтобы идеальным образом получить x_0 . Из рис. 6.3 видно, что вектор нашего начального состояния $|\psi\rangle = (|00\rangle + |01\rangle + |10\rangle + |11\rangle)/2$ отклонен на угол 30° от вектора $|\alpha\rangle$, и один поворот на угол 60° переводит $|\psi\rangle$ в $|\beta\rangle$. Вы можете самостоятельно (с использованием квантовых схем) непосредственно проверить тот факт, что измерение над двумя верхними кубитами дает результат x_0 (после однократного использования оракула). Напротив, с использованием классического компьютера (или классической схемы) попытка различить четыре состояния потребует в среднем 2,25 обращений к оракулу.

главы. В конкретных применениях, конечно, необходимо понимать, как именно устроен оракул, и в каждой из таких конкретных задач будет обсуждаться реализация используемого в ней оракула.

Упражнение 6.6. Проверьте, что элементы, заключенные в пунктирную рамку на нижнем рисунке вставки 6.1, выполняют операцию условного фазового сдвига $(2|00\rangle\langle 00| - I)$ (с точностью до несущественного общего фазового множителя).

6.2 Квантовый поиск как квантовое моделирование

Правильность квантового алгоритма поиска легко проверить, но неясно, как можно было бы придумать такой алгоритм «с нуля». В этом разделе мы ознакомим читателя с эвристическими средствами, с помощью которых можно «получить» квантовый алгоритм поиска, с тем чтобы у читателя выработался некий интуитивный подход, полезный в сложном деле построения квантовых алгоритмов. В качестве полезного побочного эффекта мы получим *детерминированный* квантовый алгоритм поиска. Поскольку цель состоит в приобретении интуиции, а не общности, для простоты предположим, что у задачи квантового поиска только одно решение x .

Предлагаемый метод состоит из двух шагов. Вначале необходимо угадать гамильтониан, который решает задачу. Точнее говоря, мы выписываем гамильтониан H , который так зависит от решения x и начального состояния $|\psi\rangle$, что квантовая система, эволюция которой описывается оператором H , перейдет из состояния $|\psi\rangle$ в $|x\rangle$ за некоторое заданное время. После нахождения такого гамильтониана и начального состояния можно перейти ко второму шагу, который заключается в попытке смоделировать действие гамильтониана с использованием квантовой схемы. Удивительно, но следуя этой процедуре, можно быстро получить квантовый алгоритм поиска! Мы уже встречались с этой процедурой из двух шагов, когда изучали универсальность в квантовых схемах (см. задачу 4.3), и она также хорошо помогает в изучении квантового поиска.

Предположим, что в начале выполнения алгоритма квантовый компьютер находится в состоянии $|\psi\rangle$. Позже мы укажем это состояние, однако сейчас удобно оставить его неопределенным, пока мы не поймем работу алгоритма. Задача квантового поиска состоит в переводе состояния $|\psi\rangle$ в $|x\rangle$ или в некоторое приближение к последнему. Какой гамильтониан следует выбрать, чтобы он задавал такую эволюцию? Исходя из требований простоты, хотелось бы построить гамильтониан, оперируя только терминами « $|\psi\rangle$ » и « $|x\rangle$ ». Таким образом, гамильтониан должен быть представлен суммой слагаемых вида $|\psi\rangle\langle\psi|$, $|x\rangle\langle x|$, $|\psi\rangle\langle x|$ и $|x\rangle\langle\psi|$. Вероятно, наиболее простыми гамильтонианами подобного типа являются следующие:

$$H = |x\rangle\langle x| + |\psi\rangle\langle\psi|, \quad (6.18)$$

$$H = |x\rangle\langle\psi| + |\psi\rangle\langle x|. \quad (6.19)$$

Оказывается, оба этих гамильтониана приводят к квантовому алгоритму поиска! Однако пока ограничимся изучением гамильтониана (6.18). Напомним (см. подразд. 2.2.2), что через время t состояние квантовой системы, эволюция которой описывается гамильтонианом H , а начальное состояние определялось вектором $|\psi\rangle$, имеет вид

$$\exp(-iHt)|\psi\rangle. \quad (6.20)$$

С интуитивной точки зрения все выглядит замечательно: для малых t эволюция заключается в переводе состояния $|\psi\rangle$ в $(I - itH)|\psi\rangle = (1 - it)|\psi\rangle - it\langle x|\psi\rangle|x\rangle$. Таким образом, вектор $|\psi\rangle$ слегка поворачивается в сторону вектора $|x\rangle$. Проведем полный анализ для того, чтобы определить, существует ли такое t , что $\exp(-iHt)|\psi\rangle = |x\rangle$. Очевидно, что можно ограничиться двумерным пространством, порожденным векторами $|x\rangle$ и $|\psi\rangle$. Выполняя процедуру Грама–Шмидта, можно найти такой вектор $|y\rangle$, что $|x\rangle$ и $|y\rangle$ образуют ортонормированный базис в этом пространстве и $|\psi\rangle = \alpha|x\rangle + \beta|y\rangle$ для некоторых α и β , удовлетворяющих условию $\alpha^2 + \beta^2 = 1$ (для удобства выберем фазы состояний $|x\rangle$ и $|y\rangle$ таким образом, чтобы числа α и β были действительными и неотрицательными). В базисе $|x\rangle$, $|y\rangle$ получим

$$H = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} \alpha^2 & \alpha\beta \\ \alpha\beta & \beta^2 \end{bmatrix} = \begin{bmatrix} 1 + \alpha^2 & \alpha\beta \\ \alpha\beta & 1 - \alpha^2 \end{bmatrix} = I + \alpha(\beta X + \alpha Z). \quad (6.21)$$

Таким образом, выполняется равенство

$$\exp(-iHt)|\psi\rangle = \exp(-it)[\cos(\alpha t)|\psi\rangle - i \sin(\alpha t)(\beta X + \alpha Z)|\psi\rangle]. \quad (6.22)$$

Можно не учитывать общий фазовый множитель $\exp(-it)$, тогда простые алгебраические вычисления показывают, что $(\beta X + \alpha Z)|\psi\rangle = |x\rangle$, поэтому состояние системы через время t можно представить вектором

$$\cos(\alpha t)|\psi\rangle - i \sin(\alpha t)|x\rangle. \quad (6.23)$$

Следовательно, измерение, выполненное над системой через время $t = \pi/2\alpha$, даст результат $|x\rangle$ с вероятностью единица: мы нашли решение задачи поиска! К сожалению, время наблюдения зависит от α , т. е. от компоненты вектора $|\psi\rangle$ в направлении $|x\rangle$, а значит от числа x , которое мы и хотим найти. Очевидное решение этой проблемы заключается в том, чтобы попытаться подобрать число α одинаковым для всех $|x\rangle$, т. е. сделать $|\psi\rangle$ однородной суперпозицией:

$$|\psi\rangle = \frac{\sum_x |x\rangle}{\sqrt{N}}. \quad (6.24)$$

Этот выбор приводит к величине $\alpha = 1/\sqrt{N}$, одинаковой для всех x , тогда время наблюдения составит $t = \pi\sqrt{N}/2$ вне зависимости от неизвестного заранее значения x . Кроме того, состояние (6.24) обладает тем очевидным преимуществом, что мы уже знаем, как его получить с использованием преобразования Адамара.

Теперь нам известно, что гамильтониан (6.18) описывает поворот вектора $|\psi\rangle$ в $|x\rangle$. Можем ли мы найти квантовую схему, моделирующую гамильтониан (6.18), и таким образом построить квантовый алгоритм поиска? Применяя метод, изложенный в разд. 4.7, можно видеть, что естественный способ

моделирования оператора H состоит в поочередном моделировании гамильтонианов $H_1 \equiv |x\rangle\langle x|$ и $H_2 \equiv |\psi\rangle\langle\psi|$ на короткие промежутки времени Δt . Эти гамильтонианы легко моделировать, используя методы, рассмотренные в гл. 4 (рис. 6.4 и 6.5).

Упражнение 6.7. Проверьте, что схемы, показанные на рис. 6.4 и 6.5, реализуют соответственно операции $\exp(-i|x\rangle\langle x|\Delta t)$ и $\exp(-i|\psi\rangle\langle\psi|\Delta t)$, где $|\psi\rangle$ определяется уравнением (6.24).

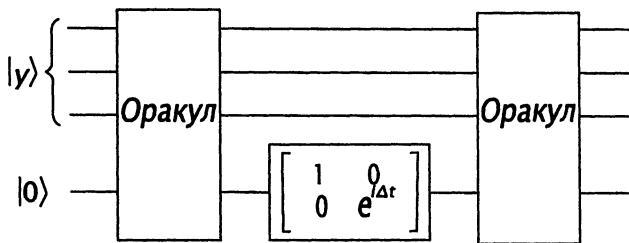


Рис. 6.4. Схема, реализующая операцию $\exp(-i|x\rangle\langle x|\Delta t)$ при помощи двух обращений к оракулу.

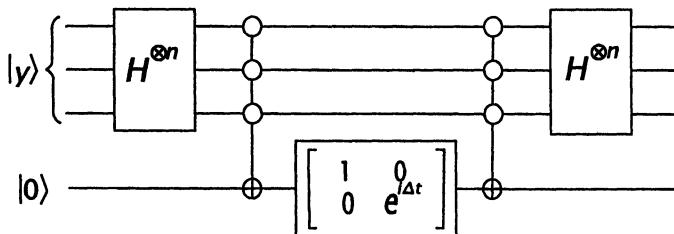


Рис. 6.5. Схема, реализующая операцию $\exp(-i|\psi\rangle\langle\psi|\Delta t)$ при помощи двух обращений к оракулу.

Число обращений к оракулу при квантовом моделировании определяется тем, насколько малый шаг по времени требуется для получения достаточно точных результатов. Предположим, мы используем шаг моделирования Δt , который дает точность $O(\Delta t^2)$. Полное количество необходимых шагов равно $t/\Delta t = \Theta(\sqrt{N}/\Delta t)$, а следовательно, накапливаемая ошибка составит $O(\Delta t^2 \times \sqrt{N}/\Delta t) = O(\Delta t \sqrt{N})$. Чтобы получить достаточно высокую вероятность успешного завершения алгоритма, необходимо, чтобы ошибка имела порядок $O(1)$, а это означает, что мы должны выбрать $\Delta t = \Theta(1/\sqrt{N})$, т. е. требуемое количество обращений к оратору равно $O(N)$ — не лучше, чем в классическом случае. Что, если попробовать воспользоваться более точным методом квантового моделирования, дающим, например, точность $O(\Delta t^3)$? Накапливаемая ошибка в этом случае составит $O(\Delta t^2 \sqrt{N})$, поэтому чтобы вероятность успешного завершения алгоритма была достаточно высока, необходимо выбрать $\Delta t = \Theta(N^{-1/4})$; тогда число обращений к оракулу имеет порядок

док $O(N^{3/4})$, что является существенным улучшением по сравнению с классическим случаем, хотя все еще не настолько хорошо, как было в квантовом алгоритме поиска в разд. 6.1! Обычно улучшение точности квантового моделирования приводит к уменьшению числа обращений к оракулу при моделировании (см. упражнение 6.8).

Упражнение 6.8. Предположим, что шаг моделирования выполняется с точностью $O(\Delta t^r)$. Покажите, что число обращений к оракулу при моделировании гамильтониана H с достаточной точностью имеет порядок $O(N^{r/2(r-1)})$. Обратите внимание, что r становится большим, когда показатель степени у N приближается к 1/2.

Мы исследовали точность квантового моделирования гамильтониана (6.18) с использованием общих результатов разд. 4.7, относящихся к квантовому моделированию. Конечно, в этом примере мы работаем с особым гамильтонианом, а не с общим случаем, поэтому было бы интересно непосредственно вычислить результат шага моделирования со временем Δt , а не полагаться на общий анализ. Это можно сделать для любого конкретного выбора метода моделирования — находить результат шага моделирования немного скучно, зато это вычисление является непосредственным. Очевидный начальный шаг — вычислить в явном виде действие моделирования в первом приближении, т. е. вычислить одно или оба из выражений $\exp(-i|x\rangle\langle x|\Delta t)\exp(-i|\psi\rangle\langle \psi|\Delta t)$ и $\exp(-i|\psi\rangle\langle \psi|\Delta t)\exp(-i|x\rangle\langle x|\Delta t)$. Результаты будут одинаковыми в обоих случаях; мы будем изучать оператор $U(\Delta t) \equiv \exp(-i|\psi\rangle\langle \psi|\Delta t)\exp(-i|x\rangle\langle x|\Delta t)$. Он действует нетривиальным образом только на пространство, порожданное операторами $|x\rangle\langle x|$ и $|\psi\rangle\langle \psi|$, поэтому ограничимся рассмотрением этого пространства, используя базис $|x\rangle$, $|y\rangle$, где $|y\rangle$ — вектор, определенный выше. Обратите внимание, что в этом представлении $|x\rangle\langle x| = (I + Z)/2 = (I + \hat{z} \cdot \vec{\sigma})/2$, где $\hat{z} \equiv (0, 0, 1)$ — единичный вектор в направлении оси z ; $|\psi\rangle\langle \psi| = (I + \vec{\psi} \cdot \vec{\sigma})/2$, где $\vec{\psi} \equiv (2\alpha\beta, 0, \alpha^2 - \beta^2)$ (напомним, что это векторное представление Блоха, см. разд. 4.2). Простое вычисление показывает, что с точностью до несущественного общего фазового множителя

$$U(\Delta t) = \left(\cos^2\left(\frac{\Delta t}{2}\right) - \sin^2\left(\frac{\Delta t}{2}\right) \vec{\psi} \cdot \hat{z} \right) I - 2i \sin\left(\frac{\Delta t}{2}\right) \left(\cos\left(\frac{\Delta t}{2}\right) \frac{\vec{\psi} + \hat{z}}{2} + \sin\left(\frac{\Delta t}{2}\right) \frac{\vec{\psi} \times \hat{z}}{2} \right) \cdot \vec{\sigma}. \quad (6.25)$$

Упражнение 6.9. Проверьте уравнение (6.25). (Указание: см. упр. 4.15.)

Уравнение (6.25) означает, что $U(\Delta t)$ — вращение на сфере Блоха вокруг оси \vec{r} , определяемой выражением

$$\vec{r} = \cos\left(\frac{\Delta t}{2}\right) \frac{\vec{\psi} + \hat{z}}{2} + \sin\left(\frac{\Delta t}{2}\right) \frac{\vec{\psi} \times \hat{z}}{2}, \quad (6.26)$$

на угол θ , задаваемый соотношением

$$\cos\left(\frac{\theta}{2}\right) = \cos^2\left(\frac{\Delta t}{2}\right) - \sin^2\left(\frac{\Delta t}{2}\right)\vec{\psi} \cdot \hat{z}, \quad (6.27)$$

которое при замене $\vec{\psi} \cdot \hat{z} = \alpha^2 - \beta^2 = (2/N - 1)$ упрощается до вида

$$\cos\left(\frac{\theta}{2}\right) = 1 - \frac{2}{N} \sin^2\left(\frac{\Delta t}{2}\right). \quad (6.28)$$

Заметьте, что $\vec{\psi} \cdot \vec{r} = \hat{z} \cdot \vec{r}$, поэтому операторы $|\psi\rangle\langle\psi|$ и $|x\rangle\langle x|$ лежат на проведенной вокруг оси \vec{r} окружности на сфере Блоха. Подведем итог: действие оператора $U(\Delta t)$ заключается в повороте оператора $|\psi\rangle\langle\psi|$ вокруг оси \vec{r} на угол θ , как показано на рис. 6.6. Мы прервем процедуру, когда выполнено уже достаточно поворотов для того, чтобы перевести оператор $|\psi\rangle\langle\psi|$ в окрестность оператора $|x\rangle\langle x|$. Вначале мы предполагали, что величина Δt мала, поскольку рассматривался случай квантового моделирования, однако из уравнения (6.28) следует, что было бы разумно выбрать $\Delta t = \pi$, чтобы максимизировать угол поворота θ . Если поступить таким образом, то получим $\cos(\theta/2) = 1 - 2/N$, что при больших N соответствует значению $\theta \approx 4/\sqrt{N}$, а число обращений к оракулу, необходимых для отыскания решения $|x\rangle$, будет иметь порядок $O(\sqrt{N})$, как и в исходном квантовом алгоритме поиска.

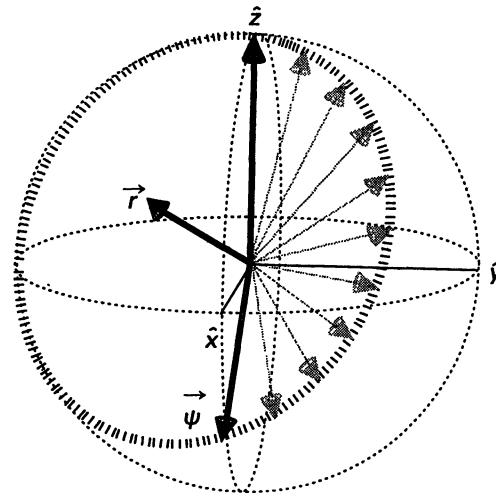


Рис. 6.6. Сфера Блоха, на которой показан поворот начального состояния $\vec{\psi}$ вокруг оси \vec{r} в сторону конечного состояния \hat{z}

В самом деле, если выбрать $\Delta t = \pi$, то такое «квантовое моделирование» идентично исходному квантовому алгоритму поиска, поскольку при квантовом моделировании применяются операторы $\exp(-i\pi|\psi\rangle\langle\psi|) = I - 2|\psi\rangle\langle\psi|$ и

$\exp(-i\pi|x\rangle\langle x|) = I - 2|x\rangle\langle x|$, которые с точностью до общего фазового множителя идентичны шагам в итерации Гровера. При таком рассмотрении изображенные на рис. 6.2 и 6.3 схемы для квантового алгоритма поиска являются упрощениями схем, показанных на рис. 6.4 и 6.5 для моделирования, в частном случае $\Delta t = \pi!$

Упражнение 6.10. Покажите, что путем подходящего выбора Δt можно получить квантовый алгоритм поиска, где используется $O(\sqrt{N})$ обращений и для которого вектор конечного состояния точно равен $|x\rangle$, т. е. алгоритм срабатывает с вероятностью единица, (а не какой-либо меньшей).

Мы получили заново квантовый алгоритм поиска другим способом — используя методы квантового моделирования. Почему этот подход действует? Можно ли его использовать для поиска других быстрых квантовых алгоритмов? Трудно определенным образом ответить на эти вопросы, однако выскажем несколько соображений, представляющих интерес. Основная процедура содержит четыре шага: 1) определить задачу, требующую решения, включая описание необходимых входных и выходных данных для квантового алгоритма; 2) угадать гамильтониан, который дает решение поставленной задачи, и проверить, что он действительно работает; 3) найти процедуру, которая моделирует гамильтониан и 4) изучить ресурсы, используемые для моделирования. Данный подход отличается от обычного в двух отношениях: необходимо угадать гамильтониан, а не квантовую схему; кроме того, отсутствует аналогия с шагами моделирования в стандартном подходе. Более важным из указанных двух различий является первое. Существует большая свобода в выборе квантовой схемы, решающей задачу. С одной стороны, эта свобода определяет большую мощь квантовых вычислений, с другой — делает поиск эффективных схем весьма непростым занятием. Напротив, определение гамильтониана — более жесткая задача, следовательно, для ее решения имеется меньше свободы, но эти же самые ограничения на самом деле упрощают поиск эффективного квантового алгоритма. Мы видели, что это происходит с квантовым алгоритмом поиска, вероятно, с помощью такого метода можно найти и другие квантовые алгоритмы — это не известно. По крайней мере неоспоримо то, что подход «квантовые алгоритмы как квантовое моделирование» дает интересную альтернативу для развития квантовых алгоритмов.

Упражнение 6.11 (квантовый поиск нескольких решений в непрерывном времени). Угадайте гамильтониан, позволяющий в непрерывном времени решить задачу поиска в случае, когда имеется M решений.

Упражнение 6.12 (альтернативный гамильтониан для квантового поиска). Пусть

$$H = |x\rangle\langle\psi| + |\psi\rangle\langle x|. \quad (6.29)$$

1. Покажите, что для поворота состояния $|\psi\rangle$ до состояния $|x\rangle$ требуется время $O(1)$, если эволюция описывается гамильтонианом H .
2. Объясните, как может быть выполнено квантовое моделирование гамильтониана H , и определите, сколько обращений к оракулу требуется в этом случае, чтобы получить решение с высокой вероятностью.

6.3 Квантовое перечисление

Насколько быстро можно определить количество решений M в задаче поиска из N элементов, если M заранее не известно? Очевидно, что на классическом компьютере потребуется $\Theta(N)$ обращений к оракулу. С помощью квантового компьютера можно определить число решений гораздо быстрее, чем с помощью обычного — необходимо использовать итерации Гровера и процедуру определения собственного числа, основанную на квантовом преобразовании Фурье (см. гл. 5). Рассмотрим важные применения этого факта. Во-первых, если мы умеем быстро определять число решений, то так же быстро можно находить решение, даже если заранее неизвестно, сколько их. Для этого нужно сначала определить число решений, а потом применить квантовый алгоритм поиска для нахождения решения. Во-вторых, квантовое перечисление позволяет установить, существует ли вообще решение для данной задачи поиска: мы просто должны понять, равно ли число решений нулю или нет. Имеются применения этой идеи, например, для решения NP-полных задач, которые могут быть сформулированы как вопрос о существовании решения задачи поиска.

Упражнение 6.13. Рассмотрите классический алгоритм для решения задачи перечисления, который выбирает равномерно и независимо k раз элементы из пространства поиска; пусть X_1, \dots, X_k — результаты, полученные при обращениях к оракулу, т. е. $X_j = 1$, если j -е обращение к оракулу дало решение задачи, и $X_j = 0$, если j -е обращение к оракулу не дало решения. Этот алгоритм выдает оценку $S \equiv N \times \sum_j X_j / k$ для числа решений задачи поиска. Покажите, что квадратичное отклонение величины S равно $\Delta S = \sqrt{M(N - M)}/k$. Докажите, что для получения с вероятностью не менее $3/4$ правильной с точностью до \sqrt{M} оценки для M при любых значениях M следует принять $k = \Omega(N)$.

Упражнение 6.14. Докажите, что любой классический алгоритм перечисления, дающий с вероятностью не меньше $3/4$ правильную оценку для M с точностью $c\sqrt{M}$ при некоторой константе c для любых значений M , должен использовать $\Omega(N)$ обращений к оракулу.

Квантовое перечисление — это применение описанной в разд. 5.2 процедуры нахождения собственного числа итерации Гровера G , позволяющее определить количество решений M задачи поиска. Пусть $|a\rangle$ и $|b\rangle$ — два собственных вектора итерации Гровера в пространстве, наложенном на векторы $|\alpha\rangle$ и $|\beta\rangle$, а θ — угол поворота, определяемый итерацией Гровера. Из уравнения (6.13) следует, что соответствующие собственные числа равны $e^{i\theta}$ и $e^{i(2\pi-\theta)}$. Для простоты анализа удобно предположить, что оракул был расширен, как это описывалось в разд. 6.1, за счет увеличения количества элементов в пространстве поиска до $2N$ и обеспечения выполнения условия $\sin^2(\theta/2) = M/2N$.

Схема определения собственного числа, используемая для квантового перечисления, показана на рис. 6.7. Ее значение состоит в том, чтобы определить θ с точностью 2^{-m} при вероятности успеха не менее $(1 - \varepsilon)$. Первый регистр содержит $t \equiv m + \lceil \log(2 + 1/2\varepsilon) \rceil$ кубитов, как в процедуре определения собственного числа, а второй включает $(N + 1)$ кубит, что является достаточным для реализации итерации Гровера на расширенном пространстве поиска. Со-

стояние второго регистра переводится в суперпозицию всех возможных входных значений с равными весами ($\sum_x |x\rangle$) с помощью преобразования Адамара. Как показано в разд. 6.1, это состояние есть суперпозиция собственных состояний $|a\rangle$ и $|b\rangle$, поэтому, согласно результату разд. 5.2, схема, изображенная на рис. 6.7, дает ответ θ или $(2\pi - \theta)$ с точностьюю $|\Delta\theta| \leq 2^{-m}$ при вероятности не менее $(1 - \varepsilon)$. Более того, ответ $2\pi - \theta$, очевидно, эквивалентен ответу θ с той же точностьюю, поэтому в действительности процедура определения собственного числа определяет значение θ с точностьюю 2^{-m} и вероятностью успеха $(1 - \varepsilon)$.

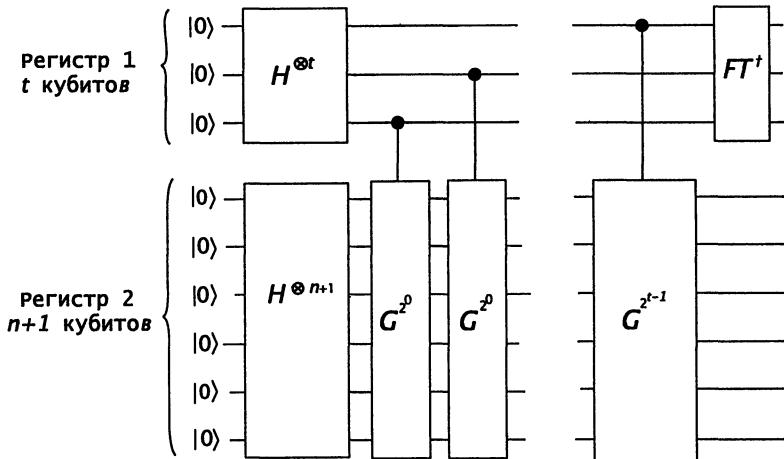


Рис. 6.7. Схема для выполнения приближенного квантового перечисления на квантовом компьютере.

Используя уравнение $\sin^2(\theta/2) = M/2N$ и нашу оценку для величины θ , получим оценку для количества решений M . Насколько большой будет ошибка ΔM в этой оценке? Выполним следующую последовательность вычислений:

$$\frac{|\Delta M|}{2N} = \left| \sin^2\left(\frac{\theta + \Delta\theta}{2}\right) - \sin^2\left(\frac{\theta}{2}\right) \right| = \quad (6.30)$$

$$= \left(\sin\left(\frac{\theta + \Delta\theta}{2}\right) + \sin\left(\frac{\theta}{2}\right) \right) \left| \sin\left(\frac{\theta + \Delta\theta}{2}\right) - \sin\left(\frac{\theta}{2}\right) \right|. \quad (6.31)$$

Из курса анализа известно, что $|\sin((\theta + \Delta\theta)/2) - \sin(\theta/2)| \leq |\Delta\theta|/2$, поэтому (с учетом очевидного тригонометрического неравенства $|\sin((\theta + \Delta\theta)/2)| < |\sin(\theta/2)| + |\Delta\theta/2|$) получим оценку

$$\frac{|\Delta M|}{2N} < \left(2 \sin\left(\frac{\theta}{2}\right) + \frac{|\Delta\theta|}{2} \right) \frac{|\Delta\theta|}{2}. \quad (6.32)$$

Сделав подстановку $\sin^2(\theta/2) = M/2N$ и учитывая тот факт, что $|\Delta\theta| \leq 2^{-m}$, получим окончательную оценку для ошибки определения величины M :

$$|\Delta M| < \left(\sqrt{2MN} + \frac{N}{2^m + 1} \right) 2^{-m}. \quad (6.33)$$

Рассмотрим пример. Предположим, мы выбрали $m = [n/2] + 1$, $\varepsilon = 1/6$. Тогда получим $t = [n/2] + 3$, поэтому алгоритм требует $\Theta(\sqrt{N})$ итераций Гровера, а следовательно, и $\Theta(\sqrt{N})$ обращений к оракулу. Согласно оценке (6.33), точность определяется неравенством $|\Delta M| < \sqrt{M/2} + 1/4 = O(\sqrt{M})$. Сравните эту оценку с упражнением 6.14, в котором утверждается, что на классическом компьютере для получения подобной точности потребовалось бы $O(N)$ обращений к оракулу.

Только что описанный пример несет двойную нагрузку. Во-первых, этот алгоритм определяет, есть ли вообще решение у задачи поиска, т. е. выполняется ли условие $M = 0$ или $M \neq 0$. Если $M = 0$, то получим, что $|\Delta M| < 1/4$, поэтому алгоритм должен дать ответ «нуль» с вероятностью не менее $5/6$. На-против, если $M \neq 0$, то легко проверить, что ответ для M будет отличен от нуля с вероятностью по крайней мере $5/6$.

Во-вторых, квантовое перечисление применяется для *нахождения* решения задачи поиска, когда число решений M неизвестно. Трудность в применении квантового алгоритма поиска заключается в том, что число повторений итерации Гровера (определенное уравнением (6.15)) зависит от знания количества решений M (см. разд. 6.1). Эта проблема может быть решена с использованием квантового алгоритма перечисления (для оценки θ и M с высокой точностью используется процедура нахождения собственного числа) с последующим применением квантового алгоритма поиска (аналогично разд. 6.1), при этом итерации Гровера будут повторяться R раз (где R определяется уравнением (6.15), а оценки для θ и M получены с помощью процедуры нахождения собственного числа). Ошибка в определении угла в этом случае не превосходит $(\pi/4)(1 + |\Delta\theta|/\theta)$, поэтому если выбрать, как и раньше, $m = [n/2] + 1$, то ошибка по углу будет не больше, чем $\pi/4 \cdot 3/2 = 3\pi/8$, что соответствует вероятности успешного завершения алгоритма поиска не менее $\cos^2(3\pi/8) = 1/2 - 1/(2\sqrt{2}) \approx 0.15$. Если вероятность получения оценки для θ с такой точностью равна $5/6$, как в нашем предыдущем примере, тогда окончательная вероятность нахождения решения задачи поиска составит $5/6 \cdot \cos^2(3\pi/8) \approx 0.12$, и она может быть приближена к единице, если несколько раз повторить комбинированную процедуру перечисления–поиска.

6.4 Ускорение решения NP-полных задач

Квантовый поиск можно использовать для ускорения решения задач в классе сложности NP (см. подразд. 3.2.2). Выше было показано (см. подраздел 6.1.1), как можно ускорить поиск простых делителей, теперь рассмотрим, как можно применить квантовый поиск к задаче о гамильтоновом цикле (НС). Напомним, что гамильтоновым циклом для данного графа называют цикл, обходящий все вершины графа «ровно» по одному разу. Задача НС заключается в определении, содержит ли данный граф гамильтонов цикл. Она относится к классу NP-полных задач, для которых неизвестны быстрые алгоритмы решения для классического компьютера (однако не доказано, что таких алгоритмов вообще не существует).

Простой алгоритм решения НС состоит в поиске по всем возможным спискам вершин длины n :

1. задать все возможные списки (v_1, \dots, v_n) вершин графа; повторы вершин разрешаются, поскольку они упрощают анализ, не влияя на содержательный результат;
2. для каждого списка проверить, задает ли он гамильтонов цикл в графе; если нет, продолжить перебор.

Поскольку существуют $n^n = 2^{n \log n}$ возможных списков вершин, которые надо перебрать, этот алгоритм требует в худшем случае $2^{n \log n}$ проверок, является ли цикл гамильтоновым. Любая задача в классе NP может быть решена аналогичным образом: если задача размера n имеет решения, которые могут быть записаны с использованием $w(n)$ бит, где $w(n)$ — некоторый многочлен от n , то поиск среди $2^{w(n)}$ гипотетических решений даст настоящее решение задачи, если оно существует.

Квантовый алгоритм поиска может быть использован для ускорения этого алгоритма за счет более быстрого выполнения поиска. Мы используем описанный в разд. 6.3 алгоритм для определения того, существует ли решение задачи поиска. Пусть $m \equiv \lceil \log n \rceil$. Пространство поиска будет представлено строкой из mn кубит, где каждый блок из m кубит используется для хранения номера отдельной вершины. Таким образом, можно записать состояния вычислительного базиса следующим образом: $|v_1, \dots, v_n\rangle$, где каждый из элементов $|v_i\rangle$ отображается подходящей строкой из m кубит, т. е. общее количество кубитов равно mn . Оракул для квантового алгоритма поиска должен применить преобразование

$$O|v_1, \dots, v_n\rangle = \begin{cases} |v_1, \dots, v_n\rangle, & \text{если } v_1, \dots, v_n \text{ не гамильтонов цикл,} \\ -|v_1, \dots, v_n\rangle, & \text{если } v_1, \dots, v_n \text{ гамильтонов цикл.} \end{cases} \quad (6.34)$$

Такой оракул легко построить по описанию графа. Следует взять классическую схему полиномиального размера, распознающую гамильтоновы циклы, и превратить ее в обратимую схему (имеющую также полиномиальный размер), выполняющую преобразование $(v_1, \dots, v_n, q) \rightarrow (v_1, \dots, v_n, q \oplus f(v_1, \dots, v_n))$, где $f(v_1, \dots, v_n) = 1$, когда v_1, \dots, v_n — гамильтонов цикл, и $f(v_1, \dots, v_n) = 0$ в противном случае. Реализация соответствующей схемы на квантовом компьютере с последним кубитом, устанавливаемым в начальный момент в состояние $(|0\rangle - |1\rangle)/\sqrt{2}$, дает требуемое преобразование. Мы не будем здесь указывать в явном виде детали, отметим лишь ключевой момент: оракул требует полиномиального по n количества элементов (это является прямым следствием того факта, что гамильтоновы циклы можно распознать классическим образом с помощью полиномиального числа элементов). Применяя вариант алгоритма поиска, который определяет, существует ли решение задачи поиска (см. разд. 6.3), мы видим, что для выяснения того, существует ли гамильтонов цикл, потребуется $O(2^{mn/2}) = O(2^{n\lceil \log n \rceil / 2})$ обращений к оракулу. Если цикл существует, легко применить комбинированный алгоритм перечисления–поиска, с

помощью которого и станет возможным найти такой цикл. Последний и будет являться решением задачи.

Таким образом, можно сделать следующие выводы.

- В классическом алгоритме перебора требуется $O(p(n)2^{n[\log n]})$ операций, чтобы определить, существует ли гамильтонов цикл, где полиномиальный множитель $p(n)$ — накладные расходы, связанные в основном с реализацией оракула, т. е. элементов, проверяющих, является ли пробный путь гамильтоновым или нет. Определяющим фактором, задающим необходимые ресурсы, является показатель степени в выражении $2^{n[\log n]}$. Классический алгоритм является детерминированным, т. е. завершается с вероятностью 1.
- Чтобы получить квантовый алгоритм, необходимо произвести $O(p(n)2^{n[\log n]/2})$ операций для определения того, существует ли гамильтонов цикл, где полиномиальный множитель $p(n)$ — накладные расходы, связанные в основном с реализацией оракула. Определяющим фактором, задающим требуемые ресурсы, является показатель степени в выражении $2^{n[\log n]/2}$. Существует конечная вероятность (например, $1/6$) ошибки в данном алгоритме; она может быть уменьшена до $1/6^r$ за счет r -кратного повторения алгоритма.
- Для реализации асимптотически квантового алгоритма требуется число операций, которое является *квадратным корнем* из числа операций, необходимых для выполнения классического алгоритма.

6.5 Квантовый поиск в неструктурированной базе данных

Представьте себе, что некто дает вам список, содержащий тысячу названий цветов, а затем спрашивает, в каком месте списка появляется название «пертская роза». Если каждое название появляется в списке лишь один раз и никакого очевидного упорядочения нет, вам в среднем придется просмотреть 500 названий, прежде чем вы отыщете «пертскую розу». Можно ли ускорить *поиск по базе данных* такого сорта, используя квантовый алгоритм поиска? Квантовый алгоритм поиска иногда упоминают как алгоритм поиска по базе данных, однако его полезность для этого применения ограничена и основывается на определенных предположениях. В этом разделе мы покажем, как квантовый алгоритм поиска может в *принципе* быть использован для поиска в неструктуреированной базе данных в исполнении, аналогичном примененному в обычном компьютере. Построенная нами картина прояснит, какие ресурсы требуются, чтобы дать возможность квантовому компьютеру проводить поиск в классической базе данных.

Предположим, что имеется база данных, содержащая $N \equiv 2^n$ записей, каждая длиной l битов. Обозначим эти записи как d_1, \dots, d_N . Мы хотим определить, где именно находится заданная строка из l битов (обозначим ее буквой s).

Классический компьютер, используемый для решения такой задачи, обычно включает две части (рис. 6.8). В одной, называемой *центральным процессором*, происходит обработка данных с использованием небольшого объема временной памяти. Вторая представляет собой большой объем *памяти*, где хранится база данных в виде строки из 2^n блоков по l битовых ячеек. Предполагается, что память пассивна — в том смысле, что она сама по себе не может обрабатывать данные. Возможно только ЗАГРУЖАТЬ данные из памяти в процессор и СОХРАНЯТЬ в памяти данные, полученные от ЦП, а также проводить манипуляции с данными, временно хранимыми в процессоре. Классические компьютеры могут быть устроены по-разному, но их разделение на процессор и память является очень распространенным и стандартным для компьютерной архитектуры.

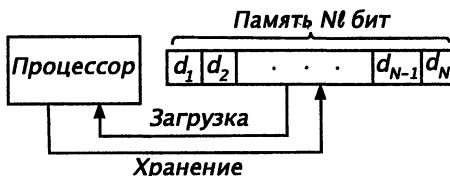


Рис. 6.8. Классический поиск по базе данных с помощью компьютера, состоящего из центрального процессора и памяти. Можно выполнить только две операции с памятью: загрузку в процессор или пересылку записи на хранение из процессора в память

В классическом случае наиболее эффективный алгоритм определения, где именно в неструктурированной базе находится заданная строка s , выглядит следующим образом. Сначала в процессор помещают n -битовый указатель записи базы данных. Предполагается, что процессор обладает достаточной емкостью для того, чтобы хранить указатель из $n \equiv \lceil \log N \rceil$ битов. Вначале этот указатель равен нулю, а потом увеличивается на единицу при каждой итерации алгоритма. На каждой итерации в процессор загружается запись из базы данных, соответствующая текущему значению указателя, после чего она сравнивается с шаблоном отыскиваемой строки. Если они совпадают, алгоритм выдает значение указателя, происходит остановка. Если они различаются, алгоритм продолжает увеличивать значение указателя. Очевидно, что при таком алгоритме записи будут загружаться из памяти в худшем случае 2^n раз. Ясно, что это наиболее эффективный алгоритм, позволяющий решить эту задачу при такой организации вычислений.

Насколько эффективно аналогичный алгоритм может быть реализован с помощью квантового компьютера? А если ускорение с помощью квантового подхода возможно, то насколько такой алгоритм окажется полезным? Сначала покажем, что ускорение возможно, а затем вернемся к вопросу о пользе такого алгоритма. Предположим, наш квантовый компьютер, как и в классическом случае, состоит из двух частей — ЦП и памяти. Будем считать, что процессор содержит четыре регистра: 1) n -кубитовый «указатель», установленный в начальный момент времени в состояние $|0\rangle$; 2) l -кубитовый регистр, приведенный при запуске алгоритма в состояние $|s\rangle$ и остающийся в таком состоянии до конца вычислений; 3) l -кубитовый регистр данных, находящийся в

начальный момент в состояние $|0\rangle$; 4) 1-кубитовый регистр, установленный в состояние $(|0\rangle - |1\rangle)/\sqrt{2}$.

Память может быть организована двумя различными способами. В простейшем случае — это квантовая память, состоящая из $N = 2^n$ ячеек по l битов, каждая из которых содержит запись базы данных $|d_x\rangle$. Второй способ предполагает построение классической памяти, содержащей $N = 2^n$ ячеек по l битов, каждая из которых содержит запись d_x . Однако в отличие от классической памяти к ней можно обращаться через указатель x , который находится в состоянии $|x\rangle$, являющемся, вообще говоря, суперпозицией нескольких значений. Этот квантовый указатель позволяет выполнять ЗАГРУЗКУ суперпозиции значений из разных ячеек памяти. Доступ к памяти работает следующим образом: если регистр указателя находится в состоянии $|x\rangle$, а регистр данных — в состоянии $|d\rangle$, то к регистру данных добавляется содержимое d_x из x -й ячейки памяти: $|d\rangle \rightarrow |d \oplus d_x\rangle$, сложение выполняется побитово по модулю 2. Сначала посмотрим, как эта возможность используется для выполнения квантового поиска, а затем обсудим пути реального построения такой памяти.

Ключевой момент в осуществлении квантового алгоритма поиска — реализация оракула, который должен осуществлять переворот фазы указателя, задающего место кубита s в памяти. Предположим, процессор находится в состоянии

$$|x\rangle|s\rangle|0\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \quad (6.35)$$

Применение операции ЗАГРУЗКА переведет компьютер в состояние

$$|x\rangle|s\rangle|d_x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \quad (6.36)$$

Теперь сравниваются второй и третий регистры, и если их значения совпадают, то к четвертому регистру применяется операция обращения бита; в противном случае ничего не меняется. Результат действия этой операции следующий:

$$|x\rangle|s\rangle|d_x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \rightarrow \begin{cases} -|x\rangle|s\rangle|d_x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}, & \text{если } d_x = s, \\ |x\rangle|s\rangle|d_x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}, & \text{если } d_x \neq s. \end{cases} \quad (6.37)$$

После этого в регистре данных восстанавливается значение $|0\rangle$ (для этого опять выполняется операция ЗАГРУЗКА). Все действия оракула оставляют неизменными значения регистров 2, 3 и 4; кроме того, они не будут запутаны с состоянием регистра 1. Таким образом, этот шаг заключается в том, чтобы перевести состояние в регистре 1 из $|x\rangle$ в $-|x\rangle$, если $d_x = s$, и оставить состояние в этом регистре неизменным в противном случае. С использованием построенного таким образом оракула можно применить квантовый алгоритм поиска для определения положения s в базе данных, выполнив $O(\sqrt{N})$ операций ЗАГРУЗКА (в то время как в классическом случае требовалось N таких операций).

На первый взгляд кажется, что для правильной работы оракула с суперпозиционными состояниями необходимо, чтобы память подчинялась квантовомеханическим законам. На самом деле, как было отмечено выше, с некоторыми

предосторожностями память может быть организована классическим образом, что, по-видимому, делает ее более устойчивой по отношению к шумам. Однако по-прежнему требуется квантовомеханическая схема *адресации*; принципиальная схема, иллюстрирующая такую организацию памяти, показана на рис. 6.9.

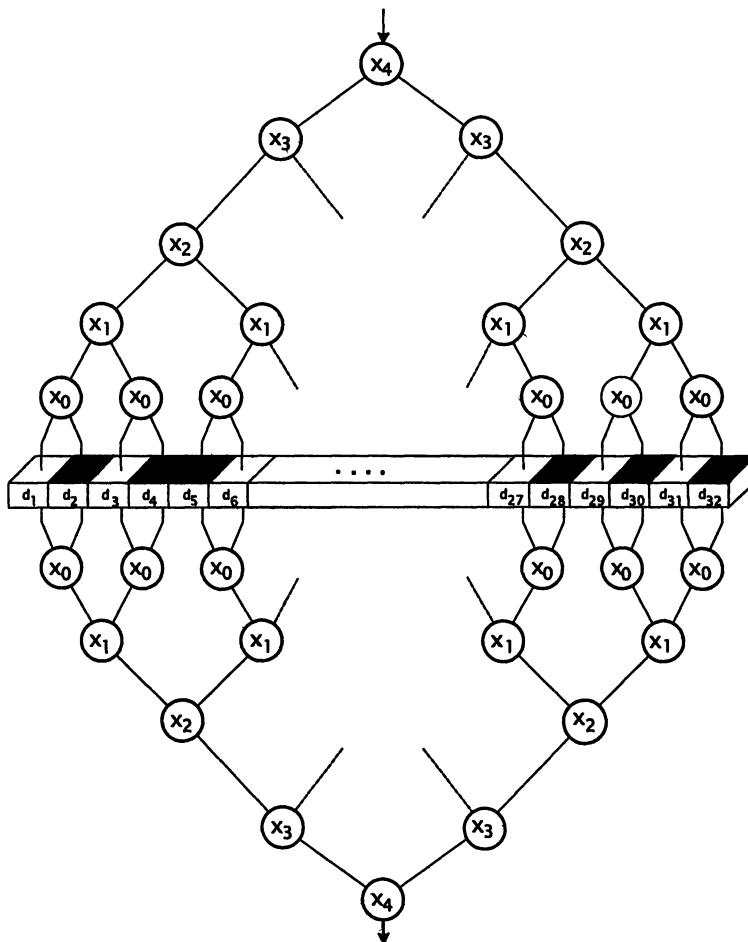


Рис. 6.9. Принципиальная схема классической памяти с 32 ячейками и пятикубитовой схемой адресации. Каждый кружок представляет собой переключатель, и обращение к нему отвечает изображенному внутри кубиту. Например, когда $|x_4\rangle = |0\rangle$, соответствующий переключатель отправляет входной кубит налево, когда $|x_4\rangle = |1\rangle$ — направо. Если $|x_4\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, то будет суперпозиция обоих путей с равными весами. Кубиты, отображающие регистр данных, входят в схему на вершине дерева и спускаются вниз к базе данных, которая меняет их состояние по правилам, определяемым содержимым памяти. Далее кубиты переводятся назад в определенную позицию, сохраняя полученную информацию. С физической точки зрения такая схема может быть реализована с использованием, например, одиночных фотонов для кубитов, содержащих значения регистров данных, которые управляются с помощью нелинейных интерферометров (см. гл. 7). Классическая база данных может быть просто кусочком пластика, в котором «нули» (светлые прямоугольники на рисунке) пропускают свет без изменений, а «единицы» (темные прямоугольники) поворачивают поляризацию падающего света на 90° .

Основная идея заключается в переходе от бинарного кодирования квантового указателя (состояния от 0 до $(2^n - 1)$ отображаются n битами) к унарному (состояния от 0 до $(2^n - 1)$ представляются положением одного «зонда» в одной из 2^n возможных позиций), с помощью которого задавался указатель записи в классической базе данных. База данных действует на «внутреннюю» степень свободы «зонда», не связанную с его положением. Далее переход от бинарного кодирования к унарному обращается, оставляя в регистре данных требуемое содержимое.

Существуют ли практические применения, в которых квантовый алгоритм поиска может быть полезен при поиске по классическим базам данных? Следует сделать два замечания. Во-первых, базы данных не являются абсолютно неструктурированными. Простые базы данных (вспомните обсуждавшийся выше список цветов) могут быть упорядочены по алфавиту, так что можно использовать бинарный поиск, при котором запись будет найдена в базе, содержащей N записей, за время $O(\log N)$. Тем не менее в некоторых базах данных используется более сложная структура, и, хотя для оптимизации классического поиска применяются сложные методы, в случае, когда рассматриваются записи достаточно сложной и непредсказуемой природы, заранее организованная структура базы данных может оказаться бесполезной; в таком случае задачу следует рассматривать как поиск в фактически неструктурированной базе данных.

Во-вторых, чтобы квантовый компьютер мог проводить поиск по классической базе данных, требуется квантовая схема адресации памяти. Описанная выше схема требует $O(N \log N)$ квантовых переключателей — т. е. примерно такой же объем (квантовой) памяти, какой требуется для хранения самой базы. Не исключено, что эти переключатели в какой-то момент станут столь же простыми и дешевыми, как и классическая память, однако пока этого не произойдет, построение квантового компьютера для выполнения квантового поиска не будет экономически выгодным по сравнению с классическими вычислительными устройствами.

Принимая во внимание приведенный выше анализ, мы можем заключить, что основным применением квантовых алгоритмов поиска вряд ли будет являться поиск в классических базах данных. Скорее, они будут использоваться в поиске решений сложных задач, таких, как задача о гамильтоновом цикле, задачи коммивояжера и выполнимости.

6.6 Оптимальность алгоритма поиска

Мы показали, что с помощью квантового компьютера можно организовать поиск среди N записей с использованием только $O(\sqrt{N})$ обращений к оракулу. Сейчас мы докажем, что никакой квантовый алгоритм не может решить эту задачу с менее чем $\Omega(\sqrt{N})$ обращениями к оракулу, т. е. что предложенный нами квантовый алгоритм является оптимальным.

Предположим, что алгоритм начинается с состояния $|\psi\rangle$. Для простоты определим нижнюю оценку для случая, когда у задачи поиска имеется толь-

ко одно решение x . Чтобы найти последнее, нам разрешается обращаться к оракулу O_x , который дает фазовый сдвиг на -1 для решения $|x\rangle$ и оставляет все остальные состояния неизменными: $O_x = I - 2|x\rangle\langle x|$. Пусть алгоритм начинается с состояния $|\psi\rangle$, а оракул O_x вызывается ровно k раз; между обращениями к оракулу применяются унитарные преобразования U_1, U_2, \dots, U_k . Введем следующие определения:

$$|\psi_k^x\rangle \equiv U_k O_x U_{k-1} O_x \dots U_1 O_x |\psi\rangle, \quad (6.38)$$

$$|\psi_k\rangle \equiv U_k U_{k-1} \dots U_1 |\psi\rangle. \quad (6.39)$$

Другими словами, $|\psi_k\rangle$ — состояние, которое получается в результате последовательного применения операций U_1, \dots, U_k без обращений к оракулу. Пусть $|\psi_0\rangle = |\psi\rangle$. Наша задача заключается в том, чтобы оценить величину

$$D_k \equiv \sum_x \|\psi_k^x - \psi_k\|^2, \quad (6.40)$$

где использовано обозначение ψ вместо $|\psi\rangle$ для упрощения записи формул. Интуитивно ясно, что D_k — мера вызванного оракулом *отклонения* после k шагов от эволюции, которая имела бы место без оракула. Если эта величина мала, то все состояния $|\psi_k^x\rangle$ примерно одинаковы и значение x невозможно определить правильно с высокой вероятностью. Стратегия доказательства состоит: а) в оценке величины D_k , которая показывает, что она не может расти быстрее, чем $O(k^2)$; б) в доказательстве того, что величина D_k должна иметь порядок $\Omega(N)$, если можно различить N вариантов. Объединив эти два результата, получим требуемую нижнюю оценку.

Вначале докажем по индукции, что $D_k \leq 4k^2$. Для $k = 0$ это утверждение очевидно (Так как $D_0 = 0$). Обратите внимание на тот факт, что

$$D_{k+1} = \sum_x \|O_x \psi_k^x - \psi_k\|^2 \quad (6.41)$$

$$= \sum_x \|O_x(\psi_k^x - \psi_k) + (O_x - I)\psi_k\|^2. \quad (6.42)$$

Принимая во внимание неравенство $\|b + c\|^2 \leq \|b\|^2 + 2\|b\|\|c\| + \|c\|^2$ при $b \equiv O_x(\psi_k^x - \psi_k)$ и $c \equiv (O_x - I)\psi_k = -2\langle x|\psi_k|x\rangle$ придем к неравенству

$$D_{k+1} \leq \sum_x (\|\psi_k^x - \psi_k\|^2 + 4\|\psi_k^x - \psi_k\||\langle x|\psi_k\rangle| + 4|\langle\psi_k|x\rangle|^2). \quad (6.43)$$

Применив неравенство Коши-Шварца ко второму члену в правой части и заметив, что $\sum_x |\langle x|\psi_k\rangle|^2 = 1$, получим

$$D_{k+1} \leq D_k + 4 \left(\sum_x \|\psi_k^x - \psi_k\|^2 \right)^{1/2} \left(\sum_{x'} |\langle\psi_k|x'\rangle|^2 \right)^{1/2} + 4 \quad (6.44)$$

$$\leq D_k + 4\sqrt{D_k} + 4. \quad (6.45)$$

С учетом предположения индукции ($D_k \leq 4k^2$) получим

$$D_{k+1} \leq 4k^2 + 8k + 4 = 4(k+1)^2, \quad (6.46)$$

что завершает доказательство по индукции.

Чтобы завершить доказательство, нужно показать, что вероятность успешного выполнения алгоритма может быть высокой только в том случае, когда D_k имеет порядок $\Omega(N)$. Предположим, что $|\langle x|\psi_k^x \rangle|^2 \geq 1/2$ для всех x , т. е. наблюдение дает решение задачи поиска с вероятностью не менее $1/2$. Замена $|x\rangle$ на $e^{i\theta}|x\rangle$ не изменяет вероятности успеха, поэтому без потери общности можно предположить, что $\langle x|\psi_k^x \rangle = |\langle x|\psi_k^x \rangle|$, следовательно,

$$\|\psi_k^x - x\|^2 = 2 - 2|\langle x|\psi_k^x \rangle| \leq 2 - \sqrt{2}. \quad (6.47)$$

Введя определение $E_k \equiv \sum_x \|\psi_k^x - x\|^2$, мы заметим, что $E_k \leq (2 - \sqrt{2})N$. Теперь мы в состоянии доказать, что D_k имеет порядок $\Omega(N)$. Используя определение $F_k \equiv \sum_x \|x - \psi_k\|^2$, получим

$$D_k = \sum_x \|(\psi_k^x - x) + (x - \psi_k)\|^2 \quad (6.48)$$

$$\geq \sum_x \|\psi_k^x - x\|^2 - 2 \sum_x \|\psi_k^x - x\| \|x - \psi_k\| + \sum_x \|x - \psi_k\|^2 \quad (6.49)$$

$$= E_k + F_k - 2 \sum_x \|\psi_k^x - x\| \|x - \psi_k\|. \quad (6.50)$$

Применив неравенство Коши–Шварца, приедем к следующей формуле: $\sum_x \|\psi_k^x - x\| \|x - \psi_k\| \leq \sqrt{E_k F_k}$, поэтому

$$D_k \geq E_k + F_k - 2\sqrt{E_k F_k} = (\sqrt{F_k} - \sqrt{E_k})^2. \quad (6.51)$$

В упражнении 6.15 вам предлагается показать, что $F_k \geq 2N - 2\sqrt{N}$. Этот факт совместно с неравенством $E_k \leq (2 - \sqrt{2})N$ дает неравенство $D_k \geq cN$ для достаточно больших N , где c — произвольная константа, меньшая, чем $(\sqrt{2} - \sqrt{2 - \sqrt{2}})^2 \approx 0,42$. С учетом неравенства $D_k \leq 4k^2$ можно получить формулу

$$k \geq \sqrt{cN/4}. \quad (6.52)$$

Таким образом, для получения вероятности успеха не ниже $1/2$ в задаче поиска необходимо сделать $\Omega(\sqrt{N})$ обращений к оракулу.

Упражнение 6.15. Покажите (с использованием неравенства Коши–Шварца), что для любого нормированного вектора состояния $|\psi\rangle$ и базиса $|x\rangle$ из N ортонормированных векторов выполняется неравенство

$$\sum_x \|\psi - x\|^2 \geq 2N - 2\sqrt{N}. \quad (6.53)$$

Упражнение 6.16. Предположим, мы выдвигаем только требование, чтобы вероятность ошибки при усреднении по всем возможным значениям x (а не по

всем значениям x) была менее $1/2$. Покажите, что для решения такой задачи поиска по-прежнему необходимо $O(\sqrt{N})$ обращений к оракулу.

Приведенное выше утверждение о том, что квантовый алгоритм поиска по существу оптимален, является одновременно захватывающим и разочаровывающим. Захватывающим оно является постольку, поскольку оказывается, по крайней мере в данной задаче, что мы полностью проникли в глубины квантовой механики — дальнейшее улучшение невозможно. Разочаровывающим оно является потому, что можно было бы надеяться на существенно большее ускорение по сравнению со степенным, полученным в квантовом алгоритме поиска. Можно помечтать о том, чтобы выполнять поиск в пространстве из N элементов, используя $O(\log N)$ обращений к оракулу. Если бы такой алгоритм существовал, он бы позволил эффективно решать **NP**-полные задачи на квантовом компьютере, поскольку с его помощью можно было бы перебирать $2^{w(n)}$ возможных вариантов с использованием $w(n)$ обращений к оракулу, где многочлен $w(n)$ представляет собой длину перебираемых объектов в битах. К сожалению, такой алгоритм не существует. Это является полезной информацией для потенциальных создателей алгоритмов, так как из этого факта следует, что «наивный» алгоритм решения **NP**-полных задач с помощью поиска по базе данных заведомо не приведет к успеху.

Оsmелившись перейти в область догадок, отметим, что многие исследователи полагают, что основным источником сложности в решении **NP**-полных задач является отсутствие какой бы то ни было структуры в пространстве поиска, а также что (с точностью до полиномиальных множителей) наилучший способ решения таких задач состоит в использовании метода перебора. Если встать на эту точку зрения, то ситуация с квантовыми вычислениями не внушает оптимизма, поскольку тогда класс задач, эффективно решаемых с помощью квантового компьютера (**BQP**), не содержит **NP**-полных задач. Конечно, это всего лишь точка зрения, и все-таки возможно, что **NP**-полные задачи содержат некоторую неизвестную структуру, которая позволяет быстро решать их с помощью квантового компьютера (а возможно даже и с помощью классического). Красивым примером, иллюстрирующим эту идею, является задача разложения на простые множители, которую принято считать относящейся к классу **NPI**-задач (промежуточных по сложности между **P**- и **NP**-полными задачами). Главной идеей для эффективного решения квантовомеханическими средствами задачи разложения на множители являлось использование «спрятанной» внутри задачи структуры — она была обнаружена при сведении этой задачи к нахождению порядка. Даже когда эта удивительная структура была выявлена, стало ясно, что ее нельзя использовать для построения эффективного классического алгоритма разложения на множители, хотя, конечно, с квантовомеханическими средствами эту структуру можно использовать для построения эффективного алгоритма! Возможно, аналогичная структура скрыта и в других задачах, которые предположительно относятся к классу **NPI**, например, в задаче об изоморфизме графов, и даже, возможно, в самих **NP**-полных задачах.

Упражнение 6.17 (оптимальность для неединственных решений).

Пусть задача поиска имеет M решений. Покажите, что для нахождения решения требуется $O(\sqrt{N/M})$ обращений к оракулу.

6.7 Ограничение алгоритмов в модели черного ящика

В завершение рассмотрим обобщение квантового алгоритма поиска, которое позволяет увидеть ограничения эффективности квантовых вычислений. В начале главы мы описали задачу поиска как нахождение такого n -битового целого числа x , что функция $f: \{0, 1\}^n \rightarrow \{0, 1\}$ дает значение $f(x) = 1$. С этой задачей связана задача *разрешения*: существует ли такое число x , что $f(x) = 1$? Сложность последней задачи совпадает со сложностью задачи поиска; сама задача разрешения может быть сформулирована как вычисление булевой функции $F(X) = X_0 \vee X_1 \vee \dots \vee X_{N-1}$, где символ « \vee » указывает двоичную операцию OR (или), $X_k \equiv f(k)$, а буквой « X » обозначается множество $\{X_0, X_1, \dots, X_{N-1}\}$. В более общем случае возможно вычисление не OR, а какой-нибудь другой функции. Например, $F(X)$ может быть одной из следующих функций: AND, PARITY (сумма по модулю 2), MAJORITY ($F(X) = 1$ тогда и только тогда, когда большинство чисел X_k равно единице). Вообще говоря, можно рассматривать в качестве F любую булеву функцию. Насколько быстро (по количеству запросов) можно вычислить классическим или квантовым образом эти функции, если имеется оракул для f ?

Может показаться, что ответить на такой вопрос трудно, если о функции f ничего неизвестно. Однако на самом деле многое можно определить даже в этой модели черного ящика, где средства, с помощью которых оракул выполняет свою задачу, считаются данными, а сложность измеряется только необходимым количеством обращений к оракулу. Анализ алгоритма поиска в предыдущем разделе показал один из подходов к таким задачам, однако существует более мощный подход для определения сложности, выраженной в количестве запросов, — *метод многочленов*, который кратко будет описан ниже.

Начнем с некоторых полезных определений. Детерминированная оракульная сложность $D(F)$ — это минимальное количество обращений к оракулу на классическом компьютере, необходимое для достоверного вычисления F . Квантовый аналог $Q_E(F)$ — минимальное число обращений к оракулу, необходимое квантовому компьютеру, для вычисления достоверного F . Поскольку квантовый компьютер по своей природе выдает вероятностные результаты, более интересной величиной является сложность в оракульной модели с ограниченной ошибкой $Q_2(F)$ — минимальное количество обращений к оракулу, которое необходимо квантовому компьютеру для выдачи ответа, который равен F с вероятностью не менее $2/3$. (Величина $2/3$ выбрана достаточно произвольным образом — на самом деле требуется только, чтобы вероятность была на сколько-то больше $1/2$, т. е. чтобы она приближалась к единице после достаточного числа повторов.) Близким понятием является сложность безошибочных вероятностных алгоритмов в оракульной модели $Q_0(F)$ — минимальное число обращений

к оракулу, необходимое квантовому компьютеру, чтобы либо выдать результат, который достоверно равен F , либо (с вероятностью меньше $1/2$) сообщить, что требуемый результат не получен. Все эти оценки должны выполняться для любой функции оракула f (другими словами, для любого входа X функции F). Обратите внимание на тот факт, что $Q_2(F) \leq Q_0(F) \leq Q_E(F) \leq D(F) \leq N$.

Метод многочленов опирается на свойства мультилинейных функций (над множеством действительных чисел), которые *представляют* булевы функции. Все многочлены, которые будут рассматриваться в дальнейшем — это функции с аргументами $X_k \in \{0, 1\}$, вследствие чего они являются мультилинейными (поскольку $\bar{X}_k^2 = X_k$). Будем говорить, что многочлен $p: \mathbb{R}^N \rightarrow \mathbb{R}$ представляет функцию F , если $p(X) = F(X)$ для всех $X \in \{0, 1\}^N$ (здесь символ « \mathbb{R} » обозначает множество действительных чисел). Такой многочлен p всегда существует, можно построить его явно:

$$p(X) = \sum_{Y \in \{0, 1\}^N} F(Y) \prod_{k=0}^{N-1} [1 - (Y_k - X_k)^2]. \quad (6.54)$$

Тот факт, что представляющий F многочлен p минимальной степени определен однозначно, читателю предлагается доказать самостоятельно (см. упражнение 6.18). Минимальная степень мультилинейного представления функции F (она обозначается $\deg(F)$) является полезной мерой сложности функции F . Например, известно, что $\deg(\text{OR}) = N$, $\deg(\text{AND}) = N$, $\deg(\text{PARITY}) = N$. Известно, что степень большинства функций равна N . Более того, было доказано, что

$$D(F) \leq 2 \deg(F)^4. \quad (6.55)$$

Это утверждение задает верхнюю границу для реализации детерминированного классического вычисления при нахождении большинства булевых функций. Расширим эту идею, вводя следующее определение. Многочлен приближает F , если $|p(X) - F(X)| \leq 1/3$ для всех $X \in \{0, 1\}^N$. Минимальную степень такого приближающего многочлена обозначим $\widetilde{\deg}F$. Подробные оценки важны в вероятностных классических вычислениях и, как мы увидим позже, в описании квантового случая. Известно, что $\widetilde{\deg}(\text{PARITY}) = N$,

$$\widetilde{\deg}(\text{OR}) \in \Theta(\sqrt{N}) \quad \text{и} \quad \widetilde{\deg}(\text{AND}) \in \Theta(\sqrt{N}); \quad (6.56)$$

кроме того,

$$D(F) \leq 216 \widetilde{\deg}(F)^6. \quad (6.57)$$

Оценки из уравнений (6.55) и (6.57) — известные оценки на момент изложения данной задачи; их доказательство выходит за рамки книги. Дальнейшую информацию о них можно получить, ознакомившись с разд. «История и дополнительная литература». По-видимому, возможны и более точные оценки, однако приведенные выше результаты вполне достаточны для наших целей.

Упражнение 6.18. Докажите, что многочлен минимальной степени, представляющий булеву функцию $F(X)$, определен однозначно.

Упражнение 6.19. Покажите, что многочлен $P(X) = 1 - (1 - X_0)(1 - X_1)\dots(1 - X_{N-1})$ представляет функцию OR.

Многочлены естественным образом возникают в описании результатов квантовых алгоритмов. Представим выход квантового алгоритма \mathcal{Q} , который выполняет T обращений к оракулу O , в виде

$$\sum_{k=0}^{2^n-1} c_k |k\rangle. \quad (6.58)$$

Покажем, что амплитуды c_k — многочлены от переменных X_0, X_1, \dots, X_{N-1} степени не выше T . Любой алгоритм \mathcal{Q} может быть представлен с использованием квантовой схемы, показанной на рис. 6.10. Состояние $|\psi_0\rangle$ непосредственно перед первым обращением к оракулу может быть записано в виде

$$|\psi_0\rangle = \sum_{i,j} (a_{i0j}|i\rangle|0\rangle + a_{i1j}|i\rangle|1\rangle)|j\rangle, \quad (6.59)$$

где первый индекс соответствует n -кубитовому результату обращения к оракулу, следующий — одному кубиту, в который оракул помещает результат обращения к нему, а последний — оставшемуся $(m - n - 1)$ рабочему кубиту, используемому алгоритмом \mathcal{Q} . После обращения к оракулу получим состояние

$$|\psi_1\rangle = \sum_{i,j} (a_{i0j}|i\rangle|X_i\rangle + a_{i1j}|i\rangle|X_i \oplus 1\rangle)|j\rangle, \quad (6.60)$$

но, поскольку X_i равняется либо 0, либо 1, можно это выражение переписать следующим образом:

$$|\psi_1\rangle = \sum_{i,j} [((1 - X_i)a_{i0j} + X_i a_{i1j})|i0\rangle + ((1 - X_i)a_{i1j} + X_i a_{i0j})|i1\rangle]|j\rangle. \quad (6.61)$$

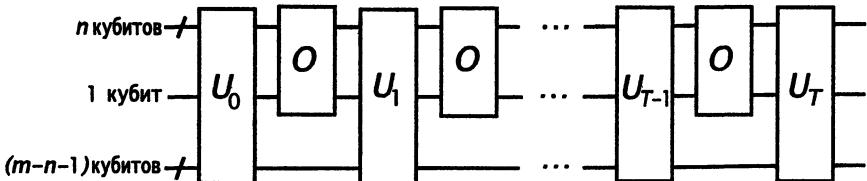


Рис. 6.10. Общая квантовая схема для квантового алгоритма, который выполняет T обращений к оракулу O . В этой схеме U_0, U_1, \dots, U_T — произвольные унитарные преобразования системы из m кубитов, а оракул действует на $(n+1)$ кубитов

Обратите внимание, что в состоянии $|\psi_0\rangle$ амплитуды состояний вычислительного базиса имели степень 0 по переменным X , в то время как для $|\psi_1\rangle$ эта степень амплитуд была равна 1 (т. е. они линейны по X). Важное наблюдение состоит в том, что никакая унитарная операция, которая выполняется в

алгоритме \mathcal{Q} до или после обращения к оракулу, не может изменить степень этих многочленов, но каждое обращение к оракулу может увеличить эту степень не более чем на единицу. Таким образом, после T обращений амплитуды представляют собой многочлены степени не выше T . Кроме того, измерение окончательного результата (6.58) в вычислительном базисе дает ответ k с вероятностью $P_k(X) = |c_k|^2$, а это действительнозначные многочлены от переменных X степени не выше $2T$.

Общая вероятность $P(X)$ получения единицы на выходе алгоритма равна сумме по некоторому подмножеству многочленов $P_k(X)$, т. е. она тоже представляет собой многочлен степени не выше $2T$. В том случае, когда алгоритм \mathcal{Q} с достоверностью выдает правильный ответ, должно выполняться равенство $P(X) = F(X)$, отсюда $\deg(F) \leq 2T$; отсюда можно сделать вывод, что

$$Q_E(F) \geq \frac{\deg(F)}{2}. \quad (6.62)$$

В случае, когда алгоритм \mathcal{Q} дает ответ с ограниченной вероятностью ошибки, можно видеть, что $P(X)$ приближает $F(X)$, поэтому $\widetilde{\deg}(F) \leq 2T$; отсюда следует неравенство

$$Q_2(F) \geq \frac{\widetilde{\deg}(F)}{2}. \quad (6.63)$$

Из оценок (6.55) и (6.62) находим соотношение

$$Q_E(F) \geq \left[\frac{D(F)}{32} \right]^{1/4}. \quad (6.64)$$

Аналогично из (6.57) и (6.63) заключаем, что,

$$Q_2(F) \geq \left[\frac{D(F)}{13824} \right]^{1/6}. \quad (6.65)$$

Это означает следующее: при вычислении булевых функций с использованием черного ящика квантовые алгоритмы могут дать в лучшем случае только полиномиальное ускорение по сравнению с классическими — и даже это не всегда возможно (поскольку $\deg(F)$ имеет порядок $\Omega(N)$ для большинства функций). В то же время известно, что $D(F) = N$, если $F = \text{OR}$, а для вероятностной классической сложности верно утверждение $R(F) \in \Theta(N)$, поэтому из оценок (6.63) и (6.56), а также известной конструкции квантового алгоритма поиска можно вывести, что $Q_2(F) \in \Theta(\sqrt{N})$. Это степенное ускорение достигается за счет квантового алгоритма поиска, а метод многочленов показывает, что результат, по-видимому, может быть обобщен на более широкий класс задач, но без дополнительного знания о структуре функции f находящегося в черном ящике оракула невозможно экспоненциальное ускорение по сравнению с классическим алгоритмом.

Упражнение 6.20. Покажите, что $Q_0(\text{OR}) \geq N$ (для этого постройте многочлен, представляющий функцию OR от выхода квантовой схемы, которая вычисляет OR с нулевой ошибкой).

Задача 6.1 (нахождение минимума). Пусть x_1, \dots, x_N — база данных из хранимых в памяти чисел (аналогичная описанной в разд. 6.5). Покажите, что на квантовом компьютере требуется только $O(\log(N)\sqrt{N})$ обращений к памяти для того, чтобы найти минимальный элемент из списка с вероятностью по крайней мере $1/2$.

Задача 6.2 (обобщенный квантовый поиск). Пусть $|\psi\rangle$ — квантовое состояние; введем определение $U_{|\psi\rangle} \equiv I - 2|\psi\rangle\langle\psi|$. Таким образом, оператор $U_{|\psi\rangle}$ меняет фазу состояния $|\psi\rangle$ на противоположную (умножает это состояние на -1), а состояния, ортогональные состоянию $|\psi\rangle$, оставляет без изменений.

1. Пусть имеется квантовая схема, реализующая такой унитарный оператор U , что $U|0\rangle^{\otimes n} = |\psi\rangle$. Объясните, как реализовать оператор $U_{|\psi\rangle}$.
2. Пусть $|\psi_1\rangle = 1$, $|\psi_2\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, $|\psi_3\rangle = (|0\rangle - i|1\rangle)/\sqrt{2}$. Допустим, что неизвестный оракул O выбирается из набора $U_{|\psi_1\rangle}$, $U_{|\psi_2\rangle}$, $U_{|\psi_3\rangle}$. Приведите квантовый алгоритм, который за одно обращение к оракулу идентифицирует его. (*Указание:* воспользуйтесь сверхплотным кодированием.)
3. **Исследование.** Рассмотрим более общий случай, когда задано k состояний $|\psi_1\rangle, \dots, |\psi_k\rangle$, а неизвестный оракул O выбирается из набора $U_{|\psi_1\rangle}, \dots, U_{|\psi_k\rangle}$. Сколько потребуется обращений к оракулу, чтобы идентифицировать его с высокой вероятностью?

Задача 6.3 (поиск по базе данных). Квантовый оракул выдает в качестве результата $|k, y \oplus X_k\rangle$, если на его вход были поданы состояние (запрос из n кубит) и один вспомогательный кубит $|y\rangle$. Покажите, что с большой вероятностью все $N = 2^n$ битов множества X могут быть получены с использованием только $N/2 + \sqrt{N}$ обращений к оракулу. Это дает общую оценку сверху $Q_2(F) \leq N/2 + \sqrt{N}$ для любого F .

Задача 6.4 (квантовый поиск и криптография). Квантовый поиск потенциально может быть использован для ускорения поиска криптографических ключей. Основная идея состоит в поиске по пространству всех возможных ключей для дешифрования, причем в каждом случае применяется ключ и осуществляется проверка, есть ли «смысл» в полученном при дешифровании сообщении. Объясните, почему эта идея «не работает» при исследовании шифра Вернама (см. разд. 12.6). В каком случае она могла быть реализована для таких систем, как DES? (Для описания системы DES см. например, [298] или [351].)

Краткое содержание главы

- **Квантовый алгоритм поиска.** Для задачи поиска с M решениями из $N = 2^n$ возможностей следует приготовить состояние $\sum_x |x\rangle$, после чего повторить $O(\sqrt{N/M})$ раз операцию $G \equiv H^{\otimes n} U H^{\otimes n} O$, где O — оракул, состояние $|x\rangle$ переводится в $-|x\rangle$, если $|x\rangle$ — решение; в противном случае это состояние не меняется; U переводит состояние $|0\rangle$ в $-|0\rangle$ и оставляет все остальные состояния вычислительного базиса неизменными. Измерение дает решение задачи поиска с высокой вероятностью.
- **Квантовый алгоритм перечисления.** Предположим, что число решений M задачи поиска неизвестно. Собственные числа оператора G равны $\exp(\pm\theta)$, где $\sin^2(\theta/2) = M/N$. Процедура оценки фазы, основанная на преобразовании Фурье, позволяет оценить M с высокой точностью, используя $O(\sqrt{N})$ обращений к оракулу. Квантовое перечисление, в свою очередь, позволяет определить, имеет ли задача поиска хотя бы одно решение, а также найти его, если решения действительно существуют, даже если их число заранее не известно.
- **Полиномиальные оценки.** Для задач, которые описываются как оценки везде определенных функций F (в отличие от частично определенных), квантовые алгоритмы в модели черного ящика могут дать не более чем полиномиальное ускорение по сравнению с классическими. В частности, $Q_2(F) \geq [D(F)/13824]^{1/6}$. Более того, реализация квантового алгоритма поиска оптимальна: она имеет скорость $\Theta(\sqrt{N})$.

История и дополнительная литература

Квантовый алгоритм поиска и его дальнейшее развитие и уточнение обязаны своим происхождением Гроверу [170], [171]. Бойер, Брассар, Хойер и Тапп [28] написали сыгравшую важную роль работу, в которой развит квантовый алгоритм поиска для случаев, когда число решений M больше единицы. Они также предложили идею квантового алгоритма перечисления, который позже был описан более подробно Брассаром, Хойером и Таппом [54]. В дальнейшем Моска [293] усовершенствовал его, используя процедуру определения собственного числа. На тот факт, что итерация Гровера может рассматриваться как произведение двух отражений, впервые было указано в обзоре Аароновой [9]. Гамильтониан (6.18) с непрерывным временем впервые исследовали Фари и Гутманн [150] (с точки зрения, отличающейся от нашей, — см. разд. 6.2). То, что алгоритм Гровера является наилучшим возможным алгоритмом поиска, основанным на использовании оракулов, было доказано Беннеттом, Бернштей-

ном, Брассаром и Вазирани [22]. Приведенный здесь вариант этого доказательства базируется на результатах, полученных Бойером, Брассаром, Хойером и Таипом [28]. Залка [430] переработал эти доказательства, чтобы показать, что квантовый алгоритм поиска асимптотически является точно оптимальным.

Метод многочленов для оценок быстродействия квантовых алгоритмов ввели в теорию квантовых вычислений Билс, Бурман, Клив и др. [25]. Превосходное обсуждение также имеется в диссертации Моски [294]; на нем построена значительная часть рассуждений разд. 6.7. Некоторое количество результатов дано в этом разделе без доказательств, приведем более точные указания, относящиеся к ним: неравенство (6.55) в [25] приписывается Нисану и Смоленскому, однако его вывод до сих пор остается неопубликованным; утверждение (6.56) получено из теоремы, доказанной Патури [313]; неравенство (6.57) приведено в [25]. В работе [25] дана лучшая оценка, чем (6.65), но она требует использования понятия *блоковой чувствительности*, которое выходит за пределы тематики, рассматриваемой в нашей книге. Совершенно другой подход к оценкам квантовых алгоритмов, использующих черный ящик, с доказательствами, основанными на запутывании, провел Амбайнис [15].

Задача 6.1 восходит к Дюрру и Хойеру [121]. Задача 6.3 представлена в работе ван Дама [398].

Глава 7

КВАНТОВЫЕ КОМПЬЮТЕРЫ: ФИЗИЧЕСКАЯ РЕАЛИЗАЦИЯ

Возможно, что в будущем компьютеры будут весить не больше 1,5 тонн.

Популярная Механика, прогнозируя стремительный марш науки, 1949

Я полагаю, что на всем мировом рынке мы не сможем продать больше пяти компьютеров.

Томас Ватсон, президент IBM, 1943

Большой интерес к теории квантовых вычислений и квантовой информации связан с надеждой на то, что устройства, обрабатывающие квантовую информацию, действительно могут быть реализованы в Природе. Иначе эта теория была бы просто математическим курьезом. Однако, экспериментальная реализация квантовых схем, алгоритмов и каналов связи оказалась чрезвычайно сложной задачей. В этой главе мы рассмотрим основные принципы, которыми следует руководствоваться при разработке устройств, обрабатывающих квантовую информацию, и изучим несколько моделей таких устройств.

В разд. 7.1 мы начнем с обзора компромиссов, на которые приходится идти при выборе физической системы для реализации квантового компьютера. Их обсуждение позволит нам в разд. 7.2 сформулировать условия, достаточные для реализации квантовых вычислений. Эти условия иллюстрируются примерами в разд. 7.3–7.7, где рассматриваются пять различных физических систем: простой гармонический осциллятор, фотоны и нелинейные оптические среды, квантовая электродинамика в резонаторах, ионы в ловушке, ядерный магнитный резонанс в молекулах. Для каждой системы кратко обсуждаются соответствующая физическая аппаратура, гамильтониан, описывающий ее динамику, способы управления системой, позволяющие выполнять квантовые вычисления, и, наконец, ее принципиальные недостатки. Физика каждой из этих систем сама по себе является отдельной наукой и ее детальное изложение не является целью данной книги. Вместо этого мы приведем лишь тот круг понятий, который является существенным для теории квантовых вычислений и информации, чтобы можно было оценить и сложности экспериментальной реализации и потенциальные возможности каждого метода. Мы также надеемся, что анализ этих систем с точки зрения квантовой теории информации будет полезным и поучительным, поскольку он позволяет чрезвычайно просто выве-

сти некоторые важные физические законы. В заключительном разд. 7.8 кратко рассматривается ряд других физических систем, которые могут использоватьсь для реализации квантовых компьютеров: квантовые точки, сверхпроводящие гранулы и спины в полупроводниках. Для удобства читателя, желающего понять лишь основную идею того или иного метода, в конце каждого раздела приводится его краткое содержание.

7.1 Основные принципы

Каким требованиям необходимо удовлетворять при реализации квантового компьютера? В разд. 1.5 мы уже упоминали, что элементарный объект нашей теории — квантовый бит, или кубит (двухуровневая квантовая система), в принципе существует в Природе. Мы также кратко обсудили его возможные физические воплощения. Для того, чтобы реализовать квантовый компьютер, мы должны не просто выбрать «хорошее» физическое представление для кубита (в котором воплощены его квантовые свойства), но и найти систему, в которой динамика кубитов управляема. Более того, мы должны уметь приготовить некоторый набор начальных состояний и измерять конечный результат.

Трудности при экспериментальной реализации связаны с тем, что, как правило, можно удовлетворить лишь какой-то части этих требований. Например, монета может находиться в двух состояниях и является хорошим представлением бита. В то же время это плохое представление кубита, поскольку суперпозиции двух состояний живут очень короткое время. Отдельный ядерный спин во внешнем магнитном поле является очень хорошим представлением кубита, поскольку суперпозиции состояний «спин вдоль поля» и «спин против поля» могут сохраняться вплоть до нескольких дней. Но создать квантовый компьютер на основе ядерных спинов очень сложно, поскольку связь отдельного спина с внешним миром слабая и измерить его ориентацию чрезвычайно трудно. Тот факт, что мы сталкиваемся с несколькими почти не совместимыми требованиями, является достаточно общим: чтобы сохранять квантовые состояния, квантовый компьютер должен быть хорошо изолирован от окружающей среды. Но в то же время его кубиты должны быть достаточно доступны, чтобы можно было выполнять вычисления и считывать результаты. При реализации квантового компьютера нужно балансировать между этими почти несовместимыми требованиями. Поэтому правильный вопрос не в том, *как* построить квантовый компьютер, а в том, *насколько хороший* квантовый компьютер возможно построить.

Какие физические системы являются перспективными с точки зрения обработки квантовой информации? При оценке перспективности той или иной системы ключевую роль играет понятие *квантового шума*, или *потери когерентности* (гл. 8), т. е. процессов, нарушающих желаемую эволюцию системы. Действительно, наибольшая длина квантового вычисления может быть грубо представлена как отношение τ_K к $\tau_{\text{оп}}$. τ_K это время, в течение которого в системе сохраняется квантовая когерентность, а $\tau_{\text{оп}}$ это длительность выполнения элементарного унитарного преобразования (действующего на небольшое

число кубитов). В действительности в большинстве систем τ_K и $\tau_{\text{оп}}$ связаны друг с другом, поскольку они определяются силой взаимодействия системы с окружающей средой. Тем не менее, отношение $\lambda = \tau_{\text{оп}}/\tau_K$ может меняться в удивительно широком диапазоне, что видно из рис. 7.1.

Система	τ_K	$\tau_{\text{оп}}$	$n_{\text{оп}} = \lambda^{-1}$
Спин ядра	$10^{-2}\text{--}10^8$	$10^{-3}\text{--}10^{-6}$	$10^5\text{--}10^{14}$
Спин электрона	10^{-3}	10^{-7}	10^4
Ионная ловушка	10^{-1}	10^{-14}	10^{13}
Электрон – Au	10^{-8}	10^{-14}	10^6
Электрон – GaAs	10^{-10}	10^{-13}	10^3
Квантовая точка	10^{-6}	10^{-9}	10^3
Оптический резонатор	10^{-5}	10^{-14}	10^9
СВЧ резонатор	10^0	10^{-4}	10^4

Рис. 7.1. Грубые оценки времени потери когерентности τ_K (сек), времени выполнения одной операции $\tau_{\text{оп}}$ (сек) и максимального числа операций $n_{\text{оп}} = \lambda^{-1} = \tau_K/\tau_{\text{оп}}$ для различных вариантов физической реализации системы взаимодействующих квантовых битов. Несмотря на большое число вариантов, даны только три принципиально различных представления кубита. спин, заряд и фотон. В ионной ловушке используются тонкие или сверхтонкие переходы в удерживаемом атоме (разд. 7.6), соответствующие перевороту спина электрона или ядра. Оценки для электронов в золоте и GaAs, а также для квантовых точек приведены для зарядового представления, при котором квантовая степень свободы описывает наличие-отсутствие дополнительного электрона на электроде или в какой-то ограниченной области. Для оптических и СВЧ резонаторов кубиты представлены фотонами (с частотой от гигагерц до сотен терагерц) различных мод резонатора. К данным оценкам следует относиться достаточно критически они дают лишь представление о перспективности того или иного метода.

Эти оценки позволяют лишь грубо оценить перспективность различных физических подходов к реализации квантового компьютера, поскольку при фактической реализации возникает много новых существенных источников шума и погрешностей. Например, если кубит представлен двумя электронными уровнями атома, и переходы между ними вызываются лазерным импульсом, то с некоторой вероятностью будут происходить переходы на неиспользуемые уровни. Такие процессы также должны рассматриваться как источник шума. Вообще, все что приводит к потере (квантовой) информации, должно рассматриваться как шум. Теория квантового шума будет более детально обсуждаться в гл. 8.

7.2 Условия для квантового вычисления

Вернемся к детальному обсуждению упомянутых в начале предыдущего раздела четырех фундаментальных требований, которым необходимо удовлетворять при проведении квантовых вычислений. Мы должны уметь:

1. адекватно представлять квантовую информацию;

2. выполнять универсальный набор унитарных преобразований;
3. приготавливать начальное состояние;
4. измерять конечный результат.

7.2.1 Представление квантовой информации

Квантовые вычисления основаны на преобразовании квантовых состояний. Квантовые биты (кубиты) представляют собой двухуровневые квантовые системы и являются элементарными «кирпичиками» для построения квантового компьютера. Поэтому нам будет удобно представлять при помощи кубитов пары базисных состояний и их физические реализации. Например, четыре состояния частицы со спином $3/2$, $|m = +3/2\rangle$, $|m = +1/2\rangle$, $|m = -1/2\rangle$ и $|m = -3/2\rangle$, могут использоваться для представления двух кубитов.

Важно понимать, что для реализации вычислений нам нужно задать лишь *конечный* набор базисных состояний. Например, координата x частицы, движущейся вдоль прямой, задает плохой набор базисных состояний для вычислений, даже если предположить, что все состояния $|x\rangle$ и любые суперпозиции $\sum_x c_x |x\rangle$ могут быть реализованы. Причина состоит в том, что x пробегает непрерывный ряд значений, пространство состояний является бесконечномерным, и в отсутствие шума количество информации, которую можно представить таким способом, бесконечно. Например, в идеальном мире все тексты Шекспира могли бы быть зашифрованы бесконечной последовательностью цифр двоичного числа $x = 0.010111011001\dots$. Очевидно, что такая ситуация совершенно нереальная, поскольку из-за наличия шума останется лишь конечное число различных состояний.

Для того, чтобы уменьшить степень потери когерентности, желательно, чтобы конечномерность пространства состояний предписывалась какой-либо симметрией. Например, состояние частицы со спином $1/2$ всегда есть линейная комбинация двух базисных векторов $|\uparrow\rangle$ и $|\downarrow\rangle$. Оно не может выйти за пределы этого двумерного пространства, и, таким образом, если частица хорошо изолирована от окружения, мы имеем почти идеальный квантовый бит.

Если выбор представления квантовой информации сделан неудачно, степень потери когерентности может стать неприемлемой. Например, во вставке 7.1 объясняется, что частица в прямоугольной яме, глубина которой достаточна для существования двух связанных состояний, была бы неудачным кубитом, поскольку возможны переходы из связанных состояний в состояния непрерывного спектра. Такие переходы разрушают состояние кубита и, следовательно, приводят к потере когерентности. Для одиночного кубита степень потери когерентности можно оценивать по минимальному времени жизни произвольной суперпозиции состояний. Например, для спинов и атомов можно использовать T_2 — время поперечной релаксации состояний типа $(|0\rangle + |1\rangle)/\sqrt{2}$. Заметим, что время продольной релаксации T_1 соответствует переходу из возбужденного состояния $|1\rangle$ в основное $|0\rangle$ и, таким образом, описывает *классическое* время жизни состояния, которое обычно больше, чем T_2 .

Вставка 7.1. Прямоугольная потенциальная яма и кубиты

Рассматриваемая система обычно называется прямоугольной потенциальной ямой и представляет собой частицу в одномерном ящике, описываемую уравнением Шредингера (2.86). Гамильтониан системы имеет вид $H = p^2/2m + V(x)$, где $V(x) = 0$ при $0 < x < L$ и $V(x) = \infty$ в противном случае. Собственные состояния в координатном представлении имеют вид

$$|\psi_n\rangle = \sqrt{\frac{2}{L}} \sin\left(\frac{n\pi}{L}x\right), \quad (7.1)$$

где n — целое число, $|\psi_n(t)\rangle = e^{-iE_nt}|\psi_n\rangle$ и $E_n = n^2\pi^2/2mL^2$. Гамильтониан, таким образом, имеет дискретный спектр. Предположим, что мы проводим эксперимент так, что можно ограничиться только двумя низшими энергетическими уровнями. Тогда произвольную волновую функцию можно записать как $|\psi\rangle = a|\psi_1\rangle + b|\psi_2\rangle$. Поскольку

$$|\psi(t)\rangle = e^{-i(E_1+E_2)/2t}[ae^{-i\omega t}|\psi_1\rangle + be^{i\omega t}|\psi_2\rangle], \quad (7.2)$$

где $\omega = (E_1 - E_2)/2$, можно рассматривать только амплитуды a и b , так что наше состояние представляется *абстрактным* двухкомпонентным вектором $|\psi\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$. Таким образом, эта двухуровневая система представляется кубитом! Какие преобразования мы можем выполнять над таким кубитом? Его эволюция во времени описывается эффективным гамильтонианом $H = \hbar\omega Z$, который может быть «выключен» переходом во врачающуюся систему отсчета. Для того, чтобы выполнять нетривиальные операции с этим кубитом, мы можем добавить к H возмущение. Посмотрим, что произойдет при добавлении к $V(x)$ возмущения

$$\delta V(x) = -V_0(t) \frac{9\pi^2}{16L} \left(\frac{x}{L} - \frac{1}{2} \right). \quad (7.3)$$

Для двухуровневой системы возмущение можно записать при помощи матричных элементов $V_{nm} = \langle\psi_n|\delta V(x)|\psi_m\rangle$, вычисление которых дает $V_{11} = V_{22} = 0$, и $V_{12} = V_{21} = V_0$. Поэтому в низшем порядке по V_0 возмущение имеет вид $H_1 = V_0(t)X$. Оно генерирует вращения вокруг оси \hat{x} . Выбирая подходящий потенциал, можно использовать аналогичный подход для выполнения других однокубитовых операций.

Итак, мы показали, как представить кубит двумя низшими состояниями в потенциальной яме и как с помощью простых возмущений потенциала реализовать однокубитовые вычислительные операции. Однако учет более высоких порядков теории возмущений, а также того обстоятельства, что реальные ямы имеют конечную глубину, приводит к тому, что начинают

играть роль более высокие энергетические уровни, и наше двухуровневое приближение перестает работать. Кроме того, в реальной жизни устройство, которое управляет потенциалом, также является квантовой системой. Взаимодействие этого устройства с системой, выполняющей вычисления, приводит к потере когерентности.

7.2.2 Реализация унитарных операторов

Эволюция замкнутой квантовой системы является унитарной и полностью определяется ее гамильтонианом. Однако, чтобы выполнять квантовые вычисления, нужно иметь возможность реализовать произвольный унитарный оператор из некоторого универсального набора (разд. 4.5). Например, манипулируя параметрами P_x и P_y , в гамильтониане $H = P_x(t)X + P_y(t)Y$, описывающем динамику отдельного спина, можно реализовать произвольные вращения этого спина (упр. 4.10).

В соответствии с теоремами разд. 4.5 произвольный унитарный оператор может быть представлен композицией спиновых вращений и операций СНОТ. Таким образом, естественно стремиться к экспериментальной реализации этих двух квантовых логических операций. При этом, однако, неявно подразумевается, что мы умеем отличать кубиты друг от друга, и в частности, применять все вышеупомянутые операции к любому выбранному кубиту или паре кубитов. Это может быть не простой задачей для многих физических систем. Например, в случае ионов в ловушке можно возбудить лазерным лучом только один выбранный ион при условии, что расстояние между ионами не меньше длины волны лазера.

Случайные погрешности при реализации унитарных операторов могут привести к потере когерентности. В гл. 8 мы увидим, что суммарный эффект случайных скачков фазы (малых вращений спина вокруг оси \hat{z}) приводит к потере квантовой информации, представленной относительными фазами. Аналогично, суммарный эффект систематических погрешностей приводит к потере когерентности, если теряется информация, необходимая для их компенсации. Далее, представление о том, что параметры гамильтониана, которыми мы манипулируем, соответствуют классическим степеням свободы, является лишь приближенным. В действительности управляющая система также является квантовой, и точный гамильтониан должен включать в себя обратное действие квантового компьютера на управляющую систему. Например, для рассмотренного выше одиночного спина управляющая система — это электромагнитное поле. Таким образом классически управляемый параметр $P_x(t)$ должен быть заменен на оператор квантового поля фотонов (если использовать гамильтониан Джейнса–Каммингса, описывающий атом–фотонное взаимодействие, то $P_x(t) = \sum_k \omega_k(t)(a_k + a_k^\dagger)$, см. подразд. 7.5.2). После взаимодействия с кубитом фотон может унести с собой информацию о его состоянии, что является источником потери когерентности.

Требования к качеству реализации унитарных операторов задаются двумя параметрами: минимальной допустимой степенью совпадения \mathcal{F} (гл. 9) и максимальным допустимым временем $t_{\text{оп}}$, необходимым для выполнения элементарной операции, например спинового вращения или операции СНОТ.

7.2.3 Приготовление начального состояния

Одним из важнейших условий проведения любого вычисления (как квантового так и классического) является возможность приготовить желаемое начальное состояние. Даже если устройство выполняет вычисления абсолютно точно, от его работы будет мало пользы, если мы не можем контролировать начальные условия. В случае классических компьютеров задание определенного начального состояния обычно не вызывает сложностей, поскольку оно представляет собой просто определенную конфигурацию электрических контактов. Однако, в квантовом случае это может стать весьма трудной задачей.

Заметим, что достаточно уметь с большой точностью приготавливать какое-либо одно начальное состояние, поскольку любое другое получается из него при помощи унитарного оператора. Например в случае n спинов нас вполне устроит начальное состояние $|00\dots 0\rangle$. Может оказаться, что время жизни этого состояния не достаточно велико, но это уже другой вопрос, связанный с выбором представления квантовой информации.

Для большинства физических систем приготовление начального состояния представляет собой большую проблему. Например, ионы в ловушке могли бы быть приведены в основное состояние путем охлаждения (разд. 7.6), но практически осуществить это сложно. Для физических систем, реализующих ансамбли квантовых компьютеров, возникают дополнительные неприятности. Например, в случае ЯМР-реализации (разд. 7.7), каждая из молекул должна рассматриваться как отдельный квантовый компьютер. Чтобы получить сигнал, который можно измерить, требуется достаточно много молекул. Нужно, чтобы кубиты в каждой из молекул были приготовлены в одном и том же состоянии. Это непросто, поскольку энергии состояний $|0\rangle$ и $|1\rangle$ различаются на $\hbar\omega$, что много меньше, чем $k_B T$. С другой стороны, после того как установится термодинамическое равновесие состояние системы будет больцмановским с матрицей плотности $\rho \approx e^{-\mathcal{H}/k_B T}/Z$, где Z — нормировочный множитель, определяемый из условия $\text{tr}(\rho)=1$.

Качество приготовленного начального состояния характеризуется степенью совпадения \mathcal{F} между требуемым начальным состоянием ρ и фактически приготовленным состоянием, а также энтропией состояния ρ . Роль энтропии становится понятной на примере состояния $\rho = I/2^n$. Даже если мы умеем приготавливать состояние ρ с большой степенью совпадения, его вычислительная ценность невелика, поскольку оно не меняется при действии унитарных операторов! В идеальном случае начальное состояние является чистым и энтропия равна нулю. Если входное состояние имеет ненулевую энтропию, процедура извлечения ответа из конечного состояния вообще говоря усложнится.

7.2.4 Измерение конечного результата

Какие измерения понадобятся нам для квантовых вычислений? Удобно рассматривать измерение как процесс взаимодействия одного или более кубитов с классической системой. Это взаимодействие происходит на некотором интервале времени, по истечении которого состояние классической системы указывает нам на результат измерения. Например, измерение состояния кубита $a|0\rangle + b|1\rangle$, представленного основным и возбужденным состояниями двухуровневого атома, могло бы быть реализовано наблюдением флюoresценции. Если на выходе фотоумножителя регистрируется сигнал, значит флюoresценция имела место, и при измерении кубит был спроектирован на состояние $|1\rangle$. Вероятность такого исхода равна $|b|^2$. В противном случае никакого сигнала не регистрируется, а кубит проецируется на состояние $|0\rangle$.

Для квантовых вычислений важен процесс редукции волновой функции, происходящий при проективном измерении (подразд. 2.2.5). Хороший квантовый алгоритм дает на выходе суперпозицию состояний, которая позволяет при измерениях с большой вероятностью получить интересующий нас ответ. Например, в алгоритме Шора разложения на простые множители на каждом шаге требуется найти целое число r , исходя из того, что результат измерения является целым числом вида qc/r , где q — размерность пространства состояний. Хотя на выходе мы имеем суперпозицию состояний, в которой все возможные c представлены приблизительно с равными амплитудами, в процессе измерения эта суперпозиция случайным образом редуцируется к какому-то конкретному c . В результате мы можем с большой вероятностью определить r (используя цепные дроби, как объяснялось в гл. 5).

Можно представить себе множество трудностей, связанных с реализацией измерений; например, в схеме, описанной выше, несовершенство фотоумножителей и тепловой шум в усилителе могут исказить информацию об измеренном состоянии кубита. Кроме того, как правило, очень трудно осуществить проективные измерения (иногда называемые «сильными» измерениями), поскольку для этого требуется сильное и регулируемое взаимодействие между квантовой и классической системами. Измерения также не должны выполняться тогда, когда это не требуется; в противном случае они будут источником потери когерентности.

Удивительно, однако, что сильные измерения не являются необходимыми; для квантовых вычислений могут быть полезны и слабые измерения, выполняемые непрерывно на протяжении вычисления. Их можно использовать, если время взаимодействия с измерительным устройством велико по сравнению с временем вычисления и если используются большие ансамбли квантовых компьютеров. Суммарный сигнал, полученный от такого ансамбля, является макроскопически наблюдаемой величиной и несет информацию о квантовом состоянии. Заметим, что использование ансамблей порождает новые трудности. Например, если в алгоритме разложения на множители результатом измерения будет число $q\langle c \rangle / r$, где $\langle c \rangle$ — среднее значение c , этот алгоритм станет непригодным, поскольку $\langle c \rangle$ не должно быть целым (и значит разложение в цепные

дроби невозможно). К счастью, можно видоизменить квантовый алгоритм так, что он станет работать при измерениях с ансамблями. Мы обсудим этот вопрос в разд. 7.7.

О качестве измерения можно судить по отношению сигнала к шуму. Оно дает представление о характерной амплитуде сигнала, определяемой силой взаимодействия измерительного устройства с квантовой системой.

7.3 Гармонический осциллятор как модель квантового компьютера

Перед тем как продолжить описание физической модели реализуемого квантового компьютера, мы сделаем небольшое отступление, в котором рассмотрим чрезвычайно простую систему — гармонический осциллятор — и обсудим причины, по которым эта система не может быть хорошей моделью квантового компьютера. Формализм, развитый в этом примере, послужит основой для изучения других физических систем.

7.3.1 Физическая аппаратура

Примером простого гармонического осциллятора является частица в параболической потенциальной яме $V(x) = m\omega^2x^2/2$. В классической механике это может быть груз на пружине, совершающий колебания по мере того как потенциальная энергия пружины переходит в кинетическую энергию груза и обратно. Это также может быть электрический колебательный контур, в котором энергия распределена между емкостью и индуктивностью. В этих примерах полная энергия системы может принимать непрерывный ряд значений.

В квантовой механике, которая начинает работать, когда связь системы с внешним миром очень мала, полная энергия системы может принимать дискретный набор значений. Например полная энергия одной моды электромагнитного поля в резонаторе с большой добротностью Q кратна (с точностью до постоянного сдвига) величине $\hbar\omega$, определяемой фундаментальной постоянной \hbar и частотой моды ω .

Для простого гармонического осциллятора собственные состояния с определенной энергией будут обозначаться как $|n\rangle$, где $n = 0, 1, \dots, \infty$. Для квантовых вычислений мы должны выбрать конечное подмножество этих состояний, представляющее кубиты. Время жизни кубитов будет определяться физическими параметрами, например добротностью резонатора Q , которая может быть сделана очень большой увеличением коэффициента отражения стенок. Чтобы применить унитарный оператор, нужно дать системе эволюционировать в течение некоторого времени при определенных условиях. Однако, как станет ясно ниже, эта схема имеет недостатки. Мы начнем с описания гамильтонiana системы, а затем обсудим, как можно реализовать простые квантовые логические операции, например CNOT.

7.3.2 Гамильтониан

Гамильтониан частицы в одномерном параболическом потенциале имеет вид

$$H = \frac{p^2}{2m} + \frac{1}{2}m\omega^2x^2, \quad (7.4)$$

где p — импульс частицы, m — масса, x — координата и ω — параметр потенциала. Напомним, что x и p являются операторами в этом выражении (вставка 7.2), которое можно записать в виде

$$H = \hbar\omega \left(a^\dagger a + \frac{1}{2} \right), \quad (7.5)$$

где a^\dagger и a — повышающий и понижающий операторы, определенные как

$$a = \frac{1}{\sqrt{2m\hbar\omega}} (m\omega x + ip), \quad (7.6)$$

$$a^\dagger = \frac{1}{\sqrt{2m\hbar\omega}} (m\omega x - ip). \quad (7.7)$$

Вставка 7.2. Квантовый гармонический осциллятор

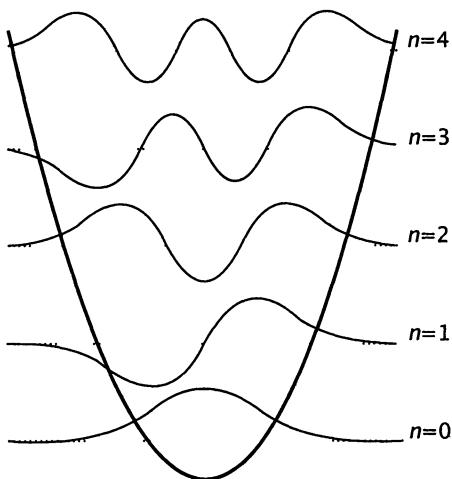
Гармонический осциллятор является чрезвычайно важным и полезным понятием при квантовом описании физической картины мира. Для понимания его свойств полезно определить собственные состояния гамильтониана (7.4). Их можно найти непосредственным решением уравнения Шröдингера

$$\frac{\hbar^2}{2m} \frac{d^2\psi_n(x)}{dx^2} + \frac{1}{2}m\omega^2x^2\psi_n(x) = E\psi_n(x) \quad (7.8)$$

относительно координатных волновых функций $\psi_n(x)$ и собственных значений E , с граничными условиями $\psi(x) \rightarrow 0$ при $x = \pm\infty$ и нормировкой $\int |\psi(x)|^2 = 1$. Пять первых решений уравнения Шröдингера графически изображены ниже.

Хотя подобные графики дают интуитивное представление о поведении системы в координатном пространстве, чаще всего нас будут интересовать абстрактные алгебраические свойства состояний. А именно, предположим, что $|\psi\rangle$ удовлетворяет (7.8) с энергией E . Определяя операторы a и a^\dagger в соответствии с (7.6)–(7.7) и используя то, что $[H, a^\dagger] = \hbar\omega a^\dagger$, находим

$$Ha^\dagger|\psi\rangle = ([H, a^\dagger] + a^\dagger H)|\psi\rangle \quad (7.9)$$



Эти функции описывают амплитуду вероятности того, что частица будет обнаружена в той или иной точке в области действия потенциала. Это значит, что $a^\dagger|\psi\rangle$ является собственным состоянием гамильтониана H с энергией $E + \hbar\omega$. Аналогично $a|\psi\rangle$ является собственным состоянием с энергией $E - \hbar\omega$. По этой причине a^\dagger и a называются повышающим и понижающим операторами. Состояние $(a^\dagger)^n|\psi\rangle$ соответствует собственному значению $E + n\hbar\omega$. Таким образом, имеется бесконечно много собственных состояний с эквидистантным энергетическим спектром и расположением между уровнями $\hbar\omega$. Кроме того, поскольку H — положительно определенный оператор, должно существовать состояние $|\psi_0\rangle$, для которого $a|\psi_0\rangle = 0$. Это основное состояние, соответствующее наименьшему собственному значению H . Введенный формализм адекватно описывает основные свойства квантового гармонического осциллятора и позволяет использовать удобное обозначение $|n\rangle$ для собственных состояний. При этом n — целое число и $H|n\rangle = \hbar(n + 1/2)|n\rangle$. В этой главе обозначения $|n\rangle$, a и a^\dagger будут встречаться довольно часто, так как гармонический осциллятор является моделью многих физических систем.

Энергия нулевых колебаний $\hbar\omega/2$ приводит к появлению ненаблюдаемого общего фазового множителя, которым мы можем пренебречь.

Собственные состояния $|n\rangle$ гамильтониана H имеют следующие свойства:

$$a^\dagger a|n\rangle = n|n\rangle, \quad (7.10)$$

$$a^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle, \quad (7.11)$$

$$a|n\rangle = \sqrt{n}|n-1\rangle, \quad (7.12)$$

где $n = 0, 1, \dots, \infty$. Ниже мы увидим, что взаимодействие с гармоническим осциллятором удобно описывать, добавляя к гамильтониану слагаемые, содержащие a и a^\dagger , а взаимодействие между двумя осцилляторами — при помощи слагаемых вида $a_1^\dagger a_2 + a_2^\dagger a_1$. В этом разделе, однако, мы ограничимся случаем одного осциллятора.

Упражнение 7.1. Используя коммутатор $[x, p] = i\hbar$, покажите, что $a^\dagger a = H/\hbar\omega - \frac{1}{2}$.

Упражнение 7.2. Используя коммутатор $[x, p] = i\hbar$, найдите $[a, a^\dagger]$.

Упражнение 7.3. Найдите коммутатор $[H, a]$. Используя полученный результат, покажите, что если $|\psi\rangle$ — собственное состояние H с энергией $E \geq n\hbar\omega$, то $a^n|\psi\rangle$ — собственное состояние с энергией $E - n\hbar\omega$.

Упражнение 7.4. Покажите, что $|n\rangle = \frac{(a^\dagger)^n}{\sqrt{n!}}|0\rangle$.

Упражнение 7.5. Проверьте, что выражения (7.11) и (7.12) согласуются с формулой (7.10) и условием нормировки $\langle n|n \rangle = 1$.

Собственные состояния эволюционируют во времени согласно уравнению Шредингера (2.86). В частности, если начальное состояние $|\psi(0)\rangle = \sum_n c_n |n\rangle$, то

$$|\psi(t)\rangle = e^{-iHt/\hbar} |\psi(0)\rangle = \sum_n c_n e^{-in\omega t} |n\rangle. \quad (7.13)$$

Мы будем предполагать, что можно точно приготовить произвольное начальное состояние осциллятора, выполнять проективные измерения (подразд. 2.2.3), но взаимодействие осциллятора с окружающей средой отсутствует.

7.3.3 Квантовые вычисления

Попробуем использовать простой гармонический осциллятор, описанный выше, для квантовых вычислений. Кубиты наиболее естественно представляются энергетическими собственными состояниями $|n\rangle$. Как при таком представлении реализовать операцию CNOT? Напомним, что действие этой операции на двухкубитовые базисные состояния имеет вид

$$\begin{aligned} |00\rangle_L &\rightarrow |00\rangle_L \\ |01\rangle_L &\rightarrow |01\rangle_L \\ |10\rangle_L &\rightarrow |11\rangle_L \\ |11\rangle_L &\rightarrow |10\rangle_L, \end{aligned} \quad (7.14)$$

Здесь индекс L указывает на то, что речь идет о логических состояниях, а не о состояниях осциллятора. Мы можем закодировать эти два кубита следующим образом:

$$\begin{aligned} |00\rangle_L &= |0\rangle \\ |01\rangle_L &= |2\rangle \\ |10\rangle_L &= (|4\rangle + |1\rangle)/\sqrt{2} \\ |11\rangle_L &= (|4\rangle - |1\rangle)/\sqrt{2}. \end{aligned} \quad (7.15)$$

Предположим, в момент $t = 0$ состояние системы является линейной комбинацией векторов $|0\rangle, |1\rangle, |2\rangle, |4\rangle$. Допустим, что система эволюционирует в течение времени $t = \pi/\hbar\omega$. При этом собственные состояния преобразуются по закону $|n\rangle \rightarrow \exp(-i\pi a^\dagger a)|n\rangle = (-1)^n|n\rangle$, поэтому состояния $|0\rangle, |2\rangle, |4\rangle$ остаются неизменными, а состояние $|1\rangle$ меняет знак. В результате для логических состояний получается искомое преобразование СНОТ.

В общем случае необходимым и достаточным условием того, что с помощью данной физической системы можно реализовать унитарный оператор U , является приближенное равенство собственных значений оператора U и оператора эволюции $T = \exp(-iHt)$, определяемого гамильтонианом H . В рассмотренном выше случае оператор СНОТ имел только два собственных значения $+1$ и -1 . Нам удалось выбрать кодировку, при которой оператор эволюции осциллятора имеет такие же собственные значения. Можно реализовать практически любой спектр собственных значений, если добавить к гамильтониану гармонического осциллятора подходящее возмущение. Кроме того, используя достаточно много базисных состояний осциллятора, можно закодировать произвольное число кубитов. Таким образом, может показаться, что квантовый компьютер реализуется при помощи простого гармонического осциллятора!

7.3.4 Недостатки

Конечно, метод, предложенный выше, имеет много недостатков. Спектр собственных значений унитарного оператора, выполняющего данное квантовое вычисление, нам, вообще говоря, неизвестен, даже если мы знаем как представить этот оператор композицией элементарных операций. В действительности для большинства задач, имеющих квантовые алгоритмы решения, знание спектра собственных значений равносильно знанию ответа задачи!

Очевидно также, что описанный подход нельзя применить, чтобы выполнить два вычисления одно за другим, так как собственные значения композиции двух унитарных операторов не выражаются через собственные значения каждого из них.

Другой очевидный недостаток идеи использования гармонического осциллятора для квантовых вычислений состоит в том, что при этом не применяется принцип цифрового представления информации. При отображении 2^n мерного пространства в пространство состояний гармонического осциллятора нам придется использовать состояния с энергией $2^n\hbar\omega$. Заметим, что при использовании n двухуровневых квантовых систем максимальная энергия была бы $n\hbar\omega$. Подобным образом, в классическом случае можно использовать либо шкалу с 2^n делениями, либо регистр из n классических битов. Квантовые вычисления основаны на цифровом представлении информации, а не на аналоговом.

Основные черты квантового компьютера, реализованного на основе гармонического осциллятора, приводятся ниже (подобное резюме мы будем делать для каждой рассматриваемой системы в конце соответствующего раздела). На этом мы заканчиваем рассмотрение отдельных осцилляторов и переходим к следующей теме — системам гармонических осцилляторов, состоящих из фотонов и атомов.

Гармонический осциллятор как модель квантового компьютера

- **Представление кубита.** Состояния с определенной энергией $|0\rangle, |1\rangle, \dots, |2^n\rangle$ одиночного гармонического осциллятора задают n кубитов.
- **Унитарная эволюция.** Для реализации унитарного оператора U необходимо сопоставить каждому собственному значению оператора U собственное значение оператора эволюции $\exp(-ita^\dagger a)$.
- **Приготовление начального состояния.** Не рассматривалось.
- **Измерение конечного результата.** Не рассматривалось.
- **Недостатки.** Не цифровое представление информации. Кроме того, сопоставление собственных значений произвольного оператора U неосуществимо, поскольку в общем случае они неизвестны.

7.4 Квантовый компьютер на оптических фотонах

Привлекательной физической системой для представления квантового бита является оптический фотон. Фотоны являются нейтральными частицами, достаточно слабо взаимодействующими друг с другом и с материей. Их можно практически без потерь переносить на большие расстояния по оптическому волокну, задерживать при помощи фазовращателей и создавать суперпозиции их состояний при помощи светоделителей. Фотоны демонстрируют основополагающие квантовые явления, например интерференцию на двух щелях. Кроме того, в нелинейных средах может иметь место фотон-фотонное взаимодействие, которое возникает благодаря нелинейному взаимодействию фотонов с веществом. Хотя схема с использованием фотонов и неидеальна, изучение этой модели квантового компьютера, ее деталей, архитектуры и недостатков является поучительным.

7.4.1 Физическая аппаратура

Мы начнем с рассмотрения одиночных фотонов, обсудим, как с их помощью представлять квантовую информацию, и опишем экспериментальную аппаратуру для управления фотонами, в частности фазовращатели, светоделители и керровские среды.

Как можно представить кубиты, используя фотоны? При обсуждении гармонического осциллятора мы уже упоминали, что энергия электромагнитного поля в резонаторе квантуется в единицах $\hbar\omega$. Каждый такой квант энергии называется фотоном. Естественно, резонатор может находиться в суперпозиции состояния с одним фотоном и основного состояния, что дает нам представление

кубита $c_0|0\rangle + c_1|1\rangle$. Однако, мы будем иметь в виду нечто иное. Рассмотрим систему из двух резонаторов, в которой имеется двукратно вырожденная фотонная мода с частотой $\hbar\omega$. Два базисных состояния кубита соответствуют одному фотону, находящемуся в первом резонаторе ($|01\rangle$), и одному фотону, находящемуся во втором резонаторе ($|10\rangle$). Состояние кубита, таким образом, представляется в виде $c_0|01\rangle + c_1|10\rangle$. Мы будем называть такое представление *двойственным*. Для наглядности будем рассматривать одиночные фотоны как волновые пакеты, движущиеся в свободном пространстве, а не в резонаторе; можно представить себе, что резонатор движется вместе с волновым пакетом. Роль резонаторов сводится к формированию двух различных пространственных мод.

Один из экспериментальных способов генерации одиночных фотонов состоит в ослаблении излучения, испускаемого лазером. Лазер излучает так называемое когерентное состояние $|\alpha\rangle$, определенное как

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle, \quad (7.16)$$

где $|n\rangle$ — состояние, в котором резонансная мода заселена n фотонами. Когерентное состояние достаточно хорошо изучено в квантовой оптике и обладает многими замечательными свойствами. Их описание, однако, выходит за рамки данной книги. Достаточно упомянуть, что когерентные состояния возникают естественным образом при описании излучения системы осцилляторов в случае, когда инверсия превышает порог генерации. Заметим, что средняя энергия равна $\langle\alpha|n|\alpha\rangle = |\alpha|^2$. В результате ослабления когерентное состояние переходит в когерентное состояние с меньшим α , что позволяет с большой вероятностью получить однофотонное состояние.

Упражнение 7.6 (собственные состояния понижающего оператора). Докажите, что когерентное состояние является собственным состоянием понижающего оператора, т. е., что $a|\alpha\rangle = \lambda|\alpha\rangle$ для некоторой λ .

Например, при $\alpha=\sqrt{0,1}$ имеем состояние $\sqrt{0,90}|0\rangle + \sqrt{0,09}|1\rangle + \sqrt{0,002}|2\rangle + \dots$. Таким образом, на выходе аттенюатора одиночный фотон будет получен с вероятностью больше 95%, а вероятность ошибки составит 5%. Заметим также, что в 90% случаев через аттенюатор не пройдет ни один фотон. Это значит, что полученный источник имеет интенсивность всего 0,1 фотона за единицу времени. Кроме того, мы не можем определить (по какому-то классическому сигналу), когда фотон был испущен, а когда нет. Поэтому нельзя синхронизировать два таких источника.

Лучшей синхронизации можно достичь, используя технику параметрического понижения частоты. Для этого фотоны с частотой ω_0 пропускаются через нелинейную оптическую среду типа KH_2PO_4 , что приводит к генерации фотонных пар на резонансных частотах $\omega_1 + \omega_2 = \omega_0$ с сохранением импульса $\vec{k}_1 + \vec{k}_2 = \vec{k}_3$. Если детектор зарегистрировал (с разрушением состояния) одиночный фотон ω_2 , то мы узнаем о существовании одиночного фотона ω_1 (рис. 7.2). Установив на выходе дополнительный селектор, открывающийся

лишь в том случае, когда детектор зарегистрировал один фотон (а не два или более), мы получим источник одиночных фотонов. Можно синхронизировать во времени несколько таких источников, подбирая правильную задержку во времени для каждой моды. Точность синхронизации определяется разрешающей способностью детектора и селектора.

Существует довольно много способов детектирования одиночных фотонов в широком спектральном диапазоне с большой квантовой эффективностью. Для нас наиболее важна способность детектора с большой вероятностью правильно определить, имеется ли на данной пространственной моде нуль фотонов или один фотон. При использовании двойственного представления это эквивалентно проективным измерениям в вычислительном базисе. На практике несовершенство детектора уменьшает вероятность правильной регистрации одиночного фотона. Вероятность того, что одиночный фотон, падающий на детектор, создаст пару носителей зарядов (фотопару), которая даст вклад в фототок, называется *квантовой эффективностью* и обозначается как η ($0 \leq \eta \leq 1$). Детектор также характеризуется своей полосой пропускания (временем отклика), уровнем шума и «темновым» током, обусловленным генерацией фотопар даже при отсутствии падающих на него фотонов.

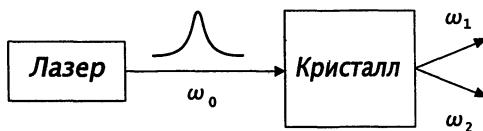


Рис. 7.2. Схема генерации одиночных фотонов методом параметрического понижения частоты

Экспериментальная техника для управления состояниями фотонов включает три важных компонента: зеркала, фазовращатели и светоделители. Зеркала с большим коэффициентом отражения отражают фотоны и изменяют направление распространения фотона в пространстве. Зеркало, в котором теряется менее 0,01% фотонов, является вполне обычным прибором. Фазовращатель представляет собой просто прозрачную пластинку, показатель преломления n которой отличается от показателя преломления вакуума n_0 . Например, показатель преломления обычного боро-силикатного стекла в оптическом диапазоне $n \approx 1,5n_0$. При прохождении фотона через пластинку толщины L его фаза изменяется на e^{ikL} , где $k = n\omega/c_0$ и c_0 — скорость света в вакууме. Таким образом, фотон, прошедший через пластинку, приобретет фазу $e^{i(n-n_0)L\omega/c_0}$ по сравнению с фотоном, прошедшим то же расстояние в вакууме.

Светоделитель представляет собой частично посеребренное стекло с коэффициентом отражения R и коэффициентом пропускания $1 - R$. Экспериментально светоделитель обычно изготавливается в виде сандвича из двух призм и тонкого металлического слоя между ними, как показано на рис. 7.3. Удобно описывать светоделитель при помощи угла θ , определенного как $\cos(\theta) = R$ (подчеркнем, что этот угол характеризует степень отражения и

может не иметь ничего общего с геометрией светоделителя). Два входа и два выхода светоделителя связаны соотношениями

$$a_{\text{вых}} = a_{\text{вх}} \cos \theta + b_{\text{вх}} \sin \theta, \quad (7.17)$$

$$b_{\text{вых}} = -a_{\text{вх}} \sin \theta + b_{\text{вх}} \cos \theta, \quad (7.18)$$

где под a и b понимаются классические амплитуды электромагнитного поля двух лучей. Здесь мы использовали нестандартный выбор фаз, который, однако, более удобен для наших целей. В специальном случае 50/50 светоделителя мы имеем $\theta = 45^\circ$.

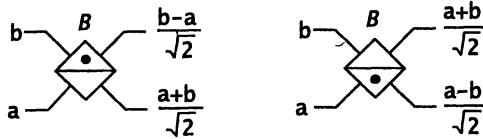


Рис. 7.3. Схематическое изображение оптического светоделителя. Показаны два входных и выходных канала, а также проиллюстрировано соглашение о выборе фаз для 50/50 светоделителя ($\theta = 45^\circ$). Два изображенных светоделителя являются взаимно обратными (графически они различаются при помощи точки внутри квадрата). Соотношения между операторами двух мод a и b на входе и на выходе приведены для случая $\theta = \pi/4$.

Как известно из нелинейной оптики, показатель преломления n некоторых веществ зависит от полной интенсивности излучения I по закону

$$n(I) = n + n_2 I. \quad (7.19)$$

Это явление известно как оптический эффект Керра и имеет место (очень слабо) в таких распространенных веществах как стекло или сахарный сироп. В легированных стеклах n_2 меняется от 10^{-14} до $10^{-7} \text{ см}^2/\text{Вт}$, а в полупроводниках от 10^{-10} до 10^2 . Представим себе эксперимент, в котором через такую среду распространяются два луча света одинаковой интенсивности, а их пути почти совпадают. При этом в случае одновременного прохождения двух лучей каждый из них приобретет дополнительную фазу $e^{i n_2 I L \omega / c_0}$. Это было бы очень хорошо, если бы длину пути L можно было сделать сколь угодно большой. К сожалению, это невозможно, поскольку среды, в которых имеет место эффект Керра, сильно поглощают свет и, кроме того, излучение рассеивается в другие пространственные моды. Как мы увидим в подразд. 7.4.3, это является главным препятствием для реализации квантового компьютера при помощи одиночных фотонов.

Мы переходим далее к квантовому описанию перечисленных выше оптических устройств.

7.4.2 Квантовые вычисления

Если квантовая информация закодирована при помощи оптического фотона в двойственном представлении $c_0|01\rangle + c_1|10\rangle$, то, используя фазовращатели, све-

тоделители и среду Керра, можно реализовать произвольное унитарное преобразование. Чтобы показать, как это делается, мы опишем квантовомеханический гамильтониан для каждого используемого оптического устройства.

Как мы видели в подразд. 7.3.2, динамика одной моды электромагнитного поля в резонаторе моделируется с помощью квантового гармонического осциллятора. При этом $|0\rangle$ — вакуумное состояние, $|1\rangle$ — однофотонное состояние, $|n\rangle = (n!)^{-1/2} (a^\dagger)^n |0\rangle$ — состояние с n фотонами. Здесь a^\dagger обозначает оператор рождения фотона на данной моде. В свободном пространстве динамика описывается гамильтонианом

$$H = \hbar\omega a^\dagger a. \quad (7.20)$$

Применяя формулу (7.13), мы заключаем, что состояние $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$ эволюционирует как $|\psi(t)\rangle = c_0|0\rangle + c_1 e^{-i\omega t}|1\rangle$. Отсюда сразу видно преимущество двойственного представления: в свободном пространстве эволюция состояния $|\varphi\rangle = c_0|01\rangle + c_1|10\rangle$ сводится к изменению общей фазы, которая ненаблюдаема. Таким образом, на подпространстве состояний двойственного представления свободный гамильтониан обращается в нуль.

Фазовращатель. Действие фазовращателя сводится к эффективному замедлению моды излучения, проходящей сквозь него. Это связано с уменьшением скорости света в среде, имеющей больший показатель преломления, а именно, время, за которое свет пройдет расстояние L в среде с показателем преломления n больше, чем соответствующее время в вакууме на $\Delta \equiv (n - n_0)L/c_0$. Обозначим через P оператор эволюции, описывающий прохождение света через фазовращатель. Тогда действие P на вакуумное состояние тривиально: $P|0\rangle = |0\rangle$, тогда как для однофотонного состояния мы имеем $P|1\rangle = e^{i\Delta}|1\rangle$.

В двойственном представлении P осуществляет полезную логическую операцию. Расположив фазовращатель на пути одной из двух мод, мы задержим вращение ее фазы по отношению к второй моде, прошедшей то же самое расстояние в вакууме. Таким образом, двойственное состояние $c_0|01\rangle + c_1|10\rangle$ перейдет в $c_0 e^{-i\Delta/2}|01\rangle + c_1 e^{i\Delta/2}|10\rangle$ с точностью до несущественного общего фазового множителя. Заметим (разд. 4.2), что если представить логические состояния как $|0\rangle_L = |01\rangle$, $|1\rangle_L = |10\rangle$, то эта операция представляет собой просто вращение вокруг оси \hat{z} , т. е.

$$R_z(\Delta) = e^{-iZ\Delta/2}, \quad (7.21)$$

где Z — матрица Паули σ^z . Поэтому можно считать, что P описывает эволюцию с гамильтонианом

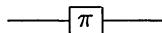
$$H = (n_0 - n)Z, \quad (7.22)$$

в течение времени L/c_0 , т. е. $P = \exp(-iHL/c_0)$.

Упражнение 7.7. Покажите что приведенная ниже схема преобразует двойственные состояния как

$$|\psi_{\text{вых}}\rangle = \begin{bmatrix} e^{i\pi} & 0 \\ 0 & 1 \end{bmatrix} |\psi_{\text{вх}}\rangle, \quad (7.23)$$

если считать, что на схеме верхний и нижний каналы соответствуют модам $|01\rangle$ и $|10\rangle$, а квадратик обозначает фазовый сдвиг на π :



Заметим, что подобные «оптические схемы» наглядно показывают картину распространения фотона в пространстве, а задание оператора эволюции, соответствующего схеме, сводится к заданию некоторой фазы для каждого из квадратиков, так же как на приведенном рисунке. В двойственном представлении свободная эволюция в соответствии с (7.20) изменяет лишь ненаблюдаемую общую фазу состояния, поэтому нам достаточно следить лишь за изменением относительной фазы.

Упражнение 7.8. Покажите, что $P|\alpha\rangle = |\alpha e^{i\Delta}\rangle$, где α — когерентное состояние (вообще, параметр α является комплексным).

Светофильтр. Эволюцию фотонных состояний при наличии светофильтра также можно описать феноменологически, но нам будет удобнее начать с гамильтониана и, исходя из этого, описать ожидаемое классическое поведение, т. е. вывести выражения (7.17)-(7.18). Напомним, что светофильтр действует на две фотонные моды, которые мы будем описывать при помощи операторов рождения a^\dagger, b^\dagger и уничтожения a, b . Гамильтониан имеет вид

$$H_{bs} = i\theta(ab^\dagger - a^\dagger b), \quad (7.24)$$

а унитарный оператор, описывающий прохождение света через светофильтр,

$$B = \exp[i\theta(ab^\dagger - a^\dagger b)]. \quad (7.25)$$

В дальнейшем нам понадобятся выражения для сопряженного действия B на операторы a и b :

$$BaB^\dagger = a \cos \theta + b \sin \theta \quad \text{и} \quad BbB^\dagger = -a \sin \theta + b \cos \theta. \quad (7.26)$$

Мы проверим эти соотношения при помощи формулы Бейкера–Кэмпбелла–Хаусдорфа (см. также упр. 4.49)

$$e^{\lambda G} A e^{-\lambda G} = \sum_{n=0}^{\infty} \frac{\lambda^n}{n!} C_n, \quad (7.27)$$

где λ — комплексное число, A, G — операторы, причем C_n определены рекурсивной последовательностью коммутаторов $C_0 = A, C_1 = [G, C_0], C_2 = [G, C_1], C_3 = [G, C_2], \dots, C_n = [G, C_{n-1}]$. В силу коммутационных соотношений $[a, a^\dagger] = 1, [b, b^\dagger] = 1$ имеем: $[G, a] = -b$ и $[G, b] = a$, где $G \equiv a^\dagger b - ab^\dagger$, что дает нам разложение оператора BaB^\dagger в ряд с коэффициентами $C_0 = a, C_1 = [G, a] = -b, C_2 = [G, C_1] = -a, C_3 = [G, C_2] = -[G, C_0] = b$ или в общем виде

$$C_n \text{ четн} = i^n a, \quad (7.28)$$

$$C_n \text{ нечетн} = i^{n+1} b. \quad (7.29)$$

Выражение для BaB^\dagger теперь находится элементарно:

$$BaB^\dagger = e^{\theta G} a e^{-\theta G} \quad (7.30)$$

$$= \sum_{n=0}^{\infty} \frac{\theta^n}{n!} C_n \quad (7.31)$$

$$= \sum_{n \text{ четн}} \frac{(i\theta)^n}{n!} a + i \sum_{n \text{ нечетн}} \frac{(i\theta)^n}{n!} b \quad (7.32)$$

$$= a \cos \theta - b \sin \theta. \quad (7.33)$$

Выражение для BbB^\dagger получится, если в приведенных выше формулах поменять местами a и b . Заметим, что вид оператора, описывающего действие светофильтра, определяется связью между светофильтром и алгеброй $SU(2)$, как объясняется во вставке 7.3.

В терминах квантовых логических элементов B осуществляет полезную операцию. Прежде всего заметим, что $B|00\rangle = |00\rangle$, т. е. если ни на одной из входных мод фотонов нет, то их не будет ни на одной из выходных мод. Если на входе имеется один фотон на моде a , то, используя $|1\rangle = a^\dagger|0\rangle$, находим

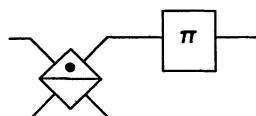
$$B|01\rangle = Ba^\dagger|00\rangle = Ba^\dagger B^\dagger B|00\rangle = (a^\dagger \cos \theta + b^\dagger \sin \theta)|00\rangle = \cos \theta|01\rangle + \sin \theta|10\rangle. \quad (7.34)$$

Аналогично $B|10\rangle = \cos \theta|10\rangle - \sin \theta|01\rangle$. Таким образом, в базисе $|0_L\rangle, |1_L\rangle$ можно записать B как

$$B = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix} = e^{i\theta Y}. \quad (7.35)$$

Используя фазовращатели и светофильтры, можно действовать на оптический кубит произвольным унитарным оператором. Это следует из теоремы 4.1, которая утверждает, что все однокубитовые операции можно реализовать с помощью вращений вокруг осей \hat{z} и \hat{y} , т. е. операторов $R_z(\alpha) = \exp(-i\alpha Z/2)$ и $R_y(\alpha) = \exp(-i\alpha Y/2)$. Действительно, фазовращатель реализует R_z , а светофильтр реализует R_y .

Упражнение 7.9 (оптический элемент Адамара). Покажите, что приведенная ниже схема в двойственном представлении реализует элемент Адамара, т. е. $|01\rangle \rightarrow (|01\rangle + |10\rangle)/\sqrt{2}$ и $|10\rangle \rightarrow (|01\rangle - |10\rangle)/\sqrt{2}$, с точностью до общего фазового множителя.



Упражнение 7.10 (интерферометр Цендера–Маха). Интерферометр является оптическим инструментом для измерения малых разностей фаз и может быть сконструирован из двух светофильтров. Данное упражнение иллюстрирует основные принципы работы интерферометра.

Вставка 7.3. Симметрия $SU(2)$ и квантовый светоделитель

Существует интересная связь между группой Ли $SU(2)$ и алгеброй двух связанных гармонических осцилляторов, которая поясняет смысл преобразования, реализуемого светоделителем. Установим следующее соответствие:

$$a^\dagger a - b^\dagger b \rightarrow Z, \quad (7.36)$$

$$a^\dagger \rightarrow \sigma_+, \quad (7.37)$$

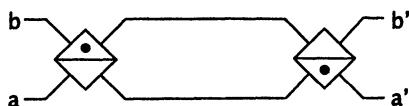
$$ab^\dagger \rightarrow \sigma_-, \quad (7.38)$$

где Z — матрица Паули и $\sigma_{\pm} = (X \pm iY)/2$ — повышающий и понижающий операторы, образованные из матриц Паули X и Y . Исходя из коммутационных соотношений для операторов a , a^\dagger , b и b^\dagger , можно легко проверить что выполняются коммутационные соотношения для матриц Паули, см. (2.40). Заметим, что оператор полного числа частиц $a^\dagger a + b^\dagger b$ коммутирует с σ_z , σ_+ и σ_- , что можно увидеть из его инвариантности относительно вращений $SU(2)$. Используя матрицы Паули $X = a^\dagger b + ab^\dagger$ и $Y = -i(a^\dagger b - ab^\dagger)$ и записывая произвольный элемент $SU(2)$ в виде

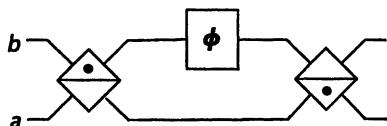
$$R(\hat{n}, \theta) = e^{-i\theta\vec{\sigma}\cdot\hat{n}/2}, \quad (7.39)$$

можно получить желаемое выражение для оператора эволюции при наличии светоделителя, взяв направление \hat{n} вдоль оси \hat{y} .

- Покажите, что приведённая ниже схема выполняет тождественное преобразование.



- В двойственном представлении найдите вращение, реализуемое приведенной ниже схемой, как функцию сдвига фазы φ .



Упражнение 7.11. Найдите $B|2,0\rangle$ для $\theta = \pi/4$.

Упражнение 7.12 (квантовый светоделитель с классическим входом). Найдите $B|\alpha\rangle|\beta\rangle$, где $|\alpha\rangle$ и $|\beta\rangle$ — два когерентных состояния, см. (7.16). (Указание: Используйте то, что $|n\rangle = \frac{(a^\dagger)^n}{\sqrt{n!}}|0\rangle$.)

Нелинейные керровские среды. Наиболее важный эффект, наблюдаемый в нелинейных средах, состоит в перекрестной фазовой модуляции между двумя различными модами излучения. При классическом описании в (7.19) появляется член n_2 , который описывает эффективное фотон-фотонное взаимодействие. Промежуточным звеном в этом взаимодействии являются атомы нелинейной среды. Квантовый гамильтониан, описывающий эффект Керра, имеет вид

$$H_{\text{xpm}} = -\chi a^\dagger a b^\dagger b, \quad (7.40)$$

где a и b — операторы уничтожения для двух мод излучения, распространяющегося в нелинейной среде. Соответственно, при прохождении света сквозь кристалл длины L квантовое состояние преобразуется унитарным оператором

$$K = e^{i\chi L a^\dagger a b^\dagger b}. \quad (7.41)$$

Коэффициент χ связан с n_2 , а также с нелинейной восприимчивостью $\chi^{(3)}$. В упр. 7.14 читателю предлагается проверить, что гамильтониан (7.40) действительно приводит к классическому эффекту Керра (7.19).

При помощи среды Керра и светоделителей можно реализовать операцию СНОТ. Преобразование однофотонных состояний в среде Керра имеет вид

$$K|00\rangle = |00\rangle, \quad (7.42)$$

$$K|01\rangle = |01\rangle, \quad (7.43)$$

$$K|10\rangle = |10\rangle, \quad (7.44)$$

$$K|11\rangle = e^{i\chi L}|11\rangle. \quad (7.45)$$

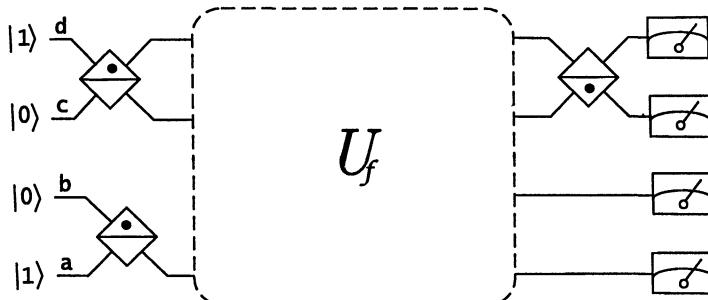
Выбор $\chi L = \pi$ дает $K|11\rangle = -|11\rangle$. Два логических кубита в двойственном представлении задаются четырьмя фотонными модами, так что рабочее пространство порождается четырьмя базисными состояниями $|e_{00}\rangle = |1001\rangle$, $|e_{01}\rangle = |1010\rangle$, $|e_{10}\rangle = |0101\rangle$, $|e_{11}\rangle = |0110\rangle$. Обратите внимание, что для удобства мы поменяли местами две фотонные моды, представляющие первый кубит (физически такая перестановка осуществляется с помощью зеркал). Допустим, что мы пропускаем вторую и третью моды через среду Керра. В этом случае $K|e_i\rangle = |e_i\rangle$ для всех i за исключением $K|e_{11}\rangle = -|e_{11}\rangle$. Это почти то, что нам нужно, поскольку операция СНОТ может быть записана как

$$\underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}}_{U_{CN}} = \frac{1}{\sqrt{2}} \underbrace{\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}}_{I \otimes H} \\
 \times \underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}}_{K} \frac{1}{\sqrt{2}} \underbrace{\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}}_{I \otimes H}, \quad (7.46)$$

где H — однокубитовый элемент Адамара (который просто реализуется с использованием светоделителей и фазовращателей), а K — преобразование Керра с $\chi L = \pi$, о котором упоминалось выше. Аналогичное устройство рассматривалось ранее с целью построения обратимого классического логического элемента (см. вставку 7.4). В однофотонном режиме такое устройство функционирует как квантовый логический элемент.

Итак, элемент CNOT может быть сконструирован с помощью среды Керра и произвольных однокубитовых операций, реализуемых светоделителями и фазовращателями. Одиночные фотоны могут генерироваться лазерами с аттенюаторами и регистрироваться фотодетекторами. Это значит, что теоретически на основе оптических элементов может быть реализован квантовый компьютер.

Упражнение 7.13 (квантовая оптическая схема Дойча–Йожа). В подразд. 1.4.4 была описана квантовая схема, решающая задачу Дойча–Йожа для одного бита. Ниже приведена оптическая версия этой схемы, работающая на однофотонных состояниях (в двойственном представлении) с использованием светоделителей, фазовращателей и среды Керра.

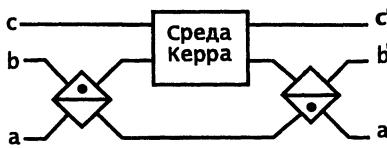


- Постройте схемы для четырех возможных классических функций U_f , используя элементы Фредкина и светоделители.

2. Почему в этих схемах можно обойтись без фазовращателей?
3. Для каждой функции U_f покажите, как с помощью интерференции можно объяснить работу квантового алгоритма.
4. Будет ли работать эта оптическая схема, если вместо однофотонных состояний использовать когерентные состояния?

Вставка 7.4. Квантовый оптический элемент Фредкина

Оптический элемент Фредкина можно построить с помощью среды Керра и двух светоделителей, как показано на приведенной ниже схеме:



Эта схема реализует унитарный оператор $U = B^\dagger K B$, где B — 50/50 светоделитель, $K = e^{i\xi b^\dagger b c^\dagger c}$ — оператор перекрестной фазовой модуляции, описывающий среду Керра, а $\xi = \chi L$ произведение константы взаимодействия и длины керровской ячейки. После упрощения имеем

$$U = \exp \left[i\xi c^\dagger c \left(\frac{b^\dagger - a^\dagger}{2} \right) \left(\frac{b - a}{2} \right) \right] \quad (7.47)$$

$$= e^{i\frac{\pi}{2} b^\dagger b} e^{\frac{\xi}{2} c^\dagger c (a^\dagger b - b^\dagger a)} e^{-i\frac{\pi}{2} b^\dagger b} e^{i\frac{\xi}{2} a^\dagger a c^\dagger c} e^{i\frac{\xi}{2} b^\dagger b c^\dagger c}. \quad (7.48)$$

В произведении (7.48) первый и третий сомножители представляют одномодовые фазовые сдвиги, а четвертый и пятый — керровские операторы перекрестной фазовой модуляции. Эти эффекты для нас не интересны и могут быть скомпенсированы. Наиболее интересен второй сомножитель, который и определяет квантовый элемент Фредкина,

$$F(\xi) = \exp \left[\frac{\xi}{2} c^\dagger c (a^\dagger b - b^\dagger a) \right]. \quad (7.49)$$

Обычный (классический) элемент Фредкина получается при $\xi = \pi$. В этом случае мы имеем на выходе $a' = a$, $b' = b$, если на моде c не было фотонов, и $a' = b$, $b' = a$, если на моде c был один фотон. Можно также отметить, что $F(\chi)$ напоминает оператор светоделителя с классическим управлением, причем угол поворота равен $\xi c^\dagger c$. Обратите внимание, что здесь не используется двойственное представление; в двойственном представлении построенный элемент Фредкина соответствовал бы элементу СНОТ.

Упражнение 7.14 (классическая перекрестная фазовая модуляция). Чтобы убедиться, что классические свойства среды Керра действительно вытекают из определения оператора K (см. формулу (7.41)), подействуем этим оператором на две моды, одна из которых находится в когерентном состоянии, а другая в состоянии $|n\rangle$. Покажите, что

$$K|\alpha\rangle|n\rangle = |\alpha e^{i\chi L_n}\rangle|n\rangle. \quad (7.50)$$

Используя полученный результат, проверьте, что

$$\rho_a = \text{Tr}[K|\alpha\rangle|\beta\rangle\langle\beta|\langle\alpha|K] \quad (7.51)$$

$$= e^{-|\beta|^2} \sum_m \frac{|\beta|^{2m}}{m!} |\alpha e^{i\chi L_m}\rangle\langle\alpha e^{i\chi L_m}|, \quad (7.52)$$

и убедитесь, что главный вклад в сумму дает $m = |\beta|^2$.

7.4.3 Недостатки

Представление кубита при помощи одиночных фотонов весьма привлекательно. Их сравнительно легко генерировать и детектировать. В двойственном представлении можно реализовать произвольный однокубитовый оператор. К сожалению, обеспечить взаимодействие между фотонами гораздо труднее — в самых лучших керровских средах взаимодействие слишком слабое, чтобы получить перекрестную фазовую модуляцию порядка π между однофотонными состояниями. Кроме того, поскольку нелинейность как правило имеет место вблизи оптического резонанса, эффект Керра неизбежно будет сопровождаться поглощением света. Теоретические оценки показывают, что на один прошедший сквозь среду фотон (т. е. подвергшийся перекрестной фазовой модуляции) приходится примерно 50 поглощенных фотонов. Это означает что в рамках современной нелинейной оптики построение квантового компьютера имеет очень мало шансов на успех.

Тем не менее, обсуждение оптического квантового компьютера дало нам представление об его *архитектуре* и системном устройстве. Теперь мы знаем, как мог бы выглядеть реальный лабораторный квантовый компьютер (конечно при условии, что в нашем распоряжении есть компоненты, отвечающие всем требованиям). Замечательно также, что его почти полностью можно построить из оптических интерферометров. Квантовая информация хранится в фазе и в числе заполнения фотонной моды, причем интерферометры позволяют переходить от одного представления к другому. Хотя построение стабильных оптических интерферометров вполне возможно, при использовании в качестве представления кубита массивной частицы это сразу станет очень сложной задачей из-за малости длины волны де Броиля. В то же время даже при оптическом представлении кубита для реализации квантовых алгоритмов потребуются оптические схемы, состоящие из большого числа интерферометров, для стабилизации которых нужно приложить много усилий.

Исторически оптические классические компьютеры сначала задумывались как многообещающая замена для электронных устройств. Однако, связанные с ними надежды в конце концов угасли, поскольку не удалось получить материалы с высокой степенью нелинейности, а также потому, что сложности с юстировкой и энергозатраты не компенсировались преимуществами в скорости и возможностью параллельных вычислений. С другой стороны, оптическая передача информации чрезвычайно важная область, например, по той причине, что энергия, необходимая для передачи бита информации на расстояние больше одного сантиметра по оптическому волокну, меньше, чем энергия, расходуемая при передаче информации по проводам. Может оказаться, что оптические кубиты найдут применение для передачи квантовой информации, например в квантовой криптографии, а не в квантовых вычислениях.

Несмотря на недостатки оптической реализации квантового компьютера, формальная теория, описывающая ее, является фундаментом для всех остальных реализаций рассматриваемых далее в этой главе. В следующем разделе мы обсудим несколько иной вариант оптического квантового компьютера, в котором используется другая (лучшая!) нелинейная среда.

Квантовый компьютер на оптических фотонах

- **Представление кубита.** Один фотон, который может находиться на двух модах $|01\rangle$ и $|10\rangle$ (или с двумя поляризациями).
- **Унитарная эволюция.** Произвольный оператор можно реализовать с помощью фазовращателей (вращения R_z), светоделителей (вращения R_y) и нелинейной среды Керра, в которой имеет место перекрестная фазовая модуляция (оператор вида $\exp[i\chi L|11\rangle\langle 11|]$).
- **Приготовление начального состояния.** Генерация однофотонных состояний (например, путем ослабления лазерного излучения).
- **Измерение конечного результата.** Детектирование одиночных фотонов (например, в фотоумножителе).
- **Недостатки.** Трудно реализовать нелинейную среду Керра с большой константой перекрестной фазовой модуляции и с малым коэффициентом поглощения.

7.5 Квантовая электродинамика в оптических резонаторах

В квантовой электродинамике резонаторов (КЭДР) рассматривается задача о взаимодействии отдельных атомов с небольшим числом оптических фотонных мод. Такое взаимодействие становится возможным, когда отдельные атомы помещаются в оптический резонатор с большой добротностью Q . Если в резонаторе имеется всего одна или две оптические моды, а напряженность

электрического поля достаточно велика, то становится существенным взаимодействие этих мод с дипольным моментом атома. При больших Q возможны процессы, в которых фотон успевает много раз вступить во взаимодействие с атомом прежде чем покинуть резонатор. Подобная экспериментальная техника замечательна тем, что позволяет изучать отдельные квантовые системы и манипулировать ими. Она также предоставляет много возможностей для теории квантового хаоса, квантовой обратной связи и квантовых вычислений.

В частности, использование техники КЭДР позволяет преодолеть основное препятствие к реализации оптического квантового компьютера, о котором шла речь в предыдущем разделе. Проблема была в том, что хотя оптические фотоны являются отличными носителями квантовой информации, взаимодействовать друг с другом они могут только в веществе. В обычных ячейках Керра вещество заполняет макроскопический объем и эффекты поглощения света играют доминирующую роль. В случае одиночных атомов этот недостаток отсутствует, хотя одиночные атомы также приводят к перекрестной фазовой модуляции фотонных мод. Можно попытаться также использовать одиночные фотоны, чтобы переносить квантовое состояние с одного атома на другой. Рассмотрение этого метода является целью настоящего раздела.

7.5.1 Физическая аппаратура

Экспериментальная установка для КЭДР включает два компонента: электромагнитный резонатор и атом. Мы начнем с описания элементарной физики резонаторов, а затем приведем некоторые факты о строении атомов и о взаимодействии атомов с фотонами.

Резонатор Фабри–Перо

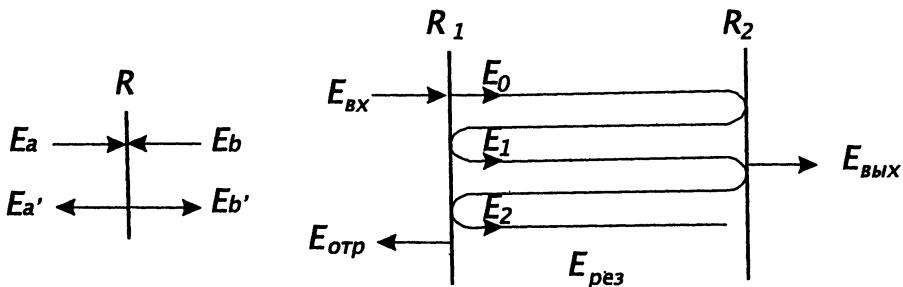
Наиболее важным взаимодействием в КЭДР является дипольное взаимодействие $\vec{d} \cdot \vec{E}$ между электрическим дипольным моментом \vec{d} и электрическим полем E . Насколько сильным может быть это взаимодействие? Дипольный момент \vec{d} фиксирован и менять его мы не можем; однако величина $|\vec{E}|$ зависит от постановки эксперимента. Если мы хотим получить большую напряженность поля в узком спектральном диапазоне и в маленьком участке пространства, удобно использовать резонатор Фабри–Перо.

Вставка 7.5. Резонатор Фабри–Перо

Основной частью резонатора Фабри–Перо является частично посеребренное зеркало, на котором происходят процессы отражения и прохождения падающих лучей E_a и E_b . В результате на выходе получаются лучи $E_{a'}$ и $E_{b'}$. Эти процессы описываются унитарным преобразованием

$$\begin{bmatrix} E_{a'} \\ E_{b'} \end{bmatrix} = \begin{bmatrix} \sqrt{R} & \sqrt{1-R} \\ \sqrt{1-R} & -\sqrt{R} \end{bmatrix} \begin{bmatrix} E_a \\ E_b \end{bmatrix}, \quad (7.53)$$

где R — коэффициент отражения зеркала. Выбор позиции для знака минус является неоднозначным и был сделан из соображений удобства. Резонатор Фабри–Перо состоит из двух параллельных зеркал с коэффициентами отражения R_1 и R_2 , на которые падает луч $E_{\text{вх}}$, (см. рисунок).



Внутри резонатора луч испытывает последовательные отражения между двумя зеркалами, приобретая дополнительную фазу $e^{i\varphi}$ в результате каждого полного цикла вперед–назад. Фаза φ является функцией длины пути и частоты света. Таким образом, используя формулу (7.53), можно записать поле внутри резонатора в виде

$$E_{\text{рез}} = \sum_k E_k = \frac{\sqrt{1 - R} E_{\text{вх}}}{1 + e^{i\varphi} \sqrt{R_1 R_2}}, \quad (7.54)$$

где $E_0 = \sqrt{1 - R_1} E_{\text{вх}}$, $E_k = -e^{i\varphi} \sqrt{R_1 R_2} E_{k-1}$. Аналогично вычисляются поля $E_{\text{вых}} = e^{i\varphi/2} \sqrt{1 - R_2} E_{\text{рез}}$ и $E_{\text{отр}} = \sqrt{R_1} E_{\text{вх}} + \sqrt{1 - R_1} \sqrt{R_2} e^{i\varphi} E_{\text{рез}}$. Наиболее важной для нас характеристикой резонатора Фабри–Перо является зависимость плотности энергии внутри резонатора от плотности энергии во входном излучении и от частоты света:

$$\frac{P_{\text{рез}}}{P_{\text{вх}}} = \left| \frac{E_{\text{рез}}}{E_{\text{вх}}} \right|^2 = \frac{1 - R_1}{|1 + e^{i\varphi} \sqrt{R_1 R_2}|^2}. \quad (7.55)$$

Следует отметить два момента. Во-первых, зависимость от φ проявляется в частотной избирательности резонатора, поскольку $\varphi = \omega d/c$, где d — расстояние между зеркалами, c — скорость света, а ω — частота света. Физически избирательность является следствием интерференции поля внутри резонатора и поля, отраженного от переднего зеркала. Во-вторых, при резонансной частоте, когда амплитуда поля внутри резонатора максимальна, отношение (7.55) оказывается приблизительно равным $1/(1 - R)$. Это свойство очень ценно с точки зрения применений в КЭДР.

Используя приближение, в котором электрическое поле содержит только одну гармонику, мы можем записать оператор напряженности электрического поля в виде

$$\vec{E}(r) = -\tilde{\epsilon} E_0 [ae^{ikr} - a^\dagger e^{-ikr}], \quad (7.56)$$

где $k = \omega/c$ — волновое число, E_0 — напряженность поля, $\tilde{\epsilon}$ — поляризация, r — пространственная координата, a^\dagger и a — фотонные операторы рождения и уничтожения, рассмотренные в подразд. 7.4.2. Во вставке 7.5 доказывается что это приближение адекватно описывает поле в резонаторе Фабри–Перо. Гамильтониан, описывающий динамику поля в резонаторе, имеет вид

$$H_{\text{поля}} = \hbar\omega a^\dagger a, \quad (7.57)$$

что вполне согласуется с классической формулой, согласно которой энергия есть интеграл от $|\vec{E}|^2$ по объему.

Упражнение 7.15. Нарисуйте график отношения (7.55) как функции фазы φ для $R_1 = R_2 = 0,9$.

Двухуровневый атом

До сих пор в этой главе речь шла или о свободных фотонах, или о фотон–фотонных взаимодействиях типа перекрестной фазовой модуляции, которые возникали при распространении фотонов в квазиклассической среде. Сейчас мы приступим к рассмотрению атомов, их электронной структуры и взаимодействия с фотонами. Разумеется, это чрезвычайно обширная тема и мы опишем лишь ту ее часть, которая важна для квантовых вычислений.

Электронные состояния и спектры атомов могут быть очень сложными (вставка 7.6), однако для наших целей достаточно использовать приближение, в котором атом имеет только два электронных состояния. Такое приближение *двухуровневого атома* оказывается приемлемым, поскольку мы имеем дело с монохроматическим излучением. В этом случае существенными являются лишь уровни, удовлетворяющие двум условиям: разность их энергий равна энергии падающего фотона и симметрия (правила отбора) не запрещает переход между уровнями. Эти ограничения связаны с законами сохранения энергии, углового момента и четности. Сохранение энергии выражается уравнением

$$\hbar\omega = E_2 - E_1, \quad (7.58)$$

где E_1 и E_2 — два уровня энергии атома. Условия сохранения углового момента и четности можно проиллюстрировать, рассмотрев матричный элемент \hat{r} между двумя орбитальными волновыми функциями, $\langle l_1, m_1 | \hat{r} | l_2, m_2 \rangle$. Без потери общности можно считать, что \hat{r} лежит в плоскости $\hat{x} - \hat{y}$. Тогда вектор \hat{r} можно разложить по сферическим гармоникам (вставка 7.6):

$$\hat{r} = \sqrt{\frac{3}{8\pi}} [(-r_x + ir_y)Y_{1,+1} + (r_x + ir_y)Y_{1,-1}]. \quad (7.59)$$

В этом базисе матричный элемент $\langle l_1, m_1 | \hat{r} | l_2, m_2 \rangle$ сводится к интегралу от сферических гармоник:

$$\int Y_{l_1 m_1}^* Y_{l_2 m_2} d\Omega, \quad (7.60)$$

где $m = \pm 1$. Данный интеграл отличен от нуля только при $m_2 - m_1 = \pm 1$ и $\Delta l = \pm 1$. Первое условие выражает сохранение углового момента, а второе — сохранение четности (оно имеет такой вид лишь в дипольном приближении, где существенны матричные элементы $\langle l_1, m_1 | \hat{r} | l_2, m_2 \rangle$). Эти два условия задают правила отбора, которые должны приниматься во внимание в модели двухуровневого атома.

Упражнение 7.16 (правила отбора в дипольном приближении). Покажите, что интеграл (7.60) отличен от нуля только при $m_2 - m_1 = \pm 1$ и $\Delta l = \pm 1$.

Вставка 7.6. Атомные уровни энергии

Электроны атома могут рассматриваться как система частиц в трехмерном ящике с гамильтонианом вида

$$H_A = \sum_k \frac{|\vec{p}_k|^2}{2m} - \frac{Ze^2}{r_k} + H_r + H_{ee} + H_{so} + H_{hf}, \quad (7.61)$$

где первый член — кинетическая энергия электронов, второй член — кулоновское притяжение электронов к положительному заряженному ядру, H_r — релятивистские поправки, H_{ee} описывает электрон-электронное взаимодействие и поправки связанные с тем, что электроны являются фермионами, H_{so} — спин орбитальное взаимодействие, которое можно интерпретировать как взаимодействие электронного спина с магнитным полем, создаваемым орбитальным движением электрона, H_{hf} соответствует сверхтонкой структуре, т. е. взаимодействию спина электрона с магнитным полем ядра. Собственные состояния H_A , как правило, хорошо классифицируются тремя целыми числами (*квантовыми числами*): n — главное квантовое число, l — орбитальный момент и m — его проекция на ось \hat{z} . Кроме того, часто важны полный спин электронов S и ядерный спин I . Собственные значения H_A в основном порядке определяются числом n , члены H_r и H_{so} приводят к поправкам порядка α^2 , а член H_{hf} приводит к поправкам порядка $10^{-3}\alpha^2$, где $\alpha = 1/137$ — постоянная тонкой структуры.

Число n задает решение одномерного уравнения Шрёдингера подобно тому, как это было для частицы в одномерном ящике, поскольку кулоновский потенциал зависит только от радиуса. Однако орбитальный момент l является специфической чертой квантования в трехмерном пространстве, как объясняется ниже. Чтобы понять его свойства, заметим, что в координатном представлении H_A кинетическая энергия пропорциональна оператору Лапласа. Угловая зависимость собственных функций оператора описывается уравнением Лапласа

$$\frac{\Phi(\varphi)}{\sin \theta} \frac{d}{d\theta} \left(\sin \theta \frac{d\Theta}{d\theta} \right) + \frac{\Theta(\theta)}{\sin^2 \theta} \frac{d\Phi(\varphi)}{d\varphi^2} + l(l+1)\Theta(\theta)\Phi(\varphi) = 0, \quad (7.62)$$

где θ и φ — обычные сферические координаты, а Φ и Θ — интересующие нас собственные функции. Решения этого уравнения $Y_{lm}(\theta, \varphi) = \Theta_{lm}(\theta)\Phi_m(\varphi)$ называются *сферическими гармониками* и имеют вид

$$Y_{lm}(\theta, \varphi) \equiv (-1)^m \sqrt{\frac{2l+1}{4\pi} \frac{(l-m)!}{(l+m)!}} P_{lm}(\cos \theta) e^{im\varphi}, \quad (7.63)$$

где P_{lm} — присоединенные полиномы Лежандра:

$$P_{lm}(x) = \frac{(1-x^2)^{m/2}}{2^l l!} \frac{d^{m+l}}{dx^{m+l}} (x^2 - 1)^l. \quad (7.64)$$

В этих уравнениях подразумевается что $-l \leq m \leq l$, причем можно показать, что допустимы только целые l и m . Число l — орбитальный момент, а m — его проекция на ось \hat{z} . Аналогично определяются проекции m_s и m_i для электронного S и ядерного I спинов. Итак, хотя описать собственные состояния атома очень сложно, для наших целей можно считать, что они классифицируются семью числами: n, l, m, S, m_s, I, m_i .

На практике электромагнитное поле никогда не бывает *идеально* монохроматичным; например, если оно генерируется лазером, конечная ширина линии возникает за счет продольных мод, шума в сигнале накачки и других источников. Точно также атом, взаимодействующий с окружающим миром, не имеет *идеально* определенных уровней энергии; малые возмущения, связанные с флуктуациями электрического потенциала, и даже взаимодействие с вакуумом приводят к размыванию уровня энергии до конечной ширины.

Тем не менее, для специально выбранных атомов и возбужденных состояний с учетом правил отбора приближение двухуровневого атома работает превосходно. В этом приближении оказывается, что, если $|\psi_1\rangle$ и $|\psi_2\rangle$ — два выбранных уровня, то матричные элементы \hat{r} имеют вид

$$r_{ij} = \langle \psi_i | \hat{r} | \psi_j \rangle \approx r_0 Y, \quad (7.65)$$

где r_0 — некоторая константа, а Y — матрица Паули (для последующих вычислений нам удобно фиксировать систему координат так, чтобы в выражении (7.65) была матрица Y), см. подразд. 2.1.3. Это позволит нам описать взаимодействие атома с приложенным к нему электрическим полем. Атомный гамильтониан, действующий на подпространстве двух выбранных уровней, имеет вид

$$H_{\text{атом}} = \frac{\hbar\omega_0}{2} Z. \quad (7.66)$$

Здесь $\hbar\omega_0$ — разность энергий выбранных уровней.

7.5.2 Гамильтониан

Взаимодействие $\vec{d} \cdot \vec{E}$ между атомом и электрическим полем в резонаторе можно описывать, используя приближение двухуровневого атома, простейшую схему квантования поля в резонаторе, и считая что радиус орбиты электрона много меньше длины волны излучения. Замечая, что $\vec{d} \sim \hat{r}$ (дипольный момент равен произведению заряда на расстояние) и принимая во внимание формулы (7.56), (7.65), получаем следующий гамильтониан взаимодействия:

$$H_I = -igY(a - a^\dagger). \quad (7.67)$$

Здесь мы считаем, что атом находится в точке $r = 0$ (соответственно в этой же точке вычисляется поле \vec{E}), плоскость поляризации поля задается ортами \hat{x}, \hat{y} , а g — некоторая константа (нас пока не будут интересовать числовые значения), описывающая силу взаимодействия. Коэффициент i появился, поскольку мы считаем g вещественной, а гамильтониан H_I должен быть эрмитовым.

При определенных условиях мы можем упростить гамильтониан H_I . Чтобы увидеть это, введем понижающие и повышающие матрицы Паули

$$\sigma_{\pm} = \frac{X \pm iY}{2}, \quad (7.68)$$

с помощью которых H_I записывается как

$$H_I = g(\sigma_+ - \sigma_-)(a - a^\dagger). \quad (7.69)$$

Приближение *врачающейся волны* заключается в том, чтобы отбросить члены $\sigma_+ a^\dagger$ и $\sigma_- a$, соответствующие удвоенным частотам. Оказывается, что иногда это приближение работает достаточно хорошо. В результате полный гамильтониан $H = H_{\text{атом}} + H_{\text{поле}} + H_I$ принимает вид

$$H = \frac{\hbar\omega_0}{2}Z + \hbar\omega a^\dagger a + g(a^\dagger \sigma_- + a \sigma_+). \quad (7.70)$$

Напомним, что здесь матрицы Паули действуют в пространстве состояний двухуровневого атома, a^\dagger и a — операторы рождения и уничтожения для одной моды электромагнитного поля, ω — частота моды, ω_0 — частота перехода атома, g — константа связи, описывающая взаимодействие атома с полем. Выражение (7.70) представляет собой гамильтониан Джейнса–Каммингса взаимодействия двухуровневых атомов с электромагнитным полем и является основным инструментом в теории КЭДР.

Этот гамильтониан можно записать в более удобной форме, введя интеграл движения $N = a^\dagger a + Z/2$, $[H, N] = 0$, а именно

$$H = \hbar\omega N + \delta Z + g(a^\dagger \sigma_- + a \sigma_+). \quad (7.71)$$

Здесь $\delta = (\omega_0 - \omega)/2$ определяет разность между частотами поля и атомного резонанса. Этот параметр обычно называется *расстройкой*. Гамильтониан

Джейнса–Каммингса чрезвычайно важен для нас, и значительная часть данной главы будет посвящена изучению его свойств и описанию с его помощью различных физических систем.

Упражнение 7.17 (собственные состояния гамильтониана Джейнса–Каммингса). Покажите, что состояния

$$|\chi_n\rangle = \frac{1}{\sqrt{2}} [|n, 1\rangle + |n+1, 0\rangle], \quad (7.72)$$

$$|\bar{\chi}_n\rangle = \frac{1}{\sqrt{2}} [|n, 1\rangle - |n+1, 0\rangle] \quad (7.73)$$

являются собственными для гамильтониана Джейнса–Каммингса (7.71) в случае $\omega = \delta = 0$, а соответствующие им собственные значения имеют вид

$$H|\chi_n\rangle = g\sqrt{n+1}|\chi_n\rangle, \quad (7.74)$$

$$H|\bar{\chi}_n\rangle = -g\sqrt{n+1}|\bar{\chi}_n\rangle. \quad (7.75)$$

В этих формулах обозначения состояний следует понимать как |поле, атом〉.

7.5.3 Поглощение и преломление для одиночного фотона и одиночного атома

Нас будет интересовать КЭДР в режиме, когда *одиночный* фотон взаимодействует с *одиночным* атомом. Это квантовый режим, в котором традиционные понятия классической теории электромагнетизма (такие, как показатель преломления или диэлектрическая проницаемость) перестают работать. Нам хотелось бы использовать одиночный атом, чтобы получить нелинейное фотон–фотонное взаимодействие.

Мы начнем с обсуждения удивительного и фундаментального эффекта, наблюдаемого в системе атом–поле и называемого *осцилляции Раби*. Можно сразу выбросить k из гамильтониана (7.71) слагаемое N , поскольку от него зависит только общая фаза. Оператор эволюции имеет вид $U = e^{-iHt}$ (здесь и далее будем полагать $\hbar = 1$). Если ограничиться однофотонными состояниями, то можно записать гамильтониан как

$$H = \begin{bmatrix} \delta & 0 & 0 \\ 0 & \delta & g \\ 0 & g & -\delta \end{bmatrix}, \quad (7.76)$$

где базисные состояния $|00\rangle$, $|10\rangle$, $|01\rangle$ расположены в порядке сверху вниз и слева направо (напомним, что левая цифра относится к полю, а правая к ато-

му). Соответственно оператор эволюции принимает следующий вид:

$$\begin{aligned} U = & e^{-i\delta t}|00\rangle\langle 00| \\ & + (\cos \Omega t + i\frac{\delta}{\Omega} \sin \Omega t)|01\rangle\langle 01| \\ & + (\cos \Omega t - i\frac{\delta}{\Omega} \sin \Omega t)|10\rangle\langle 10| \\ & - i\frac{g}{\Omega} \sin \Omega t(|01\rangle\langle 10| + |10\rangle\langle 01|). \end{aligned} \quad (7.77)$$

Особый интерес представляет последняя строка этой формулы. Из нее мы видим, что атом и поле периодически обмениваются одним квантом энергии с частотой Раби $\Omega = \sqrt{g^2 + \delta^2}$.

Упражнение 7.18 (осцилляции Раби). Используя формулу

$$e^{i\vec{n}\cdot\vec{\sigma}} = \sin |n|_i \hat{n} \cdot \vec{\sigma} \cos |n| \quad (7.78)$$

для вычисления экспоненты от H , проверьте справедливость выражения (7.77). Заметим, что данный способ описания осцилляций Раби и получения частоты Раби значительно проще, чем стандартный, в котором для нахождения Ω необходимо решать систему дифференциальных уравнений. При нашем подходе удается описать всю существенную динамику, используя только однофотонные состояния и одиночный атом.

Если нас интересует, как преобразуется состояние фотона при взаимодействии с атомом, мы должны взять частичный след по состояниям атома (подразд. 2.4.3). Вероятность того, что фотон поглотится атомом при начальном состоянии поля $|1\rangle$ и начальном состоянии атома $|0\rangle$, есть

$$\chi_r = \sum_k |\langle 0k|U|10\rangle|^2 = \frac{g^2}{g^2 + \delta^2} \sin^2 \Omega t. \quad (7.79)$$

Это обычный лоренцевский контур, описывающий поглощение света как функцию расстройки δ .

Показатель преломления (одиночного атома!) определяется теми матричными элементами U , в которых конечное состояние атома основное. Сдвиг фазы фотона в этом процессе равен разности фаз, которые они приобрели в ходе эволюции состояний $|0\rangle$ и $|1\rangle$. Этот сдвиг оказывается равным

$$\chi_i = \arg \left[e^{i\delta t} \left(\cos \Omega t - i\frac{\delta}{\Omega} \sin \Omega t \right) \right]. \quad (7.80)$$

Если мы уменьшаем g при фиксированном $\delta \neq 0$, то вероятность поглощения χ_r уменьшается как g^2 , тогда как сдвиг фазы χ_i остается практически постоянным. Это дает возможность создать материалы, в которых сдвиг фазы происходит практически без рассеяния света.

Упражнение 7.19 (лоренцевский контур поглощения). Постройте график χ_r из (7.79) для $t = 1$ и $g = 1, 2$ как функции расстройки δ , а также соответствующий график для классической вероятности поглощения (если она вам известна). Чем объясняются осцилляции?

Упражнение 7.20. Выведите выражение (7.80), используя формулу (7.77), и постройте график χ_i как функции расстройки δ для $t = 1$ и $g = 1, 2$. Сравните результат с δ/Ω^2 .

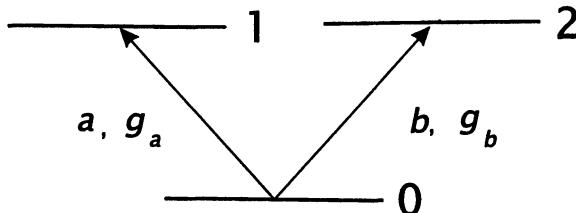


Рис. 7.4. Трехуровневый атом (уровни 0, 1 и 2), взаимодействующий с двумя ортогонально-поляризованными фотонными модами (операторы a и b). Соответствующие константы связи — g_a и g_b . Энергии переходов 0-1 и 0-2 считаются приблизительно одинаковыми

Естественное обобщение рассмотренной задачи — изучение взаимодействия двух фотонных мод (каждая из которых содержит максимум один фотон) с одним и тем же атомом. В этой задаче может возникнуть нелинейное взаимодействие между двумя модами. Напомним (подразд. 7.4.2), что нелинейную среду Керра можно описать феноменологически как среду, в которой возникает перекрестная фазовая модуляция с гамильтонианом вида $H = \chi a^\dagger a b^\dagger b$. Однако, осталось неясным каким образом этот эффект возникает из фундаментальных взаимодействий. Используя формализм данного раздела, мы можем проиллюстрировать эффект Керра на простой модели, в которой две фотонные моды с разной поляризацией взаимодействуют с трехуровневым атомом, как показано на рис. 7.4. Это взаимодействие описывается гамильтонианом типа Джейнса–Каммингса:

$$H = \delta \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} + g_a \left(a \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} + a^\dagger \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \right) + g_b \left(b \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} + b^\dagger \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \right), \quad (7.81)$$

где операторы, действующие на атом, представлены 3×3 матрицами в базисе $|0\rangle, |1\rangle, |2\rangle$. Если учитывать только те состояния, в которых на каждой моде не более одного фотона, можно записать H в матричном виде как

$$H = \begin{bmatrix} H_0 & 0 & 0 \\ 0 & H_1 & 0 \\ 0 & 0 & H_2 \end{bmatrix}, \quad (7.82)$$

где

$$H_0 = -\delta, \quad (7.83)$$

$$H_1 = \begin{bmatrix} -\delta & g_a & 0 & 0 \\ g_a & \delta & 0 & 0 \\ 0 & 0 & -\delta & g_b \\ 0 & 0 & g_b & \delta \end{bmatrix}, \quad (7.84)$$

$$H_2 = \begin{bmatrix} -\delta & g_a & g_b \\ g_a & \delta & 0 \\ g_b & 0 & \delta \end{bmatrix}. \quad (7.85)$$

Здесь выбран базис $|a, b, \text{атом}\rangle = |000\rangle$ для H_0 ; базис $|100\rangle, |001\rangle, |010\rangle, |002\rangle$ для H_1 ; базис $|110\rangle, |011\rangle, |102\rangle$ для H_2 , причем столбцы указываются слева направо. Вычислив экспоненту $U = \exp(iHt)$, можно найти однофотонные фазовые сдвиги состояний $\varphi_a = \arg(\langle 100|U|100\rangle) - \arg(\langle 000|U|000\rangle)$ и $\varphi_b = \arg(\langle 010|U|010\rangle) - \arg(\langle 000|U|000\rangle)$, а также фазовый сдвиг двухфотонного состояния $\varphi_{ab} = \arg(\langle 110|U|110\rangle) - \arg(\langle 000|U|000\rangle)$. В случае линейной среды мы имели бы $\varphi_{ab} = \varphi_a + \varphi_b$, т. е. фаза двухфотонного состояния в ходе эволюции меняется в два раза быстрее, чем фаза однофотонного состояния, поскольку $\exp[-i\omega(a^\dagger a + b^\dagger b)]|11\rangle = \exp(-2i\omega)|11\rangle$. Однако в нашем случае система нелинейна. Зависимость величины $\chi_3 = \varphi_{ab} - \varphi_a - \varphi_b$ от расстройки δ показана на рис. 7.5. В рассматриваемой физической системе эффект Керра обусловливается ненулевой амплитудой процесса, в котором атом обменивается квантами энергии с двумя оптическими модами.

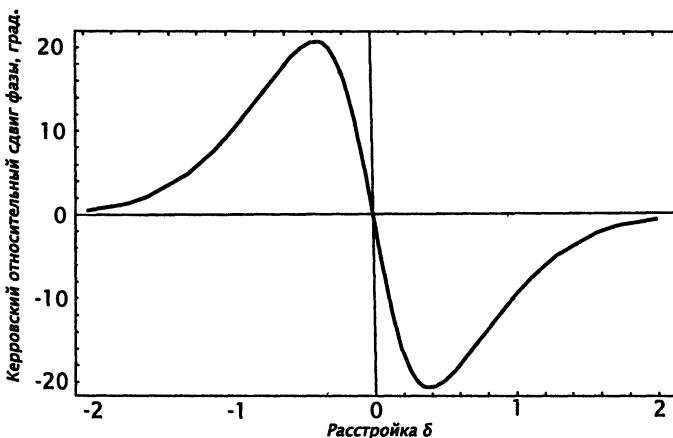


Рис. 7.5. Керровский сдвиг фазы χ_3 для $t = 0.98$ и $g_a = g_b = 1$ как функция расстройки δ . Для описания взаимодействия одиночных фотонов с одиночным трехуровневым атомом использовался гамильтониан (7.82).

Упражнение 7.21. Вычислив экспоненту от H из (7.82), покажите, что

$$\varphi_{ab} = \arg \left[e^{i\delta t} \left(\cos \Omega' t - i \frac{\delta}{\Omega'} \sin \Omega' t \right) \right], \quad (7.86)$$

где $\Omega' = \sqrt{\delta^2 + g_a^2 + g_b^2}$. Используя полученный результат, найдите керровский сдвиг фазы χ_3 . Отметим, что стандартная модель керровского взаимодействия в рамках классической нелинейной оптики значительно сложнее.

Упражнение 7.22. Перекрестная фазовая модуляция сопровождается поглощением света, которое можно охарактеризовать вероятностью поглощения фотона атомом. Вычислите эту вероятность, используя выражение $1 - |\langle 110|U|110 \rangle|^2$, где $U = \exp(-iHt)$ с H из (7.82). Сравните ее с $1 - |\langle 100|U|100 \rangle|^2$. Исследуйте зависимость от параметров δ , g_a , g_b и t .

7.5.4 Квантовые вычисления

Использование техники КЭДР для квантовых вычислений основывается на двух принципиально разных методах. В первом методе квантовая информация представляется состояниями фотонов, а резонаторы с атомами используются для создания фотон-фотонного взаимодействия. Во втором методе квантовая информация представляется состояниями атомов, а фотоны служат для передачи информации между атомами. Мы ограничимся описанием первого метода и рассмотрим эксперименты, в которых реализуются квантовые логические элементы.

Как мы видели в подразд. 7.4.2, квантовые вычисления можно проводить, используя однофотонные состояния, фазовращатели, светофильтры и керровские среды. Однако, перекрестная модуляция с фазой π , необходимая для реализации CNOT, в стандартных оптических макроскопических нелинейных приборах практически не достижима. Как показано в подразд. 7.5.3, техника КЭДР также приводит к керровскому взаимодействию, но в отличие от макроскопических сред взаимодействие может быть очень сильным даже для однофотонных состояний. Это связано с тем, что напряженность поля фотонной моды в резонаторе типа Фабри-Перо очень велика.

На рис. 7.6 иллюстрируется КЭДР-эксперимент (см. разд. “История и дополнительная литература” в конце главы), целью которого было продемонстрировать возможность реализации унитарного оператора

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & e^{i\varphi_a} & 0 & 0 \\ 0 & 0 & e^{i\varphi_b} & 0 \\ 0 & 0 & 0 & e^{i(\varphi_a+\varphi_b+\Delta)} \end{bmatrix}, \quad \text{где } \Delta = 16^\circ, \quad (7.87)$$

с использованием одиночных фотонов. В этом эксперименте на вход резонатора подавались две фотонные моды (с различными, но близкими частотами),

приготовленные в слабом когерентном состоянии, с линейной поляризацией (пробный луч) и круговой поляризацией (луч накачки). Входное состояние имело вид

$$|\psi_{\text{вх}}\rangle = |\beta^+\rangle \left[\frac{|\alpha^+\rangle + |\alpha^-\rangle}{\sqrt{2}} \right], \quad (7.88)$$

поскольку линейная поляризация эквивалентна суперпозиции двух круговых поляризаций + и - с равными весами. Для слабых когерентных состояний можно использовать приближения $|\alpha\rangle \approx |0\rangle + \alpha|1\rangle$, $|\beta\rangle \approx |0\rangle + \beta|1\rangle$ (с точностью до нормировочного множителя), что дает

$$|\psi_{\text{вх}}\rangle \approx \left[|0^+\rangle + \beta|1^+\rangle \right] \left[|0^+\rangle + \alpha|1^+\rangle + |0^-\rangle + \alpha|1^-\rangle \right]. \quad (7.89)$$

Фотоны, проходя через оптический резонатор, взаимодействуют с атомом, в результате чего фотонные состояния приобретают дополнительную фазу. Эта фаза зависит от числа фотонов на каждой из мод, имеющих поляризацию + и -. В частности, мы предполагаем, что сдвиг фазы состояния $|1^+\rangle$ для пробной моды равен $e^{i\varphi_a}$, а сдвиг фазы состояния $|1^+\rangle$ для моды накачки составляет $e^{i\varphi_b}$. Что касается состояния $|1^+1^+\rangle$, то его фаза содержит дополнительный керровский сдвиг Δ , поэтому оно переходит в $e^{i(\varphi_a + \varphi_b + \Delta)}|1^+1^+\rangle$. Все остальные состояния (например с другими поляризациями) остаются без изменений. Гамильтониан, описывающий динамику данной системы, аналогичен тому, что мы рассматривали в подразд. 7.5.3, и приводит к тому же самому эффекту, т. е. к перекрестной фазовой модуляции между фотонами пробного луча и луча накачки. Таким образом, на выходе резонатора получается состояние

$$\begin{aligned} |\psi\rangle \approx & |0^+\rangle \left[|0^+\rangle + \alpha e^{i\varphi_a} |1^+\rangle + |0^-\rangle + \alpha|1^-\rangle \right] \\ & + e^{i\varphi_b} \beta|1^+\rangle \left[|0^+\rangle + \alpha e^{i(\varphi_a + \Delta)} |1^+\rangle + |0^-\rangle + \alpha|1^-\rangle \right] \end{aligned} \quad (7.90)$$

$$\approx |0^+\rangle |\alpha, \varphi_a/2\rangle + e^{i\varphi_b} \beta|1^+\rangle |\alpha, (\varphi_a + \Delta)/2\rangle, \quad (7.91)$$

где $|\alpha, \varphi_a/2\rangle$ — когерентное состояние пробного луча с линейной поляризацией под углом $\varphi_a/2$ к вертикали. Измерения поляризации поля на выходе детектора позволили найти значения параметров модели: $\varphi_a \approx 17,5^\circ$, $\varphi_b \approx 12,5^\circ$ и $\Delta \approx 16^\circ$. Это означает, что с помощью одиночных фотонов можно реализовать универсальный двухкубитовый логический элемент (упр. 7.23), причем одиночный атом в резонаторе играет роль нелинейной керровской среды, посредством которой взаимодействуют фотоны.

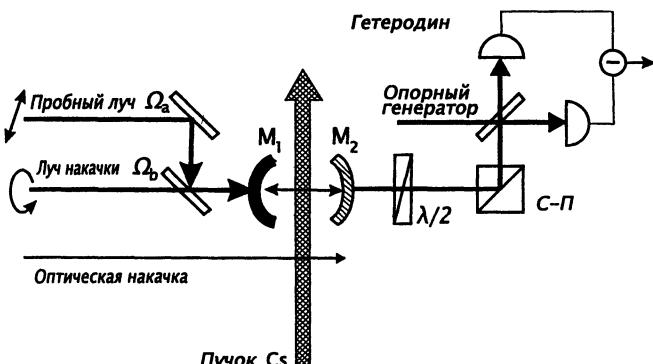


Рис. 7.6. Схема экспериментальной установки, в которой одиночные атомы обеспечивают перекрестную фазовую модуляцию между фотонами, что позволяет реализовать элементарный логический квантовый элемент. Слабый линейно поляризованный пробный луч Ω_a и более мощный поляризованный по кругу луч накачки Ω_b подаются на вход оптического резонатора с зеркалами M_1 и M_2 , имеющими большой коэффициент отражения. Дополнительный луч оптической накачки служит для приготовления атомов цезия в начальном состоянии $6S_{1/2}$, $F = 4$, $m = 4$ (на рисунке атомы перемещаются снизу вверх), причем среднее число атомов в резонаторе около единицы. Фотоны, проходящие через резонатор, взаимодействуют с атомом, так что фотон с поляризацией σ_+ индуцирует переход на уровень $6P_{3/2}$, $F' = 5$, $m' = 5$, а фотон с поляризацией σ_- индуцирует переход на уровень $6P_{3/2}$, $F' = 5$, $m' = 3$. Затем при помощи полуволновой пластины, светоделителя-поляризатора (С-П) и чувствительного гетеродинного детектора (детектирующего свет на одной определенной частоте, которая задается опорным генератором колебаний) измеряется поляризация света на выходе резонатора (Рисунок К. Тюршета.).

Относительно интерпретации этих экспериментальных результатов следует сделать несколько важных оговорок. Во-первых, существует вероятность того, что фотон поглотится в системе атом-резонатор. Это означает, что преобразование, которое мы в действительности реализуем, не унитарное. Поглощение станет особенно существенным при построении последовательностей из нескольких элементов, например при реализации CNOT (для которого требуется $\Delta = \pi$). Чтобы понять, как с этим бороться, необходимо построить адекватную нестационарную модель. Во-вторых, хотя модель, использованная нами для изучения взаимодействия между атомом и фотонами, дает удовлетворительное описание экспериментальных данных, она не является единственной возможной моделью. Можно было бы провести тот же эксперимент с однофотонными состояниями (вместо ослабленных когерентных состояний). При этом измерения запутанности между двумя модами в выходном состоянии $|\psi_{\text{вых}}\rangle$ позволили бы еще раз проверить нашу модель. К моменту проведения данного эксперимента еще не было методики для полного описания квантового процесса. Однако, в настящее время такая методика, известная как *томография процесса*, хорошо разработана (гл. 8) и, что замечательно, она позволяет полностью охарактеризовать даже дисипацию и другие неунитарные свойства. Ее применение в данном эксперименте позволило бы определить, насколько точно удалось реализовать квантовый логический элемент.

Несмотря на эти недостатки, в описанном эксперименте продемонстрированы понятия, важные для обработки квантовой информации. Он показал, что

нелинейные оптические явления, такие как взаимодействие Керра, действительно могут происходить на уровне одиночных фотонов, подтверждая таким образом модель Джейнса–Каммингса. Данный эксперимент проводился в так называемом *режиме плохого резонатора*. В этом режиме ширина атомного уровня при наличии резонатора g^2/k больше вероятности (в единицу времени) спонтанного излучения в свободном пространстве γ , но меньше обратного времени жизни фотона в резонаторе k . С другой стороны, существует *режим сильной связи*, в котором $g > k > \gamma$, позволяющий достичь больших значений относительного фазового сдвига Δ .

Возможно, наиболее важно то, что техника КЭДР предоставляет нам богатый набор взаимодействий, которые могут пригодиться для обработки квантовой информации. Мы также увидели, что использование одиночных фотонов и одиночных атомов является перспективным для реализации квантовых вычислений и что на основе гамильтониана Джейнса–Каммингса можно прийти к важным физическим законам, описывающим взаимодействие электромагнитного поля с веществом. На этом мы заканчиваем рассмотрение КЭДР, но ее основные понятия, такие как атом-фотонное взаимодействие, одиночные фотоны и атомы, гамильтониан Джейнса–Каммингса будут встречаться и далее при обсуждении ионов в ловушке и ядерного магнитного резонанса.

Упражнение 7.23. Покажите, что с помощью двухкубитового оператора (7.87) при любых φ_a , φ_b и $\Delta = \pi$ можно реализовать элемент CNOT (разрешается использовать произвольные однокубитовые операции). Заметим, что (7.87) вместе с однокубитовыми унитарными операциями дает универсальный базис при практически любом значении Δ .

Квантовая электродинамика в оптических резонаторах

- **Представление кубита.** Один фотон, который может находиться на двух модах $|01\rangle$ и $|10\rangle$ или с двумя поляризациями.
- **Унитарная эволюция.** Произвольный оператор можно реализовать с помощью фазовращателей (вращения R_z), светоделителей (вращения R_y) и системы типа КЭДР, представляющей собой резонатор Фабри–Перо, внутри которого находятся несколько атомов, взаимодействующих с фотонными модами резонатора.
- **Приготовление начального состояния.** Генерация однофотонных состояний (например путем ослабления лазерного излучения).
- **Измерение конечного результата.** Детектирование одиночных фотонов (например, с помощью фотоумножителя).
- **Недостатки.** Поскольку фотон-фотонное взаимодействие обусловлено промежуточным взаимодействием с атомом, желательно увеличить константу связи атома с полем. Однако, при этом уменьшается время когерентности атома, что ограничивает длину квантовых вычислений.

7.6 Ионы в ловушке

До сих пор в этой главе обсуждалось в основном представление кубитов при помощи фотонов. Переядем теперь к представлениям, в которых используются атомные и ядерные состояния, а именно электронный и ядерный спины, которые, как уже было отмечено в разд. 7.1, являются очень многообещающими представлениями для кубита. Спин — это странное (но реальное!) понятие. Оно обсуждается во вставке 7.7. Разности энергий различных спиновых состояний, как правило, намного меньше всех остальных характерных энергий (например, кинетической энергии атомов при комнатной температуре), что осложняет наблюдение и управление спиновыми состояниями атома. Однако, существует специальная экспериментальная техника, позволяющая контролировать спиновые состояния. Для этого небольшое количество ионизированных атомов изолируется и удерживается в электромагнитной ловушке, после чего они охлаждаются до температуры, при которой кинетическая энергия становится малой по сравнению со спиновыми энергиями. Включая внешнее резонансное электромагнитное поле, можно селективно воздействовать на некоторую пару состояний. Это составляет основу квантовых вычислений методом ионов в ловушке, который и будет обсуждаться в данном разделе. Мы начнем с рассмотрения экспериментальной установки и ее основных частей, после чего приведем выражение для гамильтониана, моделирующего систему. Далее будет описан эксперимент с ионами ${}^9\text{Be}$, демонстрирующий реализацию СНОТ. В заключение мы сделаем комментарии относительно перспектив и недостатков метода.

Упражнение 7.24. Энергия ядерного спина в магнитном поле оценивается как $\mu_N B$, где $\mu_N = eh/4\pi m_p \approx 5 \times 10^{-27}$ Дж/Тл — ядерный магнетон Бора. Найдите энергию ядерного спина в поле $B = 10$ Тл и сравните ее с тепловой энергией $k_B T$ при $T = 300$ К.

7.6.1 Физическая аппаратура

Мы обсудим два основных компонента квантового компьютера, реализуемого ионами в ловушке: электромагнитную ловушку, оборудованную лазерами и фотодетекторами, и собственно ионы.

Геометрия ловушки и лазеры

Главная часть экспериментальной установки, электромагнитная ловушка, состоит из четырех цилиндрических электродов, как показано на рис. 7.7.

Между внутренним и внешними участками каждого электрода поддерживается разность потенциалов U_0 , так что ионы находятся в статическом потенциале $\Phi_{dc} = kU_0 [z^2 - (x^2 + y^2)/2]$ (k — геометрический фактор) и, таким образом, локализованы вдоль оси \hat{z} . Однако, согласно теореме Ирнишу, заряд не может удерживаться по всем трем координатам в статическом потенциале. Чтобы добиться удержания ионов, на два из четырех электродов подава-

лось быстроосцилирующее напряжение, создающее радиочастотный потенциал $\Phi_{rf} = (V_0 \cos \Omega_T t + U_r)(1 + (x^2 - y^2)/R^2)/2$, где R — геометрический фактор, а два других электрода были заземлены. Благодаря емкостной связи между участками электродов, радиочастотный потенциал можно считать постоянным вдоль электрода. После усреднения по быстрым осцилляциям с частотой Ω_T сумма полей Φ_{dc} и Φ_{rf} создает эффективный параболический по x , y , z статический потенциал. С учетом кулоновского взаимодействия ионов это дает нам следующий гамильтониан, описывающий движение ионов в ловушке:

$$H = \sum_{i=1}^N \frac{M}{2} \left(\omega_x^2 x_i^2 + \omega_y^2 y_i^2 + \omega_z^2 z_i^2 + \frac{|\vec{p}_i|^2}{M^2} \right) + \sum_{i=1}^N \sum_{j>i} \frac{e^2}{4\pi\epsilon_0 |\vec{r}_i - \vec{r}_j|}, \quad (7.92)$$

где M — масса каждого иона, а N — число ионов. Как правило, $\omega_x, \omega_y \gg \omega_z$, так что ионы выстраиваются вдоль оси \hat{z} . При увеличении числа ионов геометрические конфигурации ионов становятся более сложными, образуя зигзагообразные и другие структуры, однако мы ограничимся простым случаем, когда в ловушке удерживается всего несколько ионов, а их равновесная конфигурация представляет собой линейную цепочку

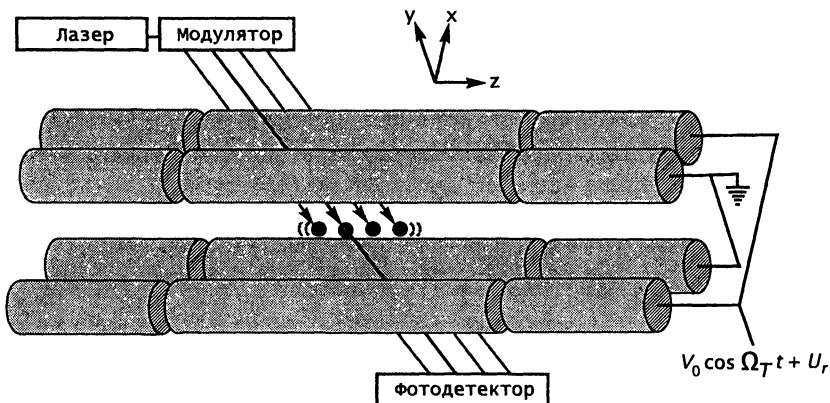


Рис. 7.7. Схематическое изображение квантового компьютера, реализованного при помощи ионов в ловушке (без соблюдения масштаба). Четыре цилиндрических электрода создают в центре ловушки потенциал, удерживающий четыре иона. Вся установка, как правило, помещается в глубокий вакуум ($\approx 10^{-8}$ Па), а ионы подаются из расположенного рядом источника. Модулированное лазерное излучение падает на ионы через окна вакуумной камеры. Воздействуя им на атомные состояния, мы можем производить вычисления и считывать результат.

Подобно тому, как груз на пружине начинает проявлять квантовые свойства, когда его связь с внешним миром становится достаточно мала, движение иона в электромагнитной ловушке начинает квантоваться, если система хорошо изолирована. Сначала мы объясним, что имеется в виду под квантованием, а затем, что значит «хорошо изолирована». Как мы видели в разд. 7.3, уровни энергии гармонического осциллятора образуют эквидистантный спектр с расстоянием между уровнями $\hbar\omega_z$. Если говорить об ионах в ловушке, то в обсуждаемом режиме достаточно рассматривать колебательную моду, в которой

линейная цепочка ионов движется как одно тело с массой NM . Мы будем называть эту моду *трансляционной*. Каждый квант энергии колебаний цепочки называется *фононом* и может рассматриваться как частица по аналогии с фотонами — квантами энергии колебаний электромагнитного поля в резонаторе.

Подобное описание в терминах фононов справедливо только при выполнении определенных условий. Прежде всего, взаимодействие с окружающей средой должно быть достаточно слабым, чтобы тепловые флуктуации не разрушали состояние системы (что делает ее поведение классическим). Флуктуации электрических и магнитных полей могут толкать ионы, вызывая случайные переходы с уровня на уровень. Подобные источники шума технически почти неизбежны. Источник напряжения, подсоединененный к электродам ловушки, не идеален: он всегда имеет конечное сопротивление. Это приводит к флуктуациям напряжения (шум Джонсона) в том числе и на частотах, к которым чувствительны ионы. Еще одним источником шума являются флуктуации электрического поля в местах соединения электродов. При увеличении интенсивности флуктуаций квантовые характеристики состояния ионов уступают место классическим статистическим средним. Например, импульс и координата ионов могут быть определены одновременно, что невозможно для квантовой системы. Тем не менее, большинство помех может быть подавлено до такой степени, что эффектами нагрева или сбоя фазы ионов за время эксперимента можно пренебречь. Важное наблюдение, которое облегчает эту задачу, состоит в том, что в приближении параболического удерживающего потенциала ионы восприимчивы к внешнему шуму лишь на некоторых резонансных частотах. Поэтому естественно ожидать, что только флуктуации на частотах вблизи ω_z будут влиять на ионы.

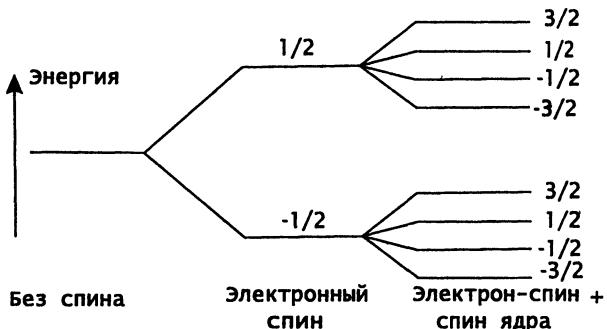
Вставка 7.7. Спин

Спин — это довольно странное понятие. Известно, что наличие у частицы спина обуславливает наличие у нее магнитного момента. Так было бы, если частицы представляли бы собой нечто вроде витка с током. Однако, электроны или кварки являются элементарными частицами, но тем не менее имеют спин. Спин любой частицы может быть либо целым либо полуцелым.

Без понятия спина нельзя обойтись даже при анализе простейших физических явлений. Частицы с целым спином называются бозонами, их примером является фотон. Отсутствие у фотона массы приводит к тому, что его состояние описывается только двумя спиновыми проекциями ± 1 (проекция спина 0 отсутствует). Они соответствуют двум ортогональным поляризациям. Дешевые пластиковые очки-поляризаторы помогают нам при поездке в автомобиле, поскольку при отражении от дорожного покрытия свет становится частично поляризованным в горизонтальном направлении (это связано с обращением в нуль коэффициента отражения

под углом Брюстера для волны, в которой вектор электрического поля лежит в плоскости падения луча). Частицы с полуцелым спином называются фермионами; к ним относятся электрон, протон и нейтрон — частицы со спином $1/2$. Их состояние описывается двумя спиновыми проекциями $\pm 1/2$ (спин вверх и спин вниз). Часто под словом «спин» понимают именно частицу со спином $1/2$.

Классификация собственных состояний атома включает задание одного или нескольких спинов. Например, ядро рассматриваемого нами ${}^9\text{Be}$ имеет спин $3/2$. При взаимодействии с магнитным полем спины ведут себя как магнитные моменты. В поле \vec{B} электрон со спином \vec{S} приобретает энергию $g_e \vec{S} \cdot \vec{B}$. Аналогично, ядро со спином \vec{I} приобретает энергию $g_n \vec{I} \cdot \vec{B}$. Расщепление атомных уровней, возникающее в магнитном поле благодаря спину, может быть схематично представлено следующим образом:



где подразумевается, что ядро имеет спин $3/2$, а электронный спин атома $1/2$. Переходы между расщепленными уровнями могут индуцироваться лазерным излучением с резонансной частотой при условии, что переход не нарушает законы сохранения (подразд. 7.5.1). В частности, закон сохранения углового момента утверждает, что при поглощении фотона должен измениться на единицу либо орбитальный момент, либо спин.

В случае непрерывных переменных, таких как координата или импульс, для квантования требуется бесконечномерное пространство состояний, и если мы хотим представлять этими переменными кубиты, необходимо искусственно уменьшать пространство состояний. Спины представляют квантовую информацию более удачно, поскольку они, по определению, соответствуют конечномерным пространствам.

Приближение одномерного параболического потенциала работает хорошо, если только температура ионов достаточно мала; иначе амплитуда их колебаний станет больше размеров той области в центре ловушки, где удерживающий потенциал можно считать параболическим. Колебательные моды, на которых ионы могут двигаться относительно друг друга (фононы с ненулевым импульсом), должны иметь энергию, значительно превышающую энергию трансляционной моды. Если все эти условия выполнены и каждый ион охлажден до его основного состояния, низколежащие состояния системы классифицируются числом фононов на трансляционной моде. Рождение таких фононов напоминает *эффект Мессбауэра*, в котором гамма-фотон поглощается ядром атома кристалла без рождения фононов, так что энергия отдачи определяется массой всего кристалла.

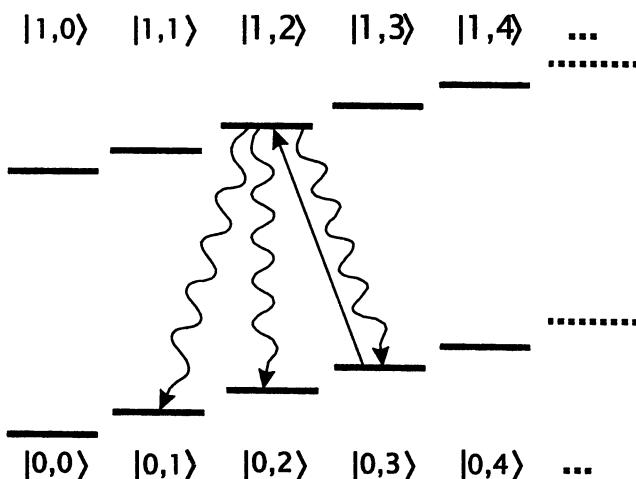


Рис. 7.8. Охлаждение методом боковой полосы. Показаны переходы между состояниями $|0, n\rangle$ и $|1, m\rangle$, где 0 и 1 — два электронных уровня, n и m — числа заполнения фононов, характеризующие колебательное состояние иона. Лазер настраивается так, что его частота меньше разности электронных уровней на энергию одного фонона. Например, начальное состояние $|0, 3\rangle$ может перейти только в $|1, 2\rangle$. Затем за счет спонтанного излучения происходит переход с примерно одинаковой вероятностью в одно из состояний $|0, 1\rangle$, $|0, 2\rangle$ или $|0, 3\rangle$ (волнистые линии). Естественно, излучение лазера генерирует также все переходы вида $|0, n\rangle \rightarrow |1, n-1\rangle$, поскольку их энергия не зависит от n . Но ионы в состоянии $|0, 0\rangle$ уже не могут поглотить фонон и, очевидно, это состояние и будет конечным состоянием ионов.

Каким образом можно охладить ионы до основного состояния? Более точно, наша цель — получить $k_B T \ll \hbar\omega_z$, где T — температура, соответствующая кинетической энергии ионов. Основная идея состоит в том, чтобы использовать для охлаждения эффект Доплера. Как мы знаем, фотон обладает не только энергией, но и импульсом $p = h/\lambda$, где λ — длина волны света. Подобно тому как свисток приближающегося поезда имеет более высокую частоту, чем у удаляющегося поезда, атом, летящий в сторону лазера, имеет частоту перехода немного выше, чем атом, летящий от лазера. Если частота лазера подобрена так, что его излучение поглощается только приближающимися атомами,

атомы начнут замедляться, поскольку импульс поглощенного фотона вычитается из импульса атома. Этот метод называется доплеровским охлаждением. Установливая надлежащим образом настроенные лазеры вдоль каждой координатной оси, мы можем охладить атомы в ловушке до температуры порядка $k_B T \approx \hbar\Gamma/2$, где Γ — излучательная ширина перехода, используемого для охлаждения. Чтобы достичь еще более низких температур, используется метод *боковой полосы*, иллюстрируемый на рис 7.8. Он позволяет достичь предела $k_B T \ll \hbar\omega_z$.

Еще одно необходимое условие состоит в том, что амплитуда колебаний ионной цепочки в удерживающем потенциале должна быть мала по сравнению с длиной волны управляющего лазера. Это условие можно сформулировать при помощи *параметра Лэмба-Дика*, $\eta \equiv 2\pi z_0/\lambda$, где λ — длина волны, $z_0 = \sqrt{\hbar/2NM\omega_z}$ — характерная амплитуда нулевых колебаний цепочки. Критерий Лэмба-Дика состоит в том что $\eta \ll 1$. Чтобы ионы в ловушке можно было использовать для квантовых вычислений, желательно иметь, по крайней мере, $\eta \approx 1$. Это гарантирует нам, что лазерный луч можно направлять на отдельные ионы, и в то же время имеется возможность возбуждать лазером фононы на трансляционной моде, что требуется для квантовых вычислений.

Атомная структура

Ловушка для удержания ионов, описанная выше, позволяет охладить ионы до такой степени, что их колебательное состояние становится близким к основному состоянию $|0\rangle$, в котором числа заполнения фононных мод равны нулю. Помимо этого мы должны приготовить внутренние состояния ионов так, чтобы их можно было использовать для хранения квантовой информации. Сейчас мы рассмотрим эти внутренние состояния, и, оценивая их время когерентности, увидим, что они хорошо подходят для представления кубита.

Внутренние состояния ионов характеризуются электронным спином S и ядерным спином I , которые складываются в полный спин $F = S + I$. Чтобы понять, как это происходит, нам понадобится формальная теория *сложения угловых моментов*. Она важна не только для описания атомных состояний, но и с точки зрения квантовой информации. Как мы видели в подразд. 7.5.1, при взаимодействии одиночного фотона с атомом угловой момент последнего может измениться только на единицу. Однако у полного углового момента атома имеется несколько составляющих: орбитальный момент, электронный спин и ядерный спин. Какая из этих составляющих изменится, частично зависит от того, между какими уровнями происходит переход. Внутренние состояния атома удобно описывать, выбрав в качестве базисных состояний собственные функции *полного углового момента* атома.

Рассмотрим в качестве примера два спина $1/2$. Если использовать обозначения, принятые для кубит, в качестве базисных состояний можно взять $|00\rangle$, $|01\rangle$, $|10\rangle$ и $|11\rangle$. Однако, если нас интересует полный спин, более естественен следующий базис:

$$|0, 0\rangle_J = \frac{|01\rangle - |10\rangle}{\sqrt{2}}, \quad (7.93)$$

$$|1, -1\rangle_J = |00\rangle, \quad (7.94)$$

$$|1, 0\rangle_J = \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \quad (7.95)$$

$$|1, 1\rangle_J = |11\rangle. \quad (7.96)$$

Эти состояния являются собственными состояниями оператора полного углового момента, определяемого как

$$J^2 = j_x^2 + j_y^2 + j_z^2, \quad (7.97)$$

где $j_x = (X_1 + X_2)/2$, $j_y = (Y_1 + Y_2)/2$ и $j_z = (Z_1 + Z_2)/2$. Состояние $|j, m_j\rangle_J$ является собственным для J^2 с собственным значением $j(j+1)$ и для j_z с собственным значением m_j . Этот базис удобен для описания многих физических взаимодействий. Например, для магнитного поля, направленного вдоль оси \hat{z} , мы имеем гамильтониан μB_z , где магнитный момент μ пропорционален m_j , проекции полного углового момента на ось \hat{z} .

Теория сложения угловых моментов достаточно нетривиальная, поэтому мы не станем погружаться в нее слишком глубоко (заинтересованному читателю мы предлагаем несколько упражнений, а также приводим некоторые полезные ссылки, см. разд. «История и дополнительная литература» в конце главы). Тем не менее даже из рассмотренного выше примера можно сделать интересные для теории квантовой информации наблюдения. Действительно, состояние $|0, 0\rangle_J$ есть не что иное как состояние Белла (подразд. 1.3.6), которое встречается в Природе достаточно редко благодаря его странным нелокальным свойствам. Почему же Природа захотела реализовать это состояние именно здесь? Это связано с симметрией взаимодействий магнитных моментов, по отношению к их перестановке. Такие симметрии встречаются в физике очень часто и могут оказаться полезными для реализации, например измерений в базисе Белла, или других операций с запутанными состояниями.

Упражнение 7.25. Покажите, что операторы полного углового момента подчиняются коммутационным соотношениям алгебры $SU(2)$, т. е. $[j_i, j_k] = i\varepsilon_{ikl}j_l$.

Упражнение 7.26. Найдите явный вид 4×4 матриц J^2 и j_z в базисе, определяемом состояниями $|j, m_j\rangle_J$.

Упражнение 7.27 (сложение угловых моментов трех спинов). Система из трех спинов $1/2$ может иметь полный угловой момент $j = 1/2$ или $j = 3/2$.

Покажите, что в качестве базисных состояний трех спинов можно выбрать

$$|3/2, 3/2\rangle = |111\rangle, \quad (7.98)$$

$$|3/2, 1/2\rangle = \frac{1}{\sqrt{3}} [|011\rangle + |101\rangle + |110\rangle], \quad (7.99)$$

$$|3/2, -1/2\rangle = \frac{1}{\sqrt{3}} [|100\rangle + |010\rangle + |001\rangle], \quad (7.100)$$

$$|3/2, -3/2\rangle = |000\rangle, \quad (7.101)$$

$$|1/2, 1/2\rangle_1 = \frac{1}{\sqrt{2}} [-|001\rangle + |100\rangle], \quad (7.102)$$

$$|1/2, -1/2\rangle_1 = \frac{1}{\sqrt{2}} [|110\rangle - |011\rangle], \quad (7.103)$$

$$|1/2, 1/2\rangle_2 = \frac{1}{\sqrt{6}} [|001\rangle - 2|010\rangle + |100\rangle], \quad (7.104)$$

$$|1/2, -1/2\rangle_2 = \frac{1}{\sqrt{6}} [-|110\rangle + 2|101\rangle - |011\rangle], \quad (7.105)$$

причем $J^2|j, m_j\rangle = j(j+1)|j, m_j\rangle$ и $j_z|j, m_j\rangle = m_j|j, m_j\rangle$, где $j_z = (Z_1 + Z_2 + Z_3)/2$ (и аналогично для j_x, j_y), а $J^2 = j_x^2 + j_y^2 + j_z^2$. Заметим, что существуют специальные методы нахождения этих состояний, однако можно действовать и методом грубой силы, непосредственно приводя 8×8 матрицы J^2 и j_z к диагональному виду.

Упражнение 7.28 (сверхтонкая структура). Поскольку нас в основном будут интересовать атомы бериллия (подразд. 7.6.4), рассмотрим сложение двух угловых моментов: ядерного спина $I = 3/2$ и электронного спина $S = 1/2$. При этом полный угловой момент может быть либо $F = 2$, либо $F = 1$. Для частицы со спином $3/2$ операторы углового момента имеют вид

$$i_x = \frac{1}{2} \begin{bmatrix} 0 & \sqrt{3} & 0 & 0 \\ \sqrt{3} & 0 & 2 & 0 \\ 0 & 2 & 0 & \sqrt{3} \\ 0 & 0 & \sqrt{3} & 0 \end{bmatrix}, \quad (7.106)$$

$$i_y = \frac{1}{2} \begin{bmatrix} 0 & i\sqrt{3} & 0 & 0 \\ -i\sqrt{3} & 0 & 2i & 0 \\ 0 & -2i & 0 & i\sqrt{3} \\ 0 & 0 & -i\sqrt{3} & 0 \end{bmatrix}, \quad (7.107)$$

$$i_z = \frac{1}{2} \begin{bmatrix} -3 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}. \quad (7.108)$$

- Покажите, что i_x , i_y , i_z подчиняются коммутационным соотношениям алгебры $SU(2)$.
- Запишите в виде матриц 8×8 операторы $f_z = i_z \otimes I + I \otimes Z/2$ (где I — единичный оператор), f_x , f_y и $F^2 = f_x^2 + f_y^2 + f_z^2$. Найдите базис $|F, m_F\rangle$, в котором диагональны операторы F^2 и f_z , т. е. $F^2|F, m_F\rangle = F(F+1)|F, m_F\rangle$ и $f_z|F, m_F\rangle = m_F|F, m_F\rangle$.

Как долго может существовать суперпозиция различных спиновых состояний? Ее время жизни ограничивается процессом *спонтанного излучения*, в котором атом переходит из возбужденного состояния в основное с испусканием фотона. Акт испускания происходит в случайный момент времени, поэтому нам понадобится вероятность испускания в единицу времени. На первый взгляд может показаться странным, что атом, в свободном пространстве не испытывающий никаких внешних воздействий, может испустить фотон. Этот процесс является простым следствием взаимодействия атома с электромагнитным полем, которое можно описывать знакомым нам (подразд. 7.5.2) гамильтонианом Джейнса–Каммингса

$$H_I = g(a^\dagger \sigma_- + a \sigma_+). \quad (7.109)$$

До сих пор мы использовали этот гамильтониан для описания взаимодействия атома с излучением лазера, однако, естественно он применим и в случае, когда лазера нет. Рассмотрим атом в возбужденном состоянии и единственную моду электромагнитного поля, на которой изначально нет фотонов. Начальное состояние системы есть $|01\rangle$ (в обозначениях $|\text{поле, атом}\rangle$). Оно не является собственным состоянием H_I и, таким образом, его эволюция во времени нестационарна. Эта эволюция описывается унитарным оператором U , определенным в (7.77). Вероятность $p_{\text{исп}} = |\langle 10 | U | 01 \rangle|^2$ того, что в момент t атом окажется в основном состоянии, испустив фотон, равна

$$p_{\text{исп}} = g^2 \frac{4 \sin^2 \frac{1}{2}(\omega - \omega_0)t}{(\omega - \omega_0)^2}, \quad (7.110)$$

в низшем порядке по константе связи атом-поле g . Здесь ω — частота фотонной моды, а $\hbar\omega_0$ — разность энергий двух атомных уровней. Теперь мы должны подставить в (7.110) константу связи¹

$$g^2 = \frac{2\pi\omega_0^2}{\hbar\omega\varepsilon} |\langle 0 | \vec{\mu} | 1 \rangle|^2, \quad (7.111)$$

¹ Для процессов с испусканием одного фотона существует два возможных канала: электрический и магнитный. В классическом пределе им соответствует дипольное и магнитно-дипольное излучение. В общем случае вероятность магнитно-дипольного испускания гораздо меньше соответствующей вероятности для дипольного процесса и имеет тот же порядок величины, что и квадрупольное излучение пары фотонов. Выражения для вероятностей испускания электрического и магнитного типов отличаются только константой связи g . В случае дипольного процесса она пропорциональна матричному элементу оператора дипольного момента, а для магнитно-дипольного излучения — матричному элементу оператора магнитного момента — Прим. ред.

где $\vec{\mu}$ — оператор электрического или магнитного момента, и учесть, что атом в свободном пространстве взаимодействует со многими фотонными модами. Проинтегрировав по всем фотонным модам (упр. 7.29) и взяв производную по времени от полной вероятности, мы найдем вероятность испускания в единицу времени:

$$\gamma_{\text{исп}} = \frac{4\omega_0^3 |\langle 0 | \vec{\mu} | 1 \rangle|^2}{3\hbar c^3}. \quad (7.112)$$

Если взять приближенное значение $|\langle 0 | \vec{\mu}_{\text{маг}} | 1 \rangle| \approx \mu_B \approx 9 \times 10^{-24}$ Дж/Тл, т. е. магнетон Бора,² а $\omega_0/2\pi \approx 10$ ГГц, то получим $\gamma_{\text{исп}}^{\text{маг}} \approx 10^{-15}$ с⁻¹. Таким образом, типичное время жизни спина в возбужденном состоянии составляет около 3 000 000 лет. Это вычисление является типичным примером оценки времен жизни атомных состояний. Как вы можете видеть, теория предсказывает необычайно большие времена жизни сверхтонких состояний и это, как правило, согласуется с экспериментами, в которых наблюдаются времена жизни от десятков секунд до десятков часов.³

Упражнение 7.29 (спонтанное излучение). Полная вероятность спонтанного излучения, может быть найдена из (7.110)–(7.111) следующим образом:

1. Возьмите интеграл

$$\frac{1}{(2\pi c)^3} \frac{8\pi}{3} \int_0^\infty \omega^2 p_{\text{исп}} d\omega. \quad (7.113)$$

Здесь множитель $8\pi/3$ возникает из-за суммирования по поляризациям и интегрирования по углам $d\Omega$, а $\omega^2/(2\pi c)^3$ представляет собой плотность фотонных состояний в трехмерном пространстве. (Указание: интеграл удобно взять, распространив интегрирование на интервал $(-\infty, \infty)$.)

2. Продифференцировав результат по t , найдите $\gamma_{\text{исп}}^{\text{маг}}$.

Использованное выражение для g^2 может быть найдено с помощью квантовой электродинамики. Однако, весь остальной вывод основан только на гамильтониане Джэйнса–Каммингса. Мы опять видим, что изучение его свойств в режиме одиночных фотонов и одиночных атомов позволяет вывести некоторые фундаментальные законы, не прибегая к теории возмущений.

Упражнение 7.30 (времена жизни электронных состояний). Подобно тому, как мы оценили вероятность испускания $\gamma_{\text{рад}}$ для спиновых состояний, можно оценить вероятность испускания для электронных переходов, в которых изменяется главное квантовое число, $\Delta n \neq 0$. Для таких переходов в главном порядке надо учитывать взаимодействие электрического дипольного момента атома $\vec{\mu}_{\text{исп}}$ с электромагнитным полем, поэтому

² Для сверхтонких уровней в з-состояниях дипольные и квадрупольные процессы запрещены, поэтому переход происходит по магнитно-дипольному механизму — Прим. ред.

³ Конечно, такие времена на много порядков больше типичных атомных масштабов времени, однако, они все же гораздо меньше полученной выше оценки. Дело в том, что в реальном эксперименте невозможно полностью изолировать атом от воздействий извне. Неконтролируемые низкочастотные возмущения приводят к так называемому $1/f$ -шуму. Именно величина этого шума и определяет время жизни сверхтонких уровней в эксперименте. — Прим. ред

$$g_{\text{исп}}^2 = \frac{2\pi\omega_0^2}{\hbar\omega} |\langle 0 | \vec{\mu}_{\text{исп}} | 1 \rangle|^2. \quad (7.114)$$

Соответственно, вероятность спонтанного излучения (в единицу времени) равна

$$\gamma_{\text{исп}} = \frac{4\omega_0^3 |\langle 0 | \vec{\mu}_{\text{исп}} | 1 \rangle|^2}{3\hbar c^3}. \quad (7.115)$$

Найдите значение $\gamma_{\text{исп}}^{\text{маг}}$, взяв $\omega_0/2\pi \approx 10^{15}$ Гц, а $|\langle 0 | \vec{\mu} | 1 \rangle| \approx qa_0$, где q — заряд электрона, а a_0 — боровский радиус. Это упражнение показывает, что времена жизни электронных состояний много меньше времени жизни сверхтонких состояний.

7.6.2 Гамильтониан

Объединяя упрощенные модели, введенные в предыдущем разделе для описания колебательных состояний ионов в ловушке и атомной структуры, мы можем написать полный гамильтониан системы. Для этого рассмотрим частицу со спином $1/2$ во внешнем электромагнитном поле, гамильтониан которого имеет вид $H_I = -\vec{\mu} \cdot \vec{B}$, где магнитный момент $\vec{\mu} = \mu_m \vec{S}$ пропорционален оператору спина S , а магнитное поле представляет собой плоскую волну $\vec{B} = B_1 \hat{x} \cos(kz - \omega t + \varphi)$ с амплитудой B_1 , волновым вектором k вдоль оси \hat{z} , частотой ω и фазой φ . В этом разделе нам будет удобно использовать обозначения $S_x = X/2$, $S_y = Y/2$ и $S_z = Z/2$ для операторов спина $1/2$, которые пропорциональны матрицам Паули с коэффициентом $\frac{1}{2}$.

Наряду с электромагнитным взаимодействием имеется также взаимодействие спина с колебательными модами. Будем считать, что частица со спином находится в параболическом удерживающем потенциале с частотой ω_z (рис. 7.9), так что ее координата описывается оператором $z = z_0(a^\dagger + a)$, где a^\dagger , a — повышающий и понижающий операторы для колебательных мод частицы, т. е. операторы рождения и уничтожения фононов.

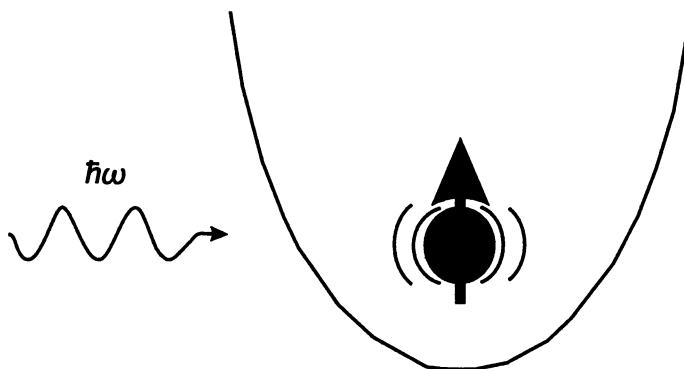


Рис. 7.9. Игрушечная модель иона в ловушке: одиночная двухуровневая частица в параболическом потенциале, взаимодействующая с электромагнитным полем

Предположим, что частица охлаждена до такой температуры, что ее колебательное состояние близко к основному, причем амплитуда колебаний частицы мала по сравнению с длиной волны внешнего излучения, т. е. параметр Лэмба–Дика $\eta \equiv kz_0$ мал. Определяя частоту Раби для спина как $\Omega = \mu_m B_1 / 2\hbar$ и вспоминая, что $S_x = (S_+ + S_-)/2$, мы можем в пределе малых η упростить гамильтониан:

$$H_I = -\vec{\mu} \cdot \vec{B} \quad (7.116)$$

$$\begin{aligned} &\approx \left[\frac{\hbar\Omega}{2} (S_+ e^{i(\varphi-\omega t)} + S_- e^{-i(\varphi-\omega t)}) \right] \\ &+ \left[i \frac{\eta\hbar\Omega}{2} \{S_+ a + S_- a^\dagger + S_+ a^\dagger + S_- a\} (e^{i(\varphi-\omega t)} - e^{-i(\varphi-\omega t)}) \right]. \end{aligned} \quad (7.117)$$

Первое слагаемое в квадратных скобках напоминает обычный гамильтониан Джейнса–Каммингса (подразд. 7.5.2), который соответствовал бы спину, закрепленному в точке $z = 0$. Однако мы сделали существенное упрощение, а именно, что электромагнитное поле классическое и фотонные операторы в гамильтониане не входят. Кvantовыми свойствами поля действительно можно пренебречь в случае, если B_1 — сильное когерентное состояние. При этом остается гамильтониан, описывающий эволюцию внутреннего атомного состояния. Когерентное состояние поля при взаимодействии с атомом практически не запутывается с состоянием атома. Читателю, заинтересовавшемуся этим вопросом, рекомендуем обратиться к задаче 7.3 в конце главы. Мы еще столкнемся с этим явлением при обсуждении резонанса в подразд. 7.7.2.

Второе слагаемое (7.117) описывает взаимодействие между колебательным и спиновым состояниями иона. Чтобы его получить, необходимо учесть зависимость магнитного поля от координаты z . Четыре слагаемых в фигурных скобках соответствуют четырем переходам (два вверх и два вниз), которые обычно называются красными и синими боковыми полосами (см. рис. 7.10).

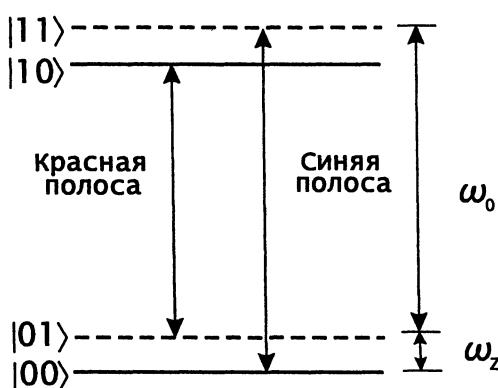


Рис. 7.10. Схема уровней энергии для игрушечной модели ионов в ловушке, демонстрирующая красные и синие боковые полосы, возникающие за счет испускания или поглощения одного фонона. Боковые полосы, описывающие поглощение или испускание нескольких фононов, как правило, не важны. Для состояний использовано обозначение $|n, m\rangle$, где n представляет состояние спина, а m — число фононов.

Переходы боковых полос имеют частоты $\omega_0 \pm \omega_z$. Чтобы убедиться в этом, мы должны учесть гамильтониан свободной частицы

$$H_0 = \hbar\omega_0 S_z + \hbar\omega_z a^\dagger a. \quad (7.118)$$

Если использовать представление взаимодействия с гамильтонианом H_0 , спиновые и фононные операторы оказываются зависящими от времени:

$$S_+(t) = S_+ e^{-\omega_0 t}, \quad S_-(t) = S_- e^{-\omega_0 t}, \quad (7.119)$$

$$a^\dagger(t) = a^\dagger e^{i\omega_z t}, \quad a(t) = a e^{-i\omega_z t}. \quad (7.120)$$

Соответственно интересующие нас члены в $H'_I = e^{iH_0 t/\hbar} H_I e^{-iH_0 t/\hbar}$ оказываются равными

$$H'_I = \begin{cases} i\frac{\eta\hbar\Omega}{2}(S_+ a^\dagger e^{i\varphi} - S_- a e^{-i\varphi}), & \omega = \omega_0 + \omega_z, \\ i\frac{\eta\hbar\Omega}{2}(S_+ a e^{i\varphi} - S_- a^\dagger e^{-i\varphi}), & \omega = \omega_0 - \omega_z, \end{cases} \quad (7.121)$$

где ω — частота внешнего поля, записанная справа.

Можно легко обобщить данную модель на случай N спинов, удерживаемых в параболическом потенциале, если предположить, что система спинов может колебаться только как единое целое, т. е., что энергия трансляционной моды много меньше энергии всех остальных колебательных мод. В этом случае достаточно просто заменить ω_z на ω_z/\sqrt{N} , поскольку эффективная масса составной частицы равна NM .

7.6.3 Квантовые вычисления

Для квантовых вычислений необходимо уметь реализовать произвольное-unitарное преобразование над внутренними состояниями атомов. Мы объясним, как это делается в три этапа. Сначала опишем, как выполнять произвольную однокубитовую операцию, действуя только на один атомный спин. Затем предложим метод, позволяющий реализовать нетривиальный двухкубитовый элемент, причем один кубит будет представлен атомным спином, а другой — фононом. И наконец объясним, как осуществить обмен квантовой информацией между спином и фононом. После этого мы опишем эксперимент, который продемонстрировал приготовление начального состояния, реализацию CNOT и измерение результата.

Однокубитовые операции

Во внешнем электромагнитном поле с частотой ω_0 в гамильтониане появляется слагаемое

$$H_I = \frac{\hbar\Omega}{2} (S_+ e^{i\varphi} + S_- e^{-i\varphi}). \quad (7.122)$$

Выбрав фазу φ и время, на которое включается поле, соответствующим образом, можно реализовать оператор $R_x(\theta) = \exp(-i\theta S_x)$ или $R_y(\theta) = \exp(-i\theta S_y)$. Согласно теореме 4.1, эти операторы позволяют выполнять произвольные операции над одним спиновым состоянием. В случае нескольких ионов будем использовать дополнительный индекс j , указывающий, к какому именно иону применяется операция, например $R_{xj}(\theta)$.

Упражнение 7.31. Постройте элемент Адамара из вращений R_y и R_z .

Управляемое переворачивание фазы

Предположим теперь, что один кубит представлен при помощи атомного спина, а второй кубит — фононными состояниями $|0\rangle$ и $|1\rangle$. Оказывается, что в этом случае можно реализовать управляемое переворачивание фазы, т. е. унитарное преобразование

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}. \quad (7.123)$$

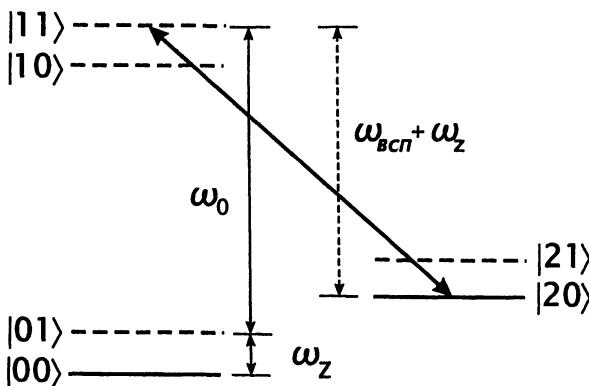


Рис. 7.11. Уровни энергии трехуровневого атома, помещенного в ионную ловушку. Для каждого атомного уровня изображено два фононных состояния. Состояния обозначаются как $|n, m\rangle$, где n — номер атомного состояния, а m — число фононов. Для реализации управляемого переворачивания фазы используется переход $|20\rangle \leftrightarrow |11\rangle$

Основную идею проще всего понять, если рассмотреть трехуровневый атом, находящийся в ловушке (в принципе, можно обойтись и двумя уровнями, см. задачу 7.4). На рис. 7.11 показаны уровни энергии такой системы. Лазерное излучение с частотой $\omega_{\text{всп}} + \omega_z$ ($\omega_{\text{всп}}$ — вспомогательная частота) индуцирует переходы между состояниями $|20\rangle$ и $|11\rangle$, которые описываются гамильтонианом

$$H_{\text{всп}} = i \frac{\eta \hbar \Omega'}{2} (S_+ e^{i\varphi} + S_- e^{-i\varphi}). \quad (7.124)$$

Отметим, что никакой другой переход на этой частоте невозможен. Выберем фазу φ и длительность импульса так, чтобы реализовать оператор $R_x(2\pi)$. В результате состояния $|11\rangle$ и $|20\rangle$ изменят знак, а все остальные состояния не изменятся (предполагается, что в начальном состоянии амплитуды неиспользуемых в вычислении состояний, таких как $|12\rangle$, равны нулю). Эта процедура позволяет реализовать нужное нам преобразование (7.123). Обозначим его как $C_j(Z)$, где j — номер иона, на который мы действуем (операция 'управляемый-Z'). Поскольку мы используем фонон трансляционной моды, он является общим для всех ионов. По этой причине в литературе используется термин кубит фононной «шины» (в соответствии с электротехнической терминологией).

Элемент обмена

Теперь объясним, как осуществить обмен кубитов, представленных спиновым и фононным состояниями. Для этого нам понадобится лазер с частотой $\omega_0 - \omega_z$. Выбирая фазу излучения и длительность импульса, можно реализовать вращение $R_y(\pi)$ подпространств $|01\rangle$ и $|10\rangle$. Соответственно, на подпространстве, порожденном векторами $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$, реализуется унитарное преобразование

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \quad (7.125)$$

Если начальным состоянием системы было $a|00\rangle + b|10\rangle$ (фононы в состоянии $|0\rangle$), то конечным состоянием будет $a|00\rangle + b|01\rangle$. Мы видим, что состояния спина и фонона поменялись местами. Обозначим операцию (7.125), примененную к иону j , как SWAP_j , а обратную к ней операцию, которая соответствует $R_y(\pi)$, как $\overline{\text{SWAP}}_j$. Операция SWAP_j не совпадает буквально с операцией обмена (поскольку $|10\rangle\langle 01|$ входит в $R_y(\pi)$ со знаком минус), но она эквивалентна ей с точностью до фазы (см. упр. 4.26). По этой причине иногда она называется не обменом, а "операцией отображения".

Элемент CNOT

Из элементов, которые мы рассмотрели, можно построить элемент CNOT с управляемым ионом j и управляемым ионом k :

$$\text{CNOT}_{jk} = H_k \overline{\text{SWAP}}_k C_j(Z) \text{SWAP}_k H_k. \quad (7.126)$$

Здесь время идет справа налево, H_k — элемент Адамара (сконструированный из вращений R_x и R_y) иона k . Аналогичным образом мы реализовали CNOT в разд. 7.4, используя светоделители и среду Керра (см. формулу (7.46)).

7.6.4 Эксперимент

Опишем эксперимент (см. разд. «История и дополнительная литература» в конце главы), в котором при помощи одного иона в ловушке был реализован

элемент СНОТ. В этом эксперименте одинокий ион ${}^9\text{Be}^+$ удерживался в ионной ловушке с коаксиальным радиочастотным резонатором, которая показана на рис. 7.12. Она геометрически отличается от линейной ловушки, изображенной на рис. 7.7, однако, принцип ее работы аналогичный. Выбор берилля диктовался удобной структурой его электронных и сверхтонких уровней (см. рис. 7.13). В качестве внутренних состояний атома, представляющих первый кубит, использовались уровни ${}^2S_{1/2}(1, 1)$ и ${}^2S_{1/2}(2, 2)$, см. упр. 7.28. Второй кубит был представлен фононными состояниями $|0\rangle$ и $|1\rangle$ (помеченными на рисунке как $n = 0$ и $n = 1$). Переход между уровнями ${}^2S_{1/2}(1, 1)$ и ${}^2S_{1/2}(2, 2)$, длина волны которого ≈ 313 нм, индуцировался при помощи не одного, а двух лазеров, так что разность их частот была равна частоте перехода. Использование такого рамановского перехода ослабляет требования, предъявляемые к стабильности фазы лазера. В качестве вспомогательного уровня использовалось состояние ${}^2S_{1/2}(2, 0)$. Расщепление терма ${}^2S_{1/2}$ достигалось за счет внешнего магнитного поля 1,8 гс. Частоты колебаний иона в ловушке были равны

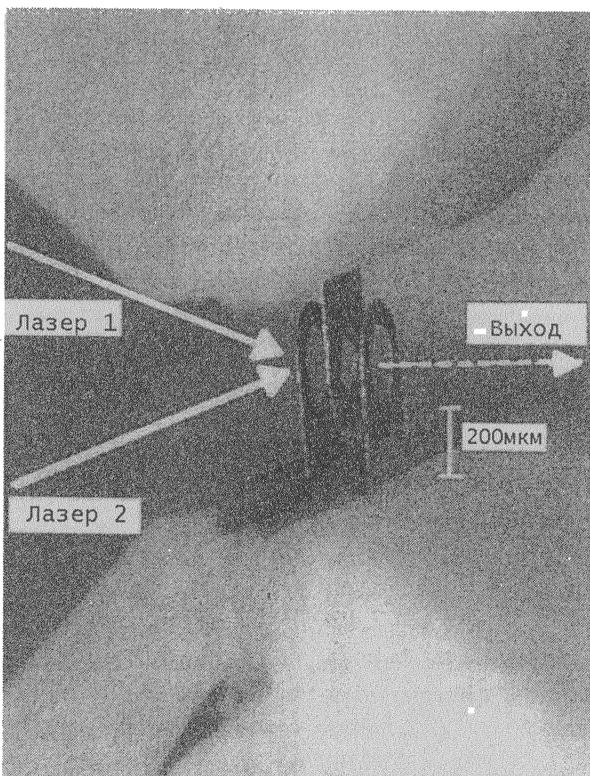


Рис. 7.12. Микроскопическая ионная ловушка с коаксиальными электродами, в которой удерживались ионы бария (все основные результаты, касающиеся ионов берилля, применимы также к ионам бария). Фотография Р. Деву и К. Куртзифера, исследовательский центр IBM.

$(\omega_x; \omega_y; \omega_z)/2\pi = (11, 2; 18, 2; 29, 8)$ МГц, а амплитуда нулевых колебаний около 7 нм, что соответствует параметру Лэмба-Дика $\eta_x = 0, 2$. Частота Раби $\Omega/2\pi = 140$ кГц. Две боковые полосы сдвинуты от нее на $\eta_x\Omega/2\pi = 30$ кГц, а для вспомогательного перехода на $\eta_x\Omega'/2\pi = 12$ кГц.

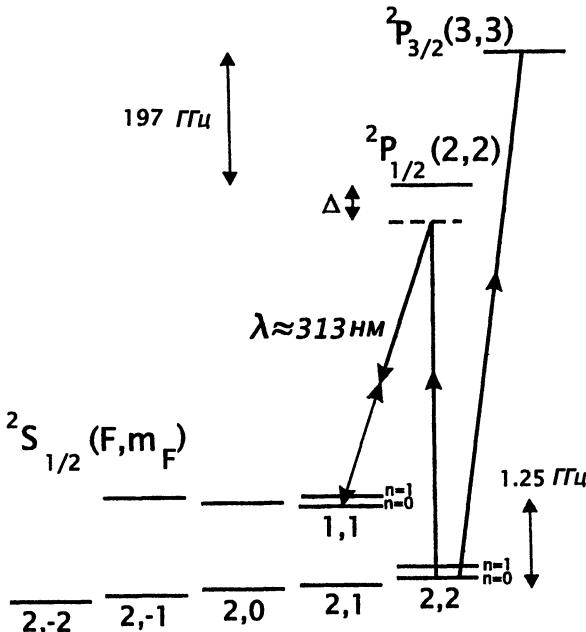


Рис. 7.13. Уровни энергии иона ${}^9\text{Be}^+$ в ионной ловушке (Рисунок К. Монро, NIST.)

В результате доплеровского охлаждения и охлаждения методом боковой полосы ион с вероятностью примерно 95% оказывался в состоянии $|00\rangle = |{}^2S_{1/2}(2, 2)\rangle|n_x = 0\rangle$. Далее с помощью однокубитовых операций приправлялось одно из четырех базисных состояний иона $|00\rangle, |01\rangle, |10\rangle, |11\rangle$, после чего выполнялась операция CNOT. Для этого использовалась последовательность из трех операций: вращение $R_y(\pi/2)$ на кубите, представленном внутренним состоянием иона, операция 'контролируемый-Z' между двумя кубитами и, наконец, вращение $R_y(-\pi/2)$ на кубите, представленном внутренним состоянием иона. Соответствующая схема изображена на рис. 7.14 и, как негрудно убедиться (упр. 7.32), она действительно реализует элемент CNOT.

Считывание конечного результата осуществлялось при помощи двух измерений флюоресцентного излучения иона. В первом измерении регистрировалась флюоресценция, соответствующая возбужденному уровню ${}^2P_{3/2}(3, 3)$. Для этого на ион направлялось лазерное излучение, поляризованное по кругу и с частотой, равной частоте перехода ${}^2S_{1/2}(2, 2) - {}^2P_{3/2}(3, 3)$. Такое излучение практически никак не взаимодействует с состоянием ${}^2S_{1/2}(1, 1)$, поэтому интенсивность флюоресцентного излучения пропорциональна вероятности того, что

атом находился в состоянии $^2S_{1/2}(2, 2)$ (а соответствующий кубит в состоянии $|0\rangle$). Заметим, что это проективное измерение.

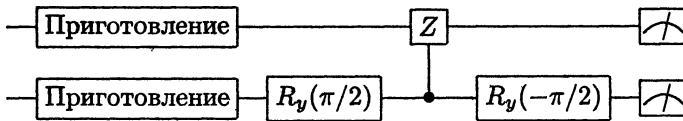


Рис. 7.14. Квантовая схема, использованная для экспериментальной реализации операции СНОТ. Верхняя линия представляет фононную моду, а нижня — внутреннее состояние иона (сверхтонкая структура).

Подобная схема измерения имеет замечательную особенность — она позволяет накапливать статистику, поскольку акт флюoresценции может циклически повторяться много раз. В каждом цикле ион поглощает фотон, переходя на уровень $^2P_{3/2}(3, 3)$, и затем испускает фотон, возвращаясь обратно на уровень $^2S_{1/2}(2, 2)$. Число таких циклов может доходить до нескольких тысяч. Что касается второго измерения, то оно аналогично первому, только предварительно применяется элемент обмена, переставляющий местами два кубита, которые представлены колебательным и внутренним состояниями иона. Таким образом мы можем проективно измерить колебательное состояние иона.

При данной постановке эксперимента результаты измерений позволяют только проверить таблицу значений элемента СНОТ, но в принципе можно приготовить суперпозиции входных состояний и, измеряя конечные матрицы плотности, полностью охарактеризовать унитарное преобразование, которое реализуется в эксперименте. Для этого надо использовать технику томографии процесса (гл. 8). Оптические системы, использованные в эксперименте, позволили реализовать СНОТ за 50 микросекунд. С другой стороны, оценивается время когерентности в сотни или даже тысячи микросекунд. Основными источниками потери когерентности являются нестабильность мощности лазера, частоты и амплитуды радиочастотного поля, формирующего ловушку, а также флуктуации внешних магнитных полей. Следует подчеркнуть, что в эксперименте использовались только один ион и только два кубита, что не очень интересно с вычислительной точки зрения. На практике элемент СНОТ нужно применять к двум различным ионам, а не к одному иону и фононной моде.

Однако, вполне возможно, что все технические трудности в данном методе преодолимы, а время когерентности можно увеличить, используя коротковременное колебательное состояние как можно реже, выигрывая на том, что время когерентности внутренних состояний атома чрезвычайно большое. Кроме того, увеличение числа ионов, по-видимому, вполне реально. Например, на рис. 7.15 показана цепочка из 40 ионов ртути, удерживаемых в ловушке. Конечно, до превращения подобной системы в полезное устройство, обрабатывающее квантовую информацию, еще далеко, но это уже технический вопрос. Возможно, когда-нибудь изображенная цепочка ионов превратится в регистр кубитов квантового компьютера.

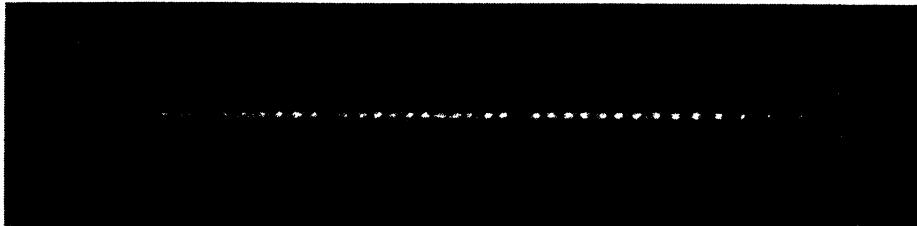


Рис. 7.15. Картина флюoresценции для ≈ 40 ионов ртути ($^{199}\text{Hg}^+$), удерживаемых в ловушке. Расстояние между соседними ионами около 15 микрон. В двух пустых узлах находятся другие изотопы ртути, которые не флюoresцируют на частоте лазера. (Перепечатано с разрешения Д. Уайнленда, NIST.)

Упражнение 7.32. Покажите, что схема, изображенная на рис. 7.14, действительно реализует элемент CNOT (с точностью до относительной фазы), в котором управляющий кубит представлен колебательным состоянием.

Ионы в ловушке как реализация квантового компьютера

- **Представление кубита.** Атомные состояния сверхтонкой структуры (ядерный спин) и низколежащие колебательные моды (фононы) удерживаются в ловушке атомов.
- **Унитарная эволюция.** Произвольное преобразование реализуется последовательностью лазерных импульсов. Они регулируют эволюцию атомных состояний, взаимодействующих с излучением, в соответствии с гамильтонианом Джейнса–Каммингса. Взаимодействие между кубитами происходит через общее фононное состояние.
- **Приготовление начального состояния.** Атомы охлаждаются (захватом в ловушку и оптическими методами) до основного состояния их колебательного движения и до основного состояния сверхтонкой структуры.
- **Измерение конечного результата.** Измерение заселенности уровней сверхтонкой структуры.
- **Недостатки.** Время жизни фононов слишком короткое. Трудно приготовить основное колебательное состояние ионов.

7.7 Ядерный магнитный резонанс

В предыдущем разделе мы видели, что ядерные спины были бы идеальной системой для реализации квантовых вычислений при условии, если бы спин–спиновые взаимодействия могли быть достаточно сильными и контролируемыми. Принципиальный недостаток идеи с использованием ионов в ловушке состоял как раз в слабости спин–спинового взаимодействия, а также в быстрой

потере когерентности. Мы могли бы поместить в ловушку не отдельный атом, а молекулу; при этом непосредственное магнитно-дипольное взаимодействие ядер и косвенное взаимодействие через орбитальные электроны привели бы к достаточно сильной связи между спинами. Однако, из-за наличия в спектре молекулы колебательных мод удержать ее в ловушке и охладить очень трудно, так что манипулирование ядерными спинами в молекуле и их измерение оптическими методами, как правило, невозможно.

С другой стороны, существует хорошо разработанный метод, позволяющий манипулировать ядерными спинами и измерять их при помощи радиочастотных импульсов. Он называется ядерным магнитным резонансом (ЯМР). Этот метод широко применяется в химии для изучения свойств жидкостей, газов и твердых веществ, для определения структуры молекул, для исследования материалов и биологических систем. Имея такое количество приложений, современная техника ЯМР позволяет проводить эксперименты, в которых наблюдаются и контролируются десятки, сотни и даже тысячи ядер.

Однако, при использовании ЯМР для квантовых вычислений возникают две проблемы. Во-первых, из-за малой величины ядерного магнитного момента необходимо использовать образцы из большого (порядка 10^8 и больше) числа молекул, для того, чтобы получить наблюдаемый сигнал. Каждая молекула может рассматриваться как отдельный маленький квантовый компьютер, но справедливо ли это для ансамбля молекул? В частности, в методе ЯМР измеряется сигнал, усредненный по молекулам. Может ли быть полезным результат вычислений, усредненный по ансамблю квантовых компьютеров? Во-вторых, при использовании метода ЯМР обычно работают с образцами при комнатной температуре, так что энергия переворота спина $\hbar\omega$ много меньше $k_B T$. Это значит, что начальное состояние системы очень близко к полностью неупорядоченному. В теории квантовых вычислений обычно рассматривается ситуация, когда начальное состояние системы чистое. Можно ли выполнять вычисления, если начальное состояние системы смешанное и имеет большую энтропию?

Решение этих двух проблем сделало ЯМР весьма привлекательным методом реализации квантовых вычислений несмотря на жесткие ограничения, связанные с термодинамической природой используемых систем. Из ЯМР-реализации можно также позаимствовать много полезного, в частности, способы управления реальными гамильтонианами, позволяющие выполнять произвольные унитарные преобразования, методы, дающие возможность обнаружить и уменьшить потерю когерентности (и систематические ошибки). Представляет интерес также сборка всех компонент в единое устройство, выполняющее некоторый квантовый алгоритм. Мы начнем с описания аппаратуры, применяемой в методе ЯМР, и общего вида гамильтониана, а затем обсудим, как при обработке квантовой информации решаются проблемы, связанные с термодинамическим начальным состоянием и с использованием ансамблей. В заключение опишем некоторые эксперименты, демонстрирующие работу квантовых алгоритмов, и укажем на недостатки метода ЯМР.

7.7.1 Физическая аппаратура

Мы начнем с общего описания используемой аппаратуры; соответствующая математическая модель будет приведена позже. Двумя основными частями импульсной установки ЯМР для жидкых образцов, которую мы будем рассматривать, являются ЯМР спектрометр и собственно образец. Молекулы, на которых наблюдается ЯМР, как правило, содержат некоторое число n протонов со спином $1/2$ (существуют и другие возможные ядра, например ^{13}C , ^{19}F , ^{15}N , ^{31}P). В магнитном поле $\sim 11,7$ Тл, протоны имеют частоту ЯМР сигнала около 500 МГц. Разности резонансных частот для различных ядер данной молекулы могут быть от нескольких до сотен килогерц. Это обусловлено различием локальных магнитных полей вблизи ядер из-за экранирующего эффекта электронного окружения. Молекулы, о которых идет речь, как правило, находятся в растворе, так что их концентрация достаточно мала и мы можем пренебречь межмолекулярным взаимодействием. Поэтому система таких молекул может быть описана как ансамбль n -кубитовых квантовых «компьютеров».

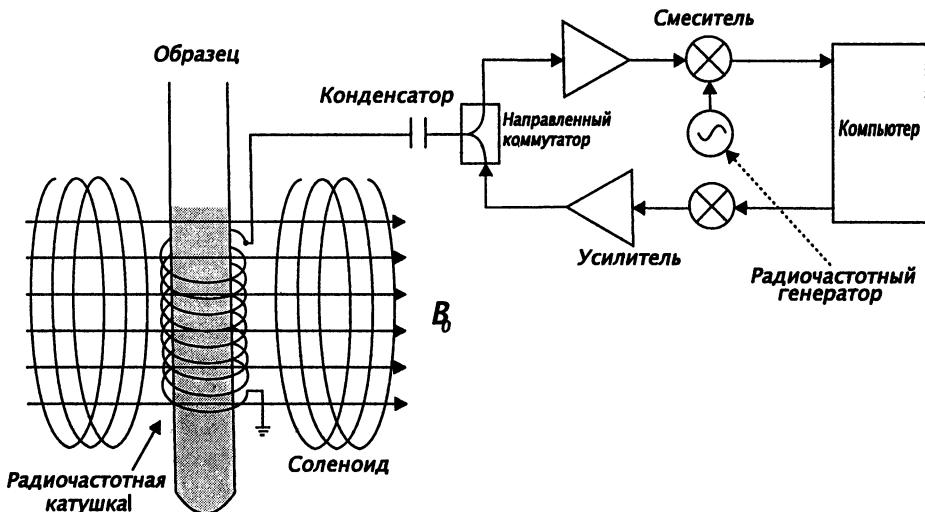


Рис. 7.16. Схематическая диаграмма ЯМР спектрометра.

ЯМР спектрометр состоит из радиочастотных катушек и большого сверхпроводящего магнита, в который в качестве сердечника помещается образец в стеклянной пробирке, как показано на рис. 7.16. Постоянное магнитное поле B_0 , направленное вдоль оси \hat{z} , тщательно настраивается, так что в пределах рабочего объема, приблизительно 1 см^3 , степень неоднородности не превышает 10^{-9} . Расположенные перпендикулярно к магниту катушки Гельмгольца формируют слабое переменное магнитное поле в плоскость $\hat{x} - \hat{y}$. Это поле можно быстро включать и выключать, что позволяет манипулировать ядерными спинами. Те же самые катушки используются также для приема радиочастотного

сигнала, возникающего при прецессии ядерных спинов (подобно тому как вращающийся магнит создает переменный индукционный ток в катушке).

Типичный эксперимент начинается с продолжительного этапа выжидания, цель которого — дать ядрам прийти в состояние термодинамического равновесия; для хорошо подготовленных жидкых образцов соответствующее время может составлять несколько минут. Затем под управлением (классического) компьютера создается последовательность радиочастотных импульсов, которая осуществляет нужное преобразование над состояниями ядер. После этого мощные усилители, формировавшие импульсы, быстро выключаются и при помощи чувствительного предусилителя измеряется конечное состояние спинов. К сигналу *свободной индукции*, который наблюдается в ходе этого измерения, применяется преобразование Фурье. По площади пиков в спектре частот можно определить состояние соответствующих спинов (рис. 7.17).

На практике существует много обстоятельств, приводящих к погрешностям в измерениях такого рода. Например, из-за пространственной неоднородности постоянного магнитного поля ядра в различных частях образца прецессируют с различной частотой, что влияет на ширину линий спектра. Не менее сложная задача — обеспечение пространственной однородности радиочастотного поля. Поскольку оно должно создаваться катушкой, расположенной перпендикулярно к основному магниту, одновременной однородности радиочастотного поля и постоянного поля B_0 добиться не удается. Как правило, радиочастотное поле генерируется маленькой катушкой и является неоднородным, что приводит к погрешностям в управлении ядрами. Важно также обеспечить вполне определенную длительность импульсов и стабильность амплитуды, фазы и частоты поля. Однако, в отличие от метода ионов в ловушке все эти параметры контролируются более просто, поскольку характерные частоты гораздо ниже. Мы еще вернемся к вопросу о погрешностях в подразд. 7.7.4 после изложения математической модели системы и методов обработки квантовой информации с помощью ЯМР.

7.7.2 Гамильтониан

Теорию ЯМР можно понять при помощи моделей с одним и двумя спинами. Сначала мы опишем, как электромагнитное излучение взаимодействует с отдельным ядерным спином. Далее мы рассмотрим физическую природу взаимодействия между ядерными спинами в молекулах. Это позволит нам описать зависимость получаемого сигнала от преобразования, осуществленного над начальным термодинамически равновесным состоянием спинов. Наконец, мы приведем феноменологическую модель потери когерентности и обсудим экспериментальное определение двух ее параметров T_1 и T_2 .

Динамика одного спина

Взаимодействие классического электромагнитного поля с магнитным моментом спина $1/2$ описывается гамильтонианом $H = -\vec{\mu} \cdot \vec{B}$, где оператор $\vec{\mu}$ пропорционален оператору спина, а $\vec{B} = B_0 \hat{z} + B_1(\hat{x} \cos \omega t + \hat{y} \sin \omega t)$ — рассматриваемое

магнитное поле. Напомним, что компонента B_0 постоянная и очень большая, а B_1 , вообще говоря, зависит от времени, но всегда на несколько порядков меньше, чем B_0 . Для изучения этой системы можно было бы применить теорию возмущений. Однако, уравнение Шрёдингера с таким гамильтонианом можно решить точно с помощью формализма матриц Паули (гл. 2), не прибегая к теории возмущений. С помощью них гамильтониан записывается как

$$H = \frac{\omega_0}{2}Z + g(X \cos \omega t + Y \sin \omega t), \quad (7.127)$$

где g и ω_0 пропорциональны амплитудам полей B_1 и B_0 соответственно, а X , Y , Z - матрицы Паули. Если положить $|\varphi(t)\rangle = e^{i\omega t Z/2} |\chi(t)\rangle$, то уравнение Шрёдингера

$$i\partial_t |\chi(t)\rangle = H |\chi(t)\rangle \quad (7.128)$$

перепишется в виде

$$i\partial_t |\varphi(t)\rangle = \left[e^{i\omega Z t/2} H e^{-i\omega Z t/2} - \frac{\omega}{2} Z \right] |\varphi(t)\rangle. \quad (7.129)$$

Поскольку

$$e^{i\omega Z t/2} X e^{-i\omega Z t/2} = (X \cos \omega t - Y \sin \omega t), \quad (7.130)$$

уравнение (7.129) после упрощений записывается как

$$i\partial_t |\varphi(t)\rangle = \left[\frac{\omega_0 - \omega}{2} Z + gX \right] |\varphi(t)\rangle, \quad (7.131)$$

где члены в квадратных скобках могут рассматриваться как эффективный гамильтониан во вращающейся системе отсчета. Решение этого уравнения имеет вид

$$|\varphi(t)\rangle = e^{i[\frac{\omega_0 - \omega}{2} Z + gX]t} |\varphi(0)\rangle. \quad (7.132)$$

Исследуя его, мы приходим к понятию *резонанса*. Действительно, используя (4.8), можно интерпретировать (7.132) как однокубитовое вращение вокруг оси

$$\hat{n} = \frac{\hat{z} + \frac{2g}{\omega_0 - \omega} \hat{x}}{\sqrt{1 + \left(\frac{2g}{\omega_0 - \omega}\right)^2}} \quad (7.133)$$

на угол

$$|\vec{n}| = t \sqrt{\left(\frac{\omega_0 - \omega}{2}\right)^2 + g^2}. \quad (7.134)$$

Если различие между ω и ω_0 велико, влияние поля B_1 на спин несущественно; ось его вращения практически параллельна оси \hat{z} , и динамика примерно совпадает с той, что задается свободным гамильтонианом в поле B_0 . Напротив, если $\omega \approx \omega_0$, можно пренебречь вкладом поля B_0 , так что даже маленькое поле B_1 может привести к значительным изменениям состояния, соответствующим дополнительному вращению вокруг оси \hat{x} . Этот чрезвычайно большой

эффект малого возмущения, имеющего надлежащую частоту, как раз и представляет собой «резонанс» в методе ядерного магнитного резонанса. Тот же самый эффект лежал в основе резонансного взаимодействия двухуровневых атомов с лазерным излучением, которое использовалось (но не объяснялось в подразд. 7.5.1).

Вообще гамильтониан одиночного спина во вращающейся системе отсчета при $\omega = \omega_0$ имеет вид

$$H = g_1(t)X + g_2(t)Y, \quad (7.135)$$

где g_1 и g_2 являются функциями поперечного радиочастотного поля.

Упражнение 7.33 (магнитный резонанс). Покажите, что формула (7.128) действительно сводится к (7.129). Для заданного гамильтониана (7.135) во вращающейся системе отсчета найдите соответствующий гамильтониан в лабораторной системе отсчета.

Упражнение 7.34 (частоты ЯМР). Используя значение ядерного магнетона Бора, найдите частоту прецессии для протона в магнитном поле 11,8 Тл. Кавказа должна быть напряженность B_1 , чтобы повернуть спин на 90° за 10 мкс?

Спин-спиновое взаимодействие

Как правило, ядра, которые мы могли бы использовать, например ^1H , ^{13}C , ^{19}F и ^{15}N , имеют несколько спинов $1/2$. Взаимодействие между спинами возникает за счет двух основных механизмов: непосредственное дипольное взаимодействие и косвенное взаимодействие, происходящее с участием орбитальных электронов. Гамильтониан, описывающий дипольное взаимодействие, имеет вид

$$H_{1,2}^D = \frac{\gamma_1 \gamma_2 \hbar}{4r^3} \left[\vec{\sigma}_1 \cdot \vec{\sigma}_2 - 3(\vec{\sigma}_1 \cdot \hat{n})(\vec{\sigma}_2 \cdot \hat{n}) \right], \quad (7.136)$$

где \hat{n} — единичный вектор, задающий направление от первого ядра ко второму, а $\vec{\sigma}$ — вектор магнитного момента (умноженный на два). В жидкости с малой вязкостью, дипольные взаимодействия исчезают при усреднении по ориентациям молекул. Действительно, если скорость поворота молекулы, определяемая вязкостью, много больше скорости, определяемой силой дипольного взаимодействия, мы можем усреднить $H_{1,2}^D$ по \hat{n} , что дает ноль.

Взаимодействие через орбитальные электроны, называемое также J -связью, возникает благодаря тому, что спины ядер взаимодействуют с электронами своих атомов (контактное взаимодействие Ферми), а волновые функции электронов различных атомов перекрываются друг с другом. Это взаимодействие описывается гамильтонианом

$$H_{1,2}^J = \frac{\hbar J}{4} \vec{\sigma}_1 \cdot \vec{\sigma}_2 = \frac{\hbar J}{4} Z_1 Z_2 + \frac{\hbar J}{8} [\sigma_+ \sigma_- + \sigma_-^* \sigma_+]. \quad (7.137)$$

Нас будет интересовать случай, когда J — скаляр (вообще говоря, это может быть тензор), что является хорошим приближением, если речь идет о жидкости и взаимодействие слабое, или когда два взаимодействующих ядра имеют сильно различающиеся частоты прецессии. В последнем случае

$$H_{12}^J \approx \frac{\hbar}{4} J Z_1 Z_2. \quad (7.138)$$

Упражнение 7.35 (вращательное утоньшение). Покажите, что при усреднении $H_{1,2}^D$ по \hat{n} действительно получается ноль.

Термодинамическое равновесие

Существенное отличие ЯМР от других физических моделей, которые рассматривались ранее в этой главе, состоит в том, что в ЯМР речь идет об ансамбле систем, и все измерения, которые мы делаем, сводятся к усреднению по ансамблю. Кроме того, мы не совершаляем никаких специальных действий, чтобы привести систему в какое-то фиксированное начальное состояние, например в основное состояние; современный уровень эксперимента это пока не позволяет.

Вместо этого мы используем в качестве начального термодинамически равновесное состояние, т. е.

$$\rho = \frac{e^{-\beta H}}{Z}, \quad (7.139)$$

где $\beta = 1/k_B T$, а $Z = \text{tr } e^{-\beta H}$ — статистическая сумма, определяемая из условия нормировки $\text{tr}(\rho) = 1$. Поскольку при комнатной температуре $\beta \approx 10^{-4}$, для большинства ядер мы можем использовать высокотемпературное приближение

$$\rho \approx 2^{-n} [1 - \beta H], \quad (7.140)$$

где n — число спинов.

Так как спин-спиновые взаимодействия малы по сравнению с частотами прецессии спинов, равновесную матрицу плотности ρ в первом приближении можно считать диагональной в Z -базисе, т. е. ее можно рассматривать как статистическую смесь чистых состояний $|00\dots 0\rangle, |00\dots 1\rangle, \dots, |11\dots 1\rangle$. Естественно, это не значит, что каждая из молекул, входящих в ансамбль, может находиться только в одном из этих состояний, поскольку представление матрицы плотности в виде смеси чистых состояний неоднозначно. В принципе истинное физическое состояние может быть измерено методом ЯМР, если есть доступ к отдельным молекулам, но экспериментально это очень сложно.

Упражнение 7.36 (термодинамически равновесное состояние ЯМР). Покажите, что для $n = 1$ равновесное состояние имеет вид

$$\rho \approx \frac{1}{2} - \frac{\hbar\omega}{2k_B T} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad (7.141)$$

а для $n = 2$ и $\omega_a \approx 4\omega_B$

$$\rho \approx \frac{1}{4} - \frac{\hbar\omega_B}{4k_B T} \begin{bmatrix} 5 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & -3 & 0 \\ 0 & 0 & 0 & -5 \end{bmatrix}. \quad (7.142)$$

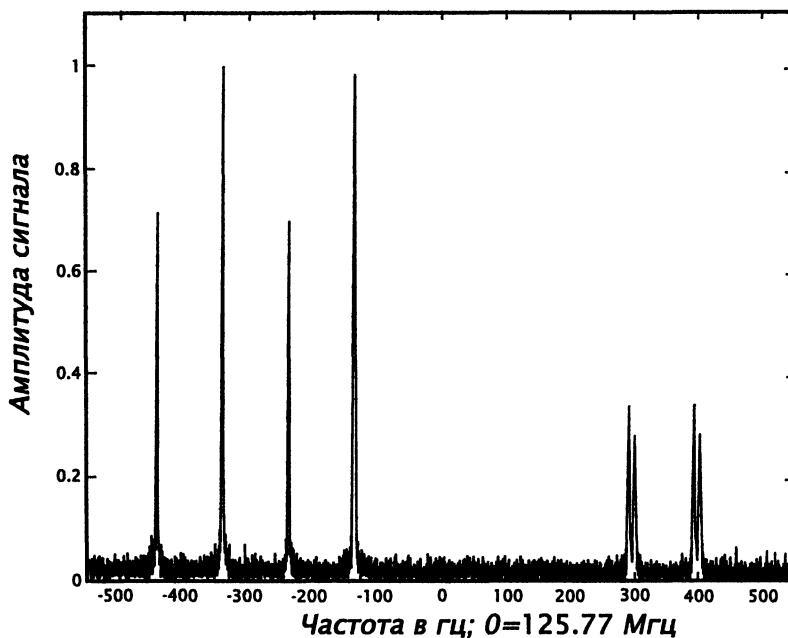


Рис. 7.17. Углеродный спектр трихлорэтилена, маркированного ^{13}C . Четыре линии справа принадлежат ядру углерода, соседнему с протоном, всего их четыре из-за спаривания с протоном и вторым ядром углерода. Четыре расположенных рядом линии слева — сигнал от второго ядра углерода. Оно дальше от протона, чем первое, поэтому спаривание слабее.

Измерение намагниченности

Основная информация, которую можно извлечь из эксперимента, заключена в сигнале свободно затухающей индукции, который мы можем записать как

$$V(t) = V_0 \operatorname{tr} \left[e^{-iHt} \rho e^{iHt} (iX_k + Y_k) \right], \quad (7.143)$$

где матрицы Паули X_k и Y_k действуют только на k -й спин, V_0 — постоянная, зависящая от геометрии катушек, добротности и максимального магнитного потока через образец. Этот сигнал поступает с приемных катушек, измеряющих намагниченность образца в плоскости $\hat{x} - \hat{y}$. В лабораторной системе отсчета этот сигнал модулируется осцилляциями на частоте прецессии ядра ω_0 . Однако, обычно сигнал $V(t)$ смешивается с опорным сигналом частоты ω_0 и после преобразования Фурье мы получим окончательный сигнал, подобный тому, что показан на рис. 7.17.

Упражнение 7.37 (ЯМР спектр для пары связанных спинов). Найдите $V(t)$ для $H = JZ_1Z_2$ и $\rho = e^{i\pi Y_1/4} \frac{1}{4}[1 - \beta \hbar \omega_0(Z_1 + Z_2)]e^{-i\pi Y_1/4}$. Сколько линий было бы в спектре первого спина, если бы гамильтониан был $H = JZ_1(Z_2 + Z_3 + Z_4)$ (с той же начальной матрицей плотности)? Какие были бы относительные высоты этих линий?

Потеря когерентности

Одной из основных характеристик сигнала свободно затухающей индукции, подробное описание которой выходит за рамки нашей модели, является экспоненциальное затухание сигнала намагниченности. Это обусловлено, в частности, неоднородностью постоянного магнитного поля, из-за которой частота прецессии спинов в разных частях образца различна. Эффекты, связанные с неоднородностями поля, в принципе являются обратимыми. Существуют также принципиально необратимые механизмы потери фазы, например спин-спиновое

взаимодействие. Другой необратимый механизм — взаимодействие ядерных спинов с окружающей средой, приводящее к установлению термодинамически равновесного состояния. В ходе этого взаимодействия полная энергия системы спинов изменяется. Если рассматривать состояние только одного спина, эти эффекты можно феноменологически описать следующим преобразованием матрицы плотности:

$$\begin{bmatrix} a & b \\ b^* & 1-a \end{bmatrix} \rightarrow \begin{bmatrix} (a - a_0)e^{-t/T_1} + a_0 & be^{-t/2T_2} \\ b^* e^{-t/2T_2} & (a_0 - a)e^{-t/T_1} + 1 - a_0 \end{bmatrix}, \quad (7.144)$$

где T_1 и T_2 — времена спин-решеточной (продольной) релаксации и спин-спиновой (поперечной) релаксации, а параметр a_0 характеризует равновесное состояние. Два времени релаксации T_1 и T_2 задают важные масштабы, характеризующие время жизни неравновесных классических состояний и квантовых суперпозиций соответственно. Существуют хорошо развитые теоретические методы вычисления T_1 и T_2 для разных веществ; их измерение играет важную роль при использовании ЯМР для химического анализа.

Хорошо известны также экспериментальные методы измерения T_1 и T_2 . Обозначим через $R_x = e^{-i\pi X/4}$ импульс, поворачивающий спин на 90° вокруг оси \hat{x} . Чтобы измерить T_1 , можно применить R_x^2 , затем выждать время τ и применить R_x . Первый импульс поворачивает спин на 180° , после чего он релаксирует в течение времени τ обратно в равновесное состояние (а на сфере Блоха, где северный полюс соответствует основному состоянию, вектор Блоха сначала переворачивается вниз, а затем релаксирует обратно). Второй импульс R_x поворачивает намагниченность на 90° в плоскость $\hat{x} - \hat{y}$, после чего она измеряется. Измеренная намагниченность M как функция τ затухает по экспоненциальному закону $M = M_0[1 - 2 \exp(-\tau/T_1)]$. Для того, чтобы определить T_2 , в первом приближении можно просто измерить ширину резонансного пика. Метод Карра–Парселла–Мэйбума–Гилла позволяет измерить время T_2 более точно. В этом методе сначала применяется операция R_x , после чего совершаются k итераций процедуры «выждать время $\tau/2$, применить R_x^2 , выждать время $\tau/2$, применить R_x^2 ». Данная последовательность импульсов осуществляет периодическую рефокусировку спинов (см. подразд. 7.7.3) и поэтому неоднородности поля B_0 становятся менее существенными. Измеренная намагниченность затухает по закону $M = M_0 e^{k\tau/T_2}$.

Гамильтониан для нескольких спинов

После обсуждения ЯМР-гамильтониана для одного и двух спинов мы можем записать ЯМР-гамильтониан для системы из n связанных спинов:

$$H = \sum_k \omega_k Z_k + \sum_{j,k} H_{j,k}^J + H^{\text{РЧ}} + \sum_{j,k} H_{j,k}^D + H^{\text{cp}}. \quad (7.145)$$

Здесь первое слагаемое описывает свободную прецессию спинов во внешнем поле, H^D — магнито-дипольное взаимодействие (7.136), H^J — спин-спиновое взаимодействие типа « J -связь», (7.137), $H^{\text{РЧ}}$ — внешнее радиочастотное магнитное поле и H^{cp} — взаимодействие с окружающей средой, т. е. совокупность процессов, приводящих к потере когерентности, см. также (7.144).

Для понимания основных свойств этого гамильтониана достаточно рассмотреть его упрощенный вариант

$$H = \sum_k \omega_k Z_k + \sum_{j,k} Z_j \otimes Z_k + \sum_k g_k^x(t) X_k + g_k^y(t) Y_k. \quad (7.146)$$

Исследование более общего гамильтониана (7.145) основывается на тех же идеях.

7.7.3 Квантовые вычисления

При обработке квантовой информации мы применяем к системе, приготовленной в надлежащем начальном состоянии, набор унитарных преобразований. В связи с использованием для этих целей ЯМР возникают три вопроса. Во-первых, как реализовать произвольное унитарное преобразование над системой из n связанных спинов, описываемой гамильтонианом (7.146)? Во-вторых, можно ли использовать термодинамически равновесное состояние (7.140) в качестве начального состояния? И наконец, можно ли заменить проективные измерения, используемые в квантовых алгоритмах, на усредненные по ансамблю изменения, которые реализуются при использовании ЯМР? Цель данного раздела состоит в том, чтобы ответить на эти вопросы.

Рефокусировка

Для реализации произвольных унитарных операторов с помощью гамильтониана (7.146) предложен очень интересный метод, обычно называемый *рефокусировкой*. Рассмотрим простой гамильтониан для двух спинов, $H = H^{\text{сис}} + H^{\text{РЧ}}$, где

$$H^{\text{сис}} = aZ_1 + bZ_2 + cZ_1Z_2. \quad (7.147)$$

Как было показано в подразд. 7.7.2, если радиочастотное поле достаточно сильное и имеет частоту, близкую к резонансной, можно использовать приближение

$$e^{-iHt/\hbar} \approx e^{-iH^{\text{РЧ}}t/\hbar}. \quad (7.148)$$

Это позволяет выполнять однокубитовые операции с большой точностью. Определим поворот спина 1 на 90° вокруг оси \hat{x} как

$$R_{x1} = e^{-i\pi X_1/4} \quad (7.149)$$

(и аналогично для спина 2). Поворот на 180° , R_{x1}^2 , как легко проверить, обладает следующим специальным свойством:

$$R_{x2}^2 e^{-iaZ_1 t} R_{x1}^2 = e^{iaZ_1 t}. \quad (7.150)$$

Это свойство используется для рефокусировки, поскольку оно позволяет эффективно обратить время для одного из спинов. Если спины с различными частотами прецессии стартовали из одной точки на сфере Блоха, то после рефокусировки они опять попадут в эту точку. Соответствующие 180° -импульсы называются импульсами рефокусировки. Заметим, что в выражении (7.150) параметр a может быть и оператором, если только он не действует на первый спин. Таким образом, можем записать

$$e^{-iH^{\text{csc}} t/\hbar} R_{x1}^2 e^{-iH^{\text{csc}} t/\hbar} R_{x1}^2 = e^{-2ibZ_2 t/\hbar}. \quad (7.151)$$

Используя аналогичные импульсы рефокусировки для спина 2, можно было бы исключить и оставшийся член гамильтониана. Таким образом, рефокусировка очень полезна, если мы хотим «выключить» какую-то часть гамильтониана (например взаимодействие между спинами), или вообще не рассматривать эволюцию во времени.

Упражнение 7.38 (рефокусировка). Проверьте соотношение (7.150) (используйте антикоммутативность матриц Паули).

Упражнение 7.39 (трехмерная рефокусировка). Предложите последовательность импульсов для рефокусировки, с помощью которой можно «выключить» произвольный гамильтониан $H^{\text{csc}} = \sum_k c_k \sigma_k$ для одиночного спина.

Упражнение 7.40 (рефокусировка дипольных взаимодействий). Предложите последовательность импульсов, с помощью которой можно привести гамильтониан дипольного взаимодействия $H_{1,2}^D$ к упрощенному виду (7.138).

Элемент CNOT

Элемент CNOT можно реализовать, используя рефокусировку и однокубитовые операции. Покажем сначала, как это делается на примере системы двух спинов с гамильтонианом (7.147). Как мы уже знаем (см. (7.46)), достаточно уметь реализовать унитарный оператор

$$U_{CZ} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}. \quad (7.152)$$

Но поскольку $\sqrt{i}e^{iZ_1Z_2\pi/4}e^{-iZ_1\pi/4}e^{-iZ_2\pi/4} = U_{CZ}$, реализация CNOT сводится к эволюции в течение времени $\hbar\pi/4c$ и к нескольким дополнительным однокубитовым операциям.

Упражнение 7.41 (реализация CNOT с помощью ЯМР). Предложите последовательность однокубитовых вращений, которая реализует CNOT на двух спинах, эволюционирующих в соответствии с гамильтонианом (7.147). (Вы можете использовать выражение (7.46), однако результат можно упростить, уменьшив число однокубитовых вращений.)

Временная, пространственная и логическая разметка

Возможность реализовать произвольное унитарное преобразование с большой точностью, используя радиочастотные импульсы, — одна из наиболее привлекательных сторон метода ЯМР для квантовых вычислений. Однако, основной недостаток состоит в том, что начальное состояние обычно есть равновесное состояние (7.140). Несмотря на то, что это состояние имеет большую энтропию, квантовые вычисления, тем не менее, могут быть выполнены с некоторыми дополнительными затратами. Для этого можно использовать временную или логическую разметку.

Временная разметка, называемая также временным усреднением, основана на двух важных обстоятельствах: все квантовые операции линейны, а все измеряемые в методе ЯМР наблюдаемые — это операторы, имеющие нулевой след (по поводу квантовых измерений см. подразд. 2.2.5). Предположим, что начальное состояние двухспиновой системы описывается матрицей плотности

$$\rho_1 = \begin{bmatrix} a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & c & 0 \\ 0 & 0 & 0 & b \end{bmatrix}, \quad (7.153)$$

где a, b, c, d — произвольные положительные числа, удовлетворяющие условию нормировки $a + b + c + d = 1$. Используя элементы CNOT, можно реализовать схему P , которая переставляет состояния, т. е.

$$\rho_2 = P\rho_1P^\dagger = \begin{bmatrix} a & 0 & 0 & 0 \\ 0 & c & 0 & 0 \\ 0 & 0 & d & 0 \\ 0 & 0 & 0 & b \end{bmatrix}, \quad (7.154)$$

и аналогично

$$\rho_3 = P^\dagger\rho_1P = \begin{bmatrix} a & 0 & 0 & 0 \\ 0 & d & 0 & 0 \\ 0 & 0 & b & 0 \\ 0 & 0 & 0 & c \end{bmatrix}. \quad (7.155)$$

Применяя произвольную заданную квантовую схему U к этим трем состояниям, мы получим (в трех независимых экспериментах, выполненных в разное время) три конечных состояния $C_k = U\rho_k U^\dagger$. Из линейности имеем

$$\sum_{k=1,2,3} C_k = \sum_k U\rho_k U^\dagger \quad (7.156)$$

$$= U \left[\sum_k \rho_k \right] U^\dagger \quad (7.157)$$

$$= (4a - 1)U \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} U^\dagger + (1 - a) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \quad (7.158)$$

При использовании метода ЯМР все измеряемые наблюдаемые M — это операторы, имеющие нулевой след $\text{tr}(M) = 0$ (например, матрицы Паули X и Y), поэтому

$$\text{tr} \left(\sum_k C_k M \right) = \sum_k \text{tr} (C_k M) \quad (7.159)$$

$$= (4a - 1) \text{tr} \left(U \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} U^\dagger M \right) \quad (7.160)$$

$$= (4a - 1) \text{tr}(U|00\rangle\langle 00|U^\dagger). \quad (7.161)$$

Это значит, что сумма трех измеренных сигналов пропорциональна сигналу, который бы мы получили, взяв в качестве начального чистое состояние $|00\rangle\langle 00|$ вместо смешанного состояния (7.153). То же самое можно проделать с произвольным числом спинов, нужно только суммировать по большему числу экспериментов и иметь достаточно большое время когерентности, чтобы успеть выполнить все необходимые унитарные операции до потери когерентности. Заметим, что эксперименты, соответствующие различным C_k , могли бы проводиться одновременно с тремя различными образцами, или с различными частями одного образца; в эксперименте для этого необходимо использовать пространственно неоднородные магнитные поля. Такая методика называется пространственной разметкой.

Упражнение 7.42 (перестановки для временной разметки). Предложите квантовую схему, которая реализует перестановки P и P^\dagger , необходимые для преобразования ρ_1 из (7.153) в ρ_2 из (7.154).

В случае логической разметки используется похожая конструкция, но при этом не требуется проведение нескольких экспериментов. Рассмотрим систему из трех эквивалентных спинов, находящуюся в состоянии

$$\rho = \delta I + \alpha \begin{bmatrix} 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -6 \end{bmatrix} \quad (7.162)$$

$$\approx \left(\delta' I + \alpha' \begin{bmatrix} 2 & 0 \\ 0 & -2 \end{bmatrix} \right)^{\otimes 3}, \quad (7.163)$$

где δI — слагаемое, пропорциональное единичному оператору, которое является ненаблюдаемым (напомним, что все наблюдаемые имеют нулевой след), а $\alpha \ll \delta$ — малый параметр. Теперь применим унитарную операцию, реализующую перестановку \tilde{P} , такую, что

$$\rho' = \tilde{P} \rho \tilde{P}^\dagger = \delta I + \alpha \begin{bmatrix} 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -6 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}. \quad (7.164)$$

Заметим, что верхний 4×4 блок этой матрицы имеет вид

$$\begin{bmatrix} 6 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & -2 \end{bmatrix} = 8|00\rangle\langle 00| - 2I, \quad (7.165)$$

где I обозначает единичную матрицу размера 4×4 . Как и в случае временной разметки, вычисление, выполненное с начальным состоянием ρ' (на подпространстве состояний $|000\rangle, |001\rangle, |010\rangle, |011\rangle$), дает при измерении сигнал, пропорциональный тому, который бы мы получили, взяв в качестве начального чистое состояние $|00\rangle\langle 00|$! Экспериментально оказывается возможным реализовать перестановку \tilde{P} и выделить сигнал от четырех нужных нам состояний.

Состояния вида $\rho = 2^{-n}(1 - \varepsilon)I + \varepsilon U|00\dots 0\rangle\langle 00\dots 0|U^\dagger$ (где U — произвольный унитарный оператор, а n — число кубитов) называются «эффективно чистыми», или «псевдо чистыми» состояниями (данное определение легко

обобщить на случай, когда размерность пространства состояний не является степенью двойки). Существует много стратегий, позволяющих приготовить эффективно чистые состояния, но, как правило, это требует дополнительных ресурсов. Мы еще вернемся к этой теме в подразд. 7.7.4. С помощью эффективно чистых состояний можно наблюдать динамику при нулевой температуре, тогда как система реально находится в высокотемпературном состоянии. Но для этого, конечно, нужно, чтобы связь данной системы с высокотемпературным окружением была достаточно слабой. Именно это и используется в квантовых вычислениях методом ЯМР.

Упражнение 7.43 (перестановки для логической разметки). Предложите квантовую схему, которая реализует перестановку \tilde{P} , необходимую для преобразования ρ_1 из (7.163) в ρ' из (7.165).

Упражнение 7.44 (логическая разметка для n спинов). Рассмотрим систему из n эквивалентных спинов с частотой прецессии ω в состоянии ρ термодинамического равновесия при температуре T . Сколько эффективно чистых спинов можно приготовить из ρ , используя логическую разметку? (Указание. Воспользуйтесь базисными состояниями с весом Хэмминга $n/2$.)

Использование ансамблевых измерений для квантовых алгоритмов

Мы показали, как над системой из n спинов, описываемых гамильтонианом (7.146), можно реализовать произвольное унитарное преобразование, а также, как исходя из равновесного состояния, можно приготовить хорошо определенное входное состояние, которое ведет себя, как чистое. Однако, чтобы выполнить все условия для квантовых вычислений, нужно еще уметь делать измерения над системой, чтобы извлекать результат вычислений. Трудность состоит в том, что результатом работы квантового алгоритма, как правило, является случайная величина. Зная ее распределение вероятностей, можно решить задачу. К сожалению, знание только среднего значения этой случайной величины вообще говоря еще не дает всей необходимой для нахождения ответа информации. Если, используя метод ЯМР, мы выполним квантовый алгоритм без всякой его модификации, то получим именно среднее значение, поскольку измерение выполняется не над отдельной n -спиновой молекулой, а над большим ансамблем таких молекул.

Эту трудность иллюстрирует следующий пример. Квантовый алгоритм разложения на множители дает в качестве промежуточного результата случайное рациональное число вида c/r , где c — неизвестное целое число, а r — целое число, которое нас интересует. Подчеркнем, что число c/r получается при использовании проективных измерений. Далее, используя классический алгоритм разложения в цепные дроби, можно с большой вероятностью определить число c (подразд. 5.3.1). Затем мы проверяем, является ли число r делителем, и если нет, повторяем весь алгоритм еще раз. К сожалению, в случае ансамблевых измерений можно узнать только среднее $\langle c/r \rangle$. Поскольку c распределено приблизительно равномерно, из этого среднего нельзя извлечь никакой информации о значении r .

Тем не менее, у этой проблемы существует простое решение, которое применимо вообще ко всем алгоритмам, связанным с задачей о скрытой подгруппе (гл. 5). Оно состоит в том, чтобы включить все классические вычисления, завершающие работу алгоритма, в квантовую часть алгоритма. Это всегда возможно, поскольку классические вычисления это частный случай квантовых. В вышеприведенном примере каждый квантовый компьютер, входящий в ансамбль (т. е. каждая молекула) должна выполнить разложение в цепную дробь, найти r и проверить, является ли r делителем. Далее, можно модифицировать алгоритм так, что в измеряемый сигнал дадут вклад лишь те молекулы, в которых проверка на делимость прошла успешно. Окончательным результатом измерения будет среднее по ансамблю число $\langle r \rangle$.

7.7.4 Эксперимент

Одним из наиболее привлекательных аспектов метода ЯМР является то, что уже удалось экспериментально осуществить некоторые квантовые вычисления. В этом разделе, завершающем обсуждение метода ЯМР, мы кратко опишем три эксперимента, продемонстрировавших томографию квантового состояния, элементарные логические элементы и квантовый алгоритм поиска. Мы также обсудим недостатки метода ЯМР.

Томография квантового состояния

Как мы обычно отлаживаем программу на классическом компьютере? Ее работу можно проанализировать, измеряя внутреннее состояние компьютера в различные моменты времени. Аналогично, в случае квантового компьютера нам потребуется методика, позволяющая определить его матрицу плотности. Эта методика называется *томографией квантового состояния*.

Напомним, что матрица плотности одного кубита может быть представлена как

$$\rho = \frac{1}{2} \left[1 + \sum_k r_k \sigma_k \right], \quad (7.166)$$

где σ_k — матрицы Паули, а r_k — вещественный трехкомпонентный вектор. Поскольку матрица Паули обладает свойством ортогональности

$$\text{tr}(\sigma_k \sigma_j) = 2\delta_{kj} \quad (7.167)$$

можно восстановить ρ , зная результаты трех измерений

$$r_k = \langle \sigma_k \rangle = \text{tr}(\rho \sigma_k). \quad (7.168)$$

Если предварительно применить нужные однокубитовые импульсы, стандартное ЯМР измерение (7.143) позволит определить $\langle \sigma_k \rangle$, и, таким образом, найти ρ . Аналогичное утверждение справедливо и для большего числа спинов. На

практике удобно работать с бесследовой частью матрицы ρ , которая называется разностной формой матрицы плотности. Примеры томографии для двух и для трех спинов показаны на рис. 7.18.

Упражнение 7.45 (ЯМР-томография квантовых состояний). Рассмотрим систему из двух спинов в состоянии ρ . В девяти экспериментах измеряется девять сигналов $V_k(t) = V_0 \text{tr} [e^{-iHt} M_k \rho M_k^\dagger e^{iHt} (iX_k + Y_k)]$, здесь $M_0 = I$, $M_1 = R_{x1}$, $M_2 = R_{y1}$, $M_3 = R_{x2}$, $M_4 = R_{x2}R_{x1}$, $M_5 = R_{x2}R_{y1}$, и т. д. Покажите что эти эксперименты позволяют однозначно восстановить состояние системы ρ .

Упражнение 7.46. Сколько экспериментов достаточно (необходимо) провести для ЯМР-томографии состояния трех спинов?

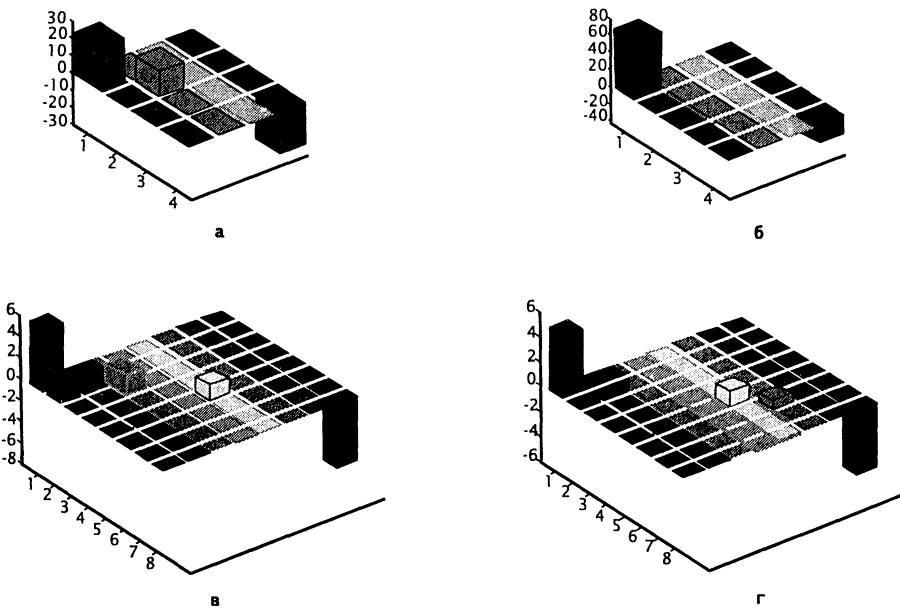


Рис. 7.18. Экспериментальное измерение матрицы плотности в разностной форме. Выбран условный масштаб по вертикальной оси и показаны лишь вещественные части матричных элементов; все мнимые части малы по сравнению с вещественными. Слева вверху а — термодинамически равновесное состояние двух спинов ЯМР наблюдался на протоне и ядре углерода в молекуле хлороформа ($^{13}\text{CHCl}_3$) в магнитном поле 11,78 Тл. Образец был приготовлен в виде раствора 0,5 миллилитров (200 миллимолей) хлороформа в ацетоне- d_6 , дегазованного и запаянного в тонкостенную пятимиллиметровую ампулу. б — эффективно чистое состояние, приготовленное с использованием временной разметки на молекуле хлороформа, см. (7.161). в — термодинамически равновесное состояние трех спинов ЯМР наблюдался на трех ядрах фтора в молекуле трифторметилена. г — эффективно чистое состояние системы из трех спинов, приготовленное с использованием логической разметки, см. (7.164).

Квантовые логические элементы

В силу ряда причин два ядерных спина протона и углерода в молекуле хлороформа представляют собой очень хорошую систему для реализации одноку-

битовых и двухкубитовых логических элементов. В поле $\approx 11,8$ Тл частоты прецессии этих спинов равны ≈ 500 МГц и ≈ 125 МГц. Таким образом, резонансные частоты хорошо разнесены и можно избирательно воздействовать на каждый спин. Частота спин-спиновой J -связи равна 215 Гц. Соответствующий ей период гораздо больше длительности радиочастотных импульсов, но вместе с тем гораздо меньше характерного времени релаксации. Типичные времена релаксации: $T_1 = 18$ с и $T_2 = 7$ с для протона; $T_1 = 25$ с и $T_2 = 0,3$ с для углерода. Такая малая величина T_2 для углерода обусловлена его взаимодействием с тремя квадрупольными моментами ядер хлора. Тем не менее, оценивая произведение наименьшего T_2 на частоту J -связи, мы видим, что за время когерентности можно реализовать примерно 60 логических элементов.

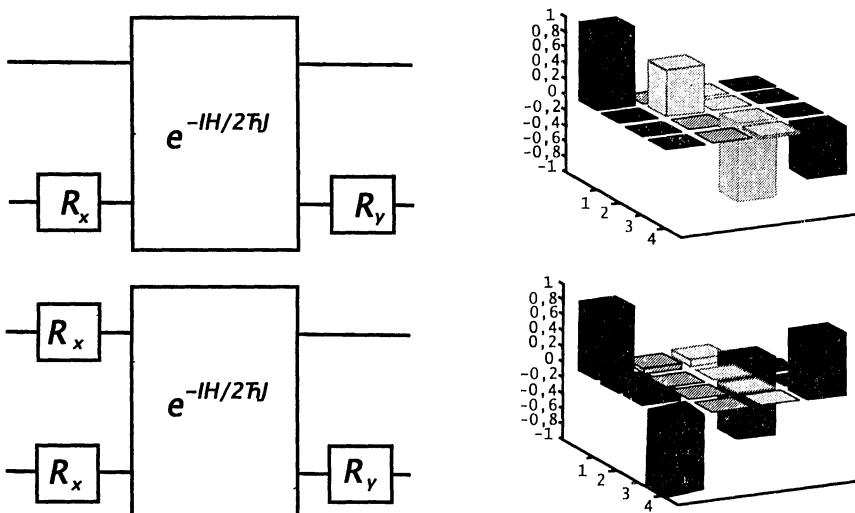


Рис. 7.19. Квантовые схемы, реализованные методом ЯМР, и вещественные части экспериментально измеренных матриц плотности в разностной форме. На изображенных схемах R_x и R_y — однокубитовые повороты на 90° вокруг осей \hat{x} и \hat{y} , реализованные радиочастотными импульсами длительности около 10 мкс. Двухкубитовый оператор $e^{-iH/2\hbar J}$ описывает свободную эволюцию в течение времени $1/2J \approx 2,3$ мс. Наверху схема для элемента CNOT с термодинамически равновесным состоянием на входе. В выходном состоянии диагональные элементы, соответствующие $|10\rangle$ и $|11\rangle$, переставлены, что соответствует классической таблице значений элемента CNOT. Внизу, схема, создающая состояние Белла $(|00\rangle - |11\rangle)/\sqrt{2}$, и результат ее работы. На вход схемы подается эффективно чистое состояние $|00\rangle$.

Гамильтониан этой двухспиновой системы хорошо аппроксимируется выражением (7.147). Его можно существенно упростить, если использовать в эксперименте два вспомогательных модулирующих осциллятора, частоты которых равны частотам прецессии протона и углерода. Во вращающейся системе отсчета, определяемой этими осцилляторами, упрощенный гамильтониан имеет вид

$$H = 2\pi\hbar Z_1 Z_2, \quad (7.169)$$

где $J = 215$ кГц. С помощью этого гамильтониана можно легко реализовать

элемент CNOT. На рис. 7.19 изображена схема, реализующая CNOT с точностью до однокубитовых фазовых сдвигов, а также схема, создающая состояние Белла. Для каждой схемы показаны экспериментально измеренные результаты.

Упражнение 7.47 (ЯМР-реализация CNOT). Проверьте, что схема, изображенная в верхней части рис. 7.19, действительно реализует элемент CNOT с точностью до однокубитовых фазовых сдвигов (т. е. что она правильно представляет классические входные состояния и после применения дополнительных однокубитовых R_z -вращений превращается в квантовый CNOT). Предложите еще одну схему из тех же самых блоков, реализующую CNOT.

Упражнение 7.48. Проверьте, что схема, изображенная в нижней части рис. 7.19, действительно создает состояние Белла $(|00\rangle - |11\rangle)/\sqrt{2}$.

Упражнение 7.49 (элемент обмена). Важное применение метода ЯМР в химии состоит в определении структуры молекул, т. е. нахождении атомов водорода, углерода и фосфора, являющихся в молекуле ближайшими соседями. Для этой цели используется последовательность импульсов, известная как INADEQUATE (incredible natural abundance double quantum transfer experiment), в ЯМР широко используются подобные обозначения. На языке квантовых вычислений эту последовательность импульсов можно описать следующим образом. Выберем пару резонансов в спектре и попытаемся применить к ней операцию CNOT. Если после проверки мы увидим, что операция CNOT действительно выполнена, то выбранные резонансы соответствуют ядрам, которые являются ближайшими соседями. Еще один важный элемент, который используется, например, в последовательности TOCSY (total correlation spectroscopy) — это элемент обмена. Предложите квантовую схему только из операторов $e^{-iH/2\hbar J}$, R_x и R_y , реализующую элемент обмена (рекомендуется начать со схемы, показанной на рис. 1.7).

Квантовые алгоритмы

Еще один простой пример квантовых вычислений методом ЯМР — это реализация алгоритма Гровера. Рассмотрим задачу поиска в списке из четырех элементов (т. е. для $n = 2$ кубитов). Это значит, что задана функция $f(x)$, $x \in \{1, 2, 3, 4\}$, такая, что $f(x) = 0$ для всех $x \neq x_0$ и $f(x_0) = 1$. Требуется найти элемент x_0 . В классическом случае для этого необходимо вычислить $f(x)$ в среднем 2,25 раз, тогда как квантовый алгоритм позволяет найти x_0 , вычисля функцию f только один раз (гл. 6, вставка 6.1).

Нам потребуются три оператора: оракул O , изменяющий знак состояния в зависимости от значения функции f , оператор Адамара $H^{\otimes 2}$, применяемый к двум кубитам одновременно, и условный сдвиг фазы P . Оракул O изменяет знак базисного состояния, соответствующего x_0 ; например, для $x_0 = 3$ он имеет вид

$$O = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}. \quad (7.170)$$

Обозначим оператор эволюции $e^{-iH/2\hbar J}$ в течение времени $t = 1/2J$ (2,3 мс для хлороформа) через τ . Тогда для $x_0 = 3$ с точностью до несущественного общего фазового множителя $O = R_{y1}\bar{R}_{x1}\bar{R}_{y1}R_{y2}\bar{R}_{x2}\bar{R}_{y2}\tau$. Оператор $H^{\otimes 2}$ есть произведение двух однокубитовых элементов Адамара $H_1 \otimes H_2$, причем $H_k = R_{xk}^2 \bar{R}_{yk}$. Наконец, оператор P , имеющий вид

$$P = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}, \quad (7.171)$$

можно реализовать как $P = R_{y1}R_{x1}\bar{R}_{y1}R_{y2}R_{x2}\bar{R}_{y2}\tau$. Используя эти результаты, итерацию алгоритма Гровера G можно реализовать как $G = H^{\otimes 2}PH^{\otimes 2}O$. Путем несложных алгебраических преобразований этот оператор можно заметно упростить, см. упр. 7.51. Обозначим через $|\psi_k\rangle = G^k|00\rangle$ состояние, полученное после k итераций в алгоритме Гровера. Как мы знаем, $\langle x_0|\psi_k\rangle \approx \sin((2k+1)\theta)$, где $\theta = \arcsin(1/\sqrt{2})$. Эта периодичность амплитуды является существенной чертой алгоритма Гровера и, естественно, попытаться проверить ее экспериментально. Для двух кубитов и $x_0 = 3$ мы должны получить $|11\rangle = |\psi_1\rangle = -|\psi_4\rangle = |\psi_7\rangle = -|\psi_{10}\rangle$, т. е., если пренебречь знаком, период равен трем.

Упражнение 7.50. Предложите квантовую схему, использующую только однокубитовые вращения и оператор $e^{-iH/2\hbar J}$, которая реализует оракул O для $x_0 = 0, 1, 2$.

Упражнение 7.51. Покажите, что благодаря взаимным сокращениям последовательных однокубитовых вращений оператор итерации в алгоритме Гровера может быть записан в виде

$$G = \begin{cases} \bar{R}_{x1}\bar{R}_{y1}\bar{R}_{x2}\bar{R}_{y2}\tau R_{x1}\bar{R}_{y1}R_{x2}\bar{R}_{y2}\tau & (x_0 = 3) \\ \bar{R}_{x1}\bar{R}_{y1}\bar{R}_{x2}\bar{R}_{y2}\tau R_{x1}\bar{R}_{y1}\bar{R}_{x2}\bar{R}_{y2}\tau & (x_0 = 2) \\ \bar{R}_{x1}\bar{R}_{y1}\bar{R}_{x2}\bar{R}_{y2}\tau \bar{R}_{x1}\bar{R}_{y1}R_{x2}\bar{R}_{y2}\tau & (x_0 = 1) \\ \bar{R}_{x1}\bar{R}_{y1}\bar{R}_{x2}\bar{R}_{y2}\tau \bar{R}_{x1}\bar{R}_{y1}\bar{R}_{x2}\bar{R}_{y2}\tau & (x_0 = 0) \end{cases}, \quad (7.172)$$

для четырех возможных значений x_0 .

На рис. 7.20 показаны теоретические и экспериментальные матрицы плотности в разностной форме $\rho_{\Delta n} = |\psi_n\rangle\langle\psi_n| - \text{tr}(|\psi_n\rangle\langle\psi_n|)/4$ для первых семи итераций алгоритма Гровера. Как и следовало ожидать, $\rho_{\Delta 1}$ отчетливо указывает нам на состояние $|11\rangle$, соответствующее $x_0 = 3$. Аналогичные результаты были получены в экспериментах с тремя оставшимися x_0 . Для измерения каждой матрицы плотности было проведено $9 \times 3 = 27$ экспериментов, поскольку каждая томография состоит из девяти серий по три эксперимента в каждой, необходимых для моделирования чистого состояния.

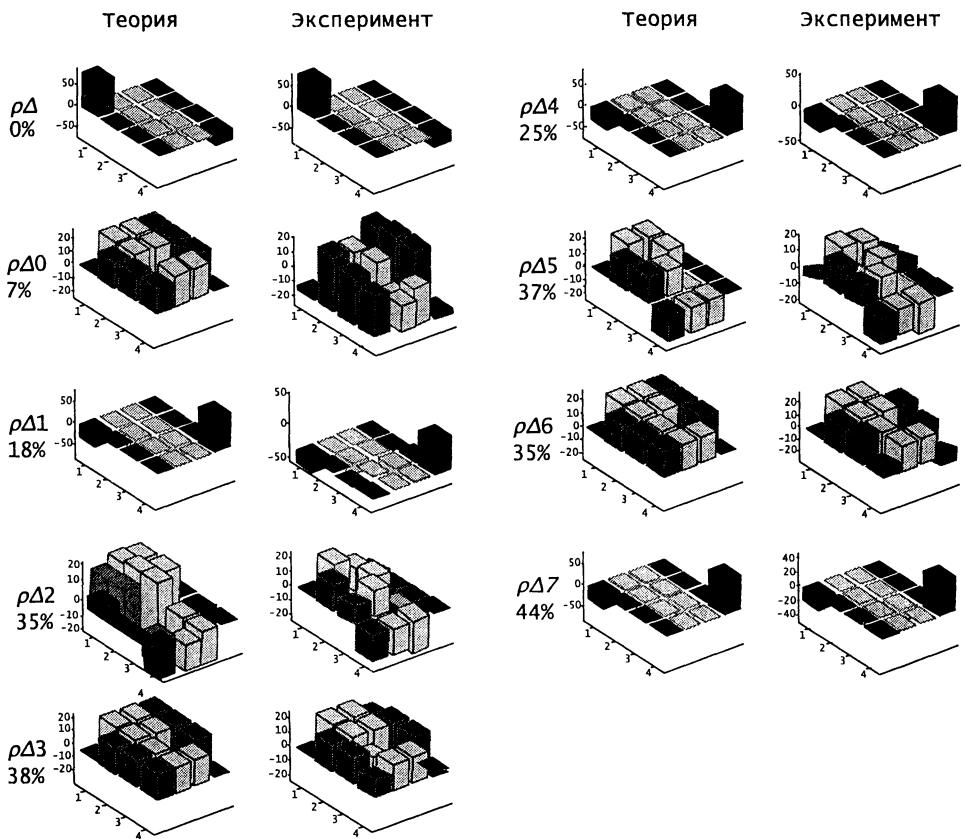


Рис. 7.20. Матрицы плотности в разностной форме для семи итераций алгоритма Гровера, полученные теоретически и в эксперименте на спинах водорода и углерода в хлороформе. Отчетливо видны три полных цикла по четыре итерации в каждом. Представлены только вещественные компоненты (теоретически все мнимые части равны нулю, а их вклад в экспериментальные результаты составляет менее 12%). Показаны также относительные ошибки $\|\rho_{\text{теор}} - \rho_{\text{экспер}}\|/\|\rho_{\text{теор}}\|$.

Самое длинное вычисление, состоящее из $n = 7$ итераций, заняло менее 35 мс, что не превышает времени когерентности. На рис. 7.20 ясно видны периодичность по числу итераций в алгоритме Гровера и хорошее согласие между теорией и экспериментом. Большое отношение сигнал-шум (порядка 10^4) было получено даже при одиночных измерениях. Численное моделирование показывает, что основными источниками ошибок (порядка 7 – 44%) являются неоднородность магнитного поля, релаксация намагниченности во время эксперимента и неточная калибровка радиочастотных импульсов (в порядке их значимости).

Недостатки

Реализация квантовых вычислений методом ЯМР успешно продемонстрировала работу квантовых алгоритмов для семи кубитов, что уже само по себе достаточно впечатляюще. Однако, существуют принципиальные ограничения, связанные с использованием временной, пространственной и логической разметок.

Действительно, введение какой-либо из этих разметок преследует цель выделить из полного сигнала, соответствующего равновесному состоянию, вклад нескольких спинов в чистом состоянии $|00\dots0\rangle$ (или в каком-то другом базисном состоянии). В случае временной и пространственной разметок мы складываем несколько сигналов, чтобы сократить все лишние слагаемые; при использовании логической разметки мы используем дополнительные спины, чтобы в какой-то части пространства состояний получить чистое состояние. Однако, какую бы разметку мы не использовали, вероятность того, что спины находятся в состоянии $|00\dots0\rangle$, не может быть больше равновесной вероятности

$$p_{00\dots0} = \frac{1}{Z} \langle 00\dots0 | e^{-\beta H} | 00\dots0 \rangle. \quad (7.173)$$

Подставляя $H = \sum_k \omega Z_k$, мы находим, что для молекулы с n спинами $p_{00\dots0}$ пропорциональна $n! 2^{-n}$. Это означает, что при фиксированной температуре амплитуда полного сигнала является экспоненциально убывающей функцией от числа эффективно чистых кубитов, выделяемых из равновесного состояния той или иной разметкой.

Использование молекулы в качестве квантового компьютера также приводит к некоторым ограничениям. Структура молекулы играет роль *архитектуры компьютера*, определяя какие пары (или группы) кубитов могут взаимодействовать друг с другом (аналогично, радиочастотные импульсы играют роль программы). Естественно, не все кубиты могут взаимодействовать друг с другом. Мы не можем убирать не нужные нам взаимодействия за исключением тех, которые можно «выключить» рефокусировкой. Кубиты отличаются друг от друга частотами прецессии ядер. При достаточно большом числе ядер мы уже не сможем избирательно воздействовать только на один кубит. Эта проблема может быть решена использованием архитектуры типа клеточного автомата, например одномерной цепи вида $X - A - B - C - A - B - C - \dots - A - B - C - Y$, концы которой соответствуют различным ядрам, а внутренняя часть состоит из повторяющейся регулярной последовательности ядер, причем разные буквы соответствуют различным ядрам. Может показаться, что это очень ограниченная модель вычислений. Однако, она позволяет выполнять произвольные квантовые алгоритмы, но с полиномиальным замедлением. Точная степень замедления конечно очень важна, например при реализации квантового алгоритма поиска, в котором достигается только квадратичное ускорение.

Существуют способы, позволяющие избежать ограничений, связанных с использованием метода разметки. Например, можно поляризовать спины ядер с

помощью какого-либо физического механизма. Используя оптическую накачку (подобную той, что применялась для охлаждения ионов, рис. 7.8) можно поляризовать электронные моменты атомов рубидия. При ван-дер-ваальсовском взаимодействии атомов рубидия с атомами ксенона образуются короткоживущие молекулы и поляризация переносится на ядра ксенона. Эта же схема

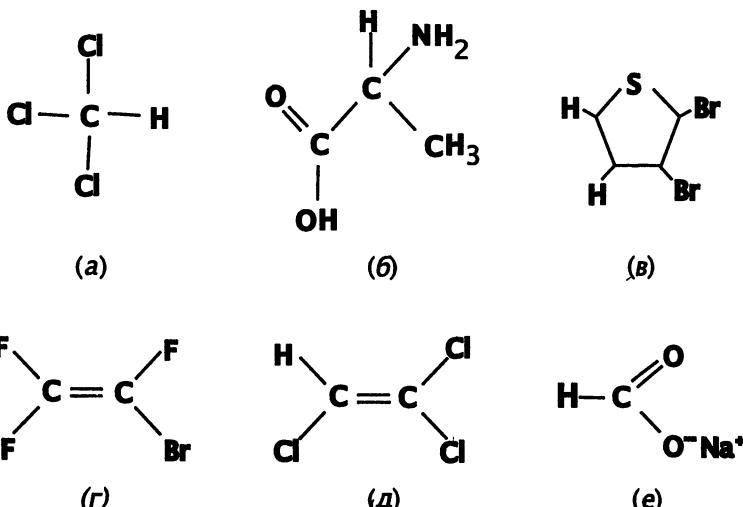


Рис. 7.21. Примеры простейших молекул, использованных в экспериментах по реализации квантовых вычислений методом ЯМР. (а) Хлороформ: два кубита, ядра водорода и углерода; использовался для реализации алгоритма Дойча-Йожа и двухкубитового квантового поиска. (б) Анилин: три кубита, ядра углерода; использовался для демонстрации исправления квантовых ошибок. Обратите внимание, что все три углеродных спина имеют разные частоты прецессии, поскольку их химические окружения не эквивалентны (например, электроотрицательность кислорода приводит к дефициту электронов вблизи соседнего ядра углерода). (в) 2,3-дигромтиофеин: два кубита, два ядра водорода; использовался для моделирования четырехуровневого «обрезанного» гармонического осциллятора. Два протона находятся на разном расстоянии от атома серы и поэтому имеют различные частоты. (г) Трифторметилен: три кубита, ядра фтора, использовался для демонстрации логической разметки, а также для реализации суперпозиции $(|000\rangle + |111\rangle)/\sqrt{2}$. (д) Трихлоратилен: три кубита, ядро водорода и два ядра углерода; использовался для демонстрации телепортации. Состояние спина протона было телепортировано на спин правого углерода. (е) Формиат натрия: два кубита, ядра водорода и углерода; использовался для реализации кодов, обнаруживающих квантовые ошибки. В этой молекуле изменением температуры раствора можно добиться совпадения времен T_2 для обоих кубитов.

была реализована для поляризации ядер гелия. По-видимому, ее можно применить и к молекулам, хотя технологически это довольно сложно. Можно также попытаться модифицировать логическую разметку. Эта разметка в сущности представляет собой алгоритм сжатия, который увеличивает относительную вероятность одного состояния в ансамбле за счет отбрасывания других состояний. Существует улучшенный вариант логической разметки, который позволяет выделить $nH(p)$ эффективно чистых кубитов, используя молекулу с n спинами, где $p = (1 - e^{-\Delta E/k_B T})/2$, ΔE – энергия переворота спина, T – температура. Процедура сжатия здесь требует лишь полиномиального числа

элементарных операций. Однако, преимущество этого метода становится существенным, только при $p \approx 0.5$. На данный момент в мощных соленоидах можно достичь $p \approx 0.4999$.

Несмотря на эти недостатки, метод ЯМР может служить основой для тестирования квантовых алгоритмов, а технические приемы, разработанные в связи с ним, могут оказаться полезными для других реализаций квантовых вычислений. Некоторые молекулы, использованные в экспериментах по квантовым вычислениям, показаны на рис. 7.21. Теория ЯМР находится на пересечении таких областей знания, как химия, физика, машиностроение и математика. Их развитие и обмен идеями несомненно приведут к дальнейшему совершенствованию метода ЯМР.

ЯМР-реализация квантового компьютера

- **Представление кубита.** Ядерный спин.
- **Унитарная эволюция.** Произвольное преобразование можно реализовать, действуя импульсными магнитными полями на спины, находящиеся в сильном постоянном магнитном поле. Спин-спиновое взаимодействие обеспечивается химической связью атомов.
- **Приготовление начального состояния.** Можно поляризовать спины в сильном магнитном поле и затем использовать методы приготовления «эффективно чистых состояний».
- **Приготовление конечного результата.** Измерение сигнала индукции, возникающего при прецессии магнитного момента.
- **Недостатки.** Если поляризация спинов в начальном состоянии не достаточно высока, при использовании эффективно чистых состояний амплитуда выходного сигнала экспоненциально убывает с ростом числа кубитов.

7.8 Другие варианты реализации

В настоящей главе мы описали лишь часть тех идей, которые были предложены для реализации квантового компьютера. При их отборе мы руководствовались желанием проиллюстрировать общие требования и трудности при их выполнении. Напомним, что нам нужно уметь адекватно представлять квантовую информацию, реализовывать унитарные преобразования, приготовлять начальное состояние и производить измерения результата.

На примере простого гармонического осциллятора мы увидели, что информация должна представляться в *цифровом виде*: элементарная единица квантовой информации (кубит, кутрит или что-то еще) должна быть представлена *собственной* физической степенью свободы, иначе потребляемые ресурсы

(например энергия) будут использоваться неэффективно. Этот пример позволил нам также ввести необходимые для дальнейшего изучения представлений кубитов математические модели. Одиночные фотоны представляют собой почти идеальные кубиты, однако фотон-фотонное взаимодействие в нелинейных оптических средах, как правило, сопровождается потерей когерентности. Эта проблема решается в системах типа КЭДР, поскольку взаимодействие между фотонами осуществляется в них посредством одиночных атомов. При обсуждении КЭДР мы ввели важное понятие двухуровневого атома и увидели, что правила отбора (в дипольном приближении), связанные с физическими симметриями, приводят к достаточно защищенному кубиту.

Естественное обобщение идеи применения правил отбора для представления кубита состоит в использовании частиц со спином $1/2$, которые, по определению, имеют только два состояния. Например, метод ионов в ловушке основан на представлении кубитов электронными и ядерными спинами. В этом методе есть свои трудности. В частности, кванты колебаний центра масс — фононы, — участвующие как промежуточное звено в спин-спиновом взаимодействии, имеют малое время когерентности. Этого можно избежать, если использовать ядерные спины молекул, в которых сильное спин-спиновое взаимодействие обусловлено химической связью атомов. Однако, детектировать сигнал от одиночного ядерного спина в настоящее время технически невозможно. Эта сложность не возникает, если использовать метод ЯМР, в котором ансамбль из $O(10^{18})$ молекул приводится в «эффективно чистое состояние». При помощи метода ЯМР стало возможным экспериментально реализовать простейшие квантовые алгоритмы. Неприятность состоит в том, что если поляризация спинов в начальном состоянии недостаточно велика, измеряемый сигнал экспоненциально мал по числу кубитов.

Как показывают эти примеры, поиск хорошей физической реализации квантового компьютера — чрезвычайно нетривиальная задача, поскольку нужно учитывать много почти взаимоисключающих требований. Все предложенные выше варианты реализации являются неудовлетворительными в том смысле, что на их основе в ближайшем будущем нельзя будет построить многокубитовый квантовый компьютер. Тем не менее это еще не значит, что данная задача не имеет решения, поскольку существует много других вариантов реализации. Некоторые из них будут кратко рассмотрены в этом заключительном разделе.

Различные реализации можно классифицировать по тому, какая физическая степень свободы используется для представления кубита. Из таблицы, приведенной на рис. 7.1, ясно, что практически любая квантующаяся физическая величина может представлять кубиты. В то же время, как мы видели, фундаментальные физические квантовые объекты, такие как фотон и спин, являются наиболее привлекательными представлениями кубита.

Существует еще одна фундаментальная величина, подходящая на роль кубита. Это электрический заряд. Современная электроника предоставляет нам замечательную возможность создавать, контролировать и измерять заряд даже в одноэлектронном режиме. Например, в *квантовых точках*, изготовленных из полупроводников, металлов или даже небольших молекул, могут быть

локализованы заряды в трехмерных потенциальных ямах. Это может быть проверено наблюдением эффекта кулоновской блокады, в частности, ступенчатой зависимости тока через квантовую точку от разности потенциалов на туннельных контактах, подсоединенных к ней. Наличие ступенек обусловлено электрической емкостью точки C , благодаря которой добавление лишнего электрона увеличивает энергию системы на $e^2/2C$. В отличие от фотонов заряды не могут рождаться и уничтожаться, они могут только перемещаться по системе. Таким образом, при представлении кубита зарядовым состоянием мы должны использовать что-то похожее на двойственное представление (подразд. 7.4.2), например, состояния $|0\rangle$ и $|1\rangle$ могут соответствовать электрону, локализованному в одной из двух квантовых точек, или двум состояниям электрона в одной точке.

Для кубитов, представленных при помощи электрических зарядов, однокубитовые операции можно реализовать, используя электростатические затворы (аналоги фазовращателей для фотонов), специальные двухканальные рассеиватели (аналог светоделителя) или туннельные контакты между квантовыми точками. Электрические заряды взаимодействуют друг с другом по закону Кулона. Поскольку это взаимодействие дальнодействующее, оно приводит к перекрестной фазовой модуляции удаленных друг от друга зарядов и является аналогом керровского фотон-фотонного взаимодействия. Управляя кулоновским взаимодействием, можно реализовывать двухкубитовые операции. Что касается измерения заряда в одноэлектронном режиме, современные полевые транзисторы вполне способны детектировать прохождение через электрическую цепь одиночных электронов. Более того, одноэлектронные транзисторы, работающие при температурах ≈ 100 мК, имеют детектирующую способность порядка $10^{-4} e/\sqrt{\text{Гц}}$ на частотах свыше 200 МГц. К сожалению, неконтролируемое движение даже сильно удаленных электрических зарядов приводит к потере когерентности. В сочетании с электрон-фононным взаимодействием это делает время когерентности зарядовых состояний относительно малым — от сотен пикосекунд до сотен фемтосекунд.

Для представления кубитов также предлагалось использовать носители заряда в сверхпроводниках. Из-за электрон-фононного взаимодействия в некоторых металлах при низких температурах электроны объединяются в куперовские пары, заряд которых равен $2e$. Точно также, как электроны можно локализовать в квантовых точках, куперовские пары могут быть локализованы в пределах небольшой металлической гранулы, так что число пар в грануле становится хорошим квантовым числом и может использоваться для представления квантовой информации. Однокубитовые операции реализуются при помощи электростатических затворов, управляющих потенциалом гранулы, и джозефсоновских контактов, соединяющих разные гранулы. Джозефсоновские контакты можно также использовать для реализации взаимодействия между кубитами, причем силу этого взаимодействия можно регулировать внешним магнитным полем с помощью сверхпроводящих квантовых интерферометров. Измерение кубитов соответствует просто измерению электрического заряда. Кубиты, представленные куперовскими парами, относительно устой-

чивы; оценки показывают, что основной вклад в потерю когерентности дает процесс спонтанного электромагнитного излучения, а соответствующее время когерентности может превышать одну микросекунду. Это гораздо больше характерного временного масштаба данных систем, имеющего порядок сотен пикосекунд. К сожалению, флуктуирующий потенциал, создаваемый внешними неконтролируемыми зарядами, ограничивает время когерентности также, как и в случае представления кубитов зарядами электронов. Чтобы избежать этой проблемы, можно представлять кубиты состояниями с различным *магнитным потоком* (например с левой и правой ориентацией) через замкнутый контур в сверхпроводнике. В этом случае потеря когерентности возникает из-за флуктуаций внешнего магнитного поля, которые можно сделать достаточно слабыми.

Короткодействующее магнитно-дипольное взаимодействие делает особенно привлекательными представления кубитов при помощи спинов в полупроводниковых системах. Например, квантовая точка, содержащая довольно много электронов, может вести себя как спин $1/2$, если в ней имеется один избыточный электрон. Соответствующее состояние можно приготовить, помещая квантовую точку в сильное магнитное поле при низких температурах, так что энергия переворота спина ΔE много больше, чем $k_B T$. Как мы видели в разд. 7.7, чтобы манипулировать одиночными спинами, можно использовать импульсные локальные магнитные поля, а двухкубитовые операции реализуются при помощи управляемого гамильтониана Гейзенберга

$$H(t) = J(t) \vec{S}_1 \cdot \vec{S}_2 = \frac{1}{4} [X_1 X_2 + Y_1 Y_2 + Z_1 Z_2], \quad (7.174)$$

где \vec{S} — операторы спина (матрицы Паули, деленные на два), а $J(t) = 4\tau_0^2(t)/u$ включает зарядовую энергию квантовой точки u и тунNELНЫЙ матричный элемент $\tau_0(t)$, который управляет локальными электростатическими затворами, помещенными между квантовыми точками. Взаимодействие (7.174) является универсальным в том смысле, что оно эквивалентно элементу CNOT (см. упражнение ниже). Теоретически спиновые состояния можно измерять, предоставляя электрону возможность туннелировать в «считывающую» paramagnитную квантовую точку или в электрометр через «спиновый фильтр», в котором амплитуда туннелирования зависит от направления спина. Проблема лишь в том, чтобы реализовать такие измерения на практике. Современные технологии пока не позволяют осуществлять измерения спина в полупроводниках с необходимой степенью точности.

Упражнение 7.52 (универсальность гамильтониана Гейзенберга).

Включая $J(t)$ в гамильтониан Гейзенберга (7.174) на соответствующее время, можно реализовать оператор эволюции $U = \exp(-i\pi \vec{S}_1 \cdot \vec{S}_2)$. Покажите, что U эквивалентен операции обмена SWAP. Элемент $\sqrt{\text{SWAP}}$, который реализуется за вдвое меньшее время, является универсальным. Найдите явный вид этого элемента и покажите, как с помощью него и однокубитовых операций реализовать элемент CNOT.

Наконец, если появятся технологии, позволяющие удерживать отдельные ядерные спины в полупроводниках, манипулировать ими и делать измерения, возможен следующий подход. Предположим, что можем поместить отдельный атом ^{31}P (ядерный спин 1/2) в заданную точку кристаллической подложки из ^{28}Si (ядерный спин 0), над которой располагаются литографически нанесенные электростатические затворы. Эти затворы позволяют управлять конфигурацией электронного облака, окружающего примесь фосфора, а значит и магнитным полем, в котором находится ядерный спин фосфора. Таким образом можно реализовать однокубитовые операции. Используя дополнительные затворы, расположенные между двумя атомами фосфора, можно искусственно сформировать электронное облако, соединяющее эти атомы (аналог химической связи), что позволяет реализовать двухкубитовые операции. Изготовить подобную структуру очень сложно — например, расстояния между затворами должны быть не более 10 нм, а примеси ^{31}P должны прикрепляться строго в предписанные им позиции. Тем не менее, данный подход показывает, что квантовые вычисления, возможно, могут быть реализованы с помощью более или менее традиционных вычислительных технологий.

Из всех описанных нами схем реализации квантового компьютера наиболее перспективными с технологической точки зрения представляются схемы, основанные на твердотельных системах. Вместе с тем, предлагаются все новые и новые варианты квантовых вычислений с использованием атомов, молекул и фотонов, например в таких системах, как оптические решетки (искусственные кристаллы, состоящие из атомов, удерживаемых в ловушке из пересекающихся световых лучей), где можно наблюдать Бозе-конденсацию. Возможно, что когда-нибудь для квантовых вычислений окажутся полезными мезоны,夸克, глюоны или даже черные дыры. Но все же основные надежды связываются именно с методами физики твердого тела. Напомним, однако, что прежде чем в конце 40-х гг. XX в. был создан транзистор, потребовались мировые инвестиции в развитие полупроводниковых технологий порядка 1 триллиона долларов США. Развитие физики конденсированного состояния уже позволило открыть много новых физических эффектов, например, сверхпроводимость, квантовый эффект Холла или кулоновскую блокаду (классический эффект, открытый в то время, когда казалось, что про классическую физику уже давно все известно).

В этой главе нас в основном интересовала реализация устройств, выполняющих квантовые вычисления. Отдельные компоненты этих устройств могут оказаться полезными для других квантовых приложений. В частности, квантовая криптография и ее экспериментальная реализация описаны в разд. 12.6. В разд. «История и дополнительная литература» приведены ссылки на экспериментальные работы по квантовой телепортации и сверхплотному кодированию. Квантовые вычисления и передача информации тесно связаны друг с другом, что видно, например, из конструкции распределенных квантовых вычислений. Их экспериментальная реализация и разработка новых алгоритмов — несомненно очень перспективная область исследований.

Интерес к квантовым компьютерам и квантовым каналам связи связан в основном с надеждой на их практическое использование. Кроме этого, как мы

увидели в настоящей главе, теория квантовых вычислений и квантовой информации способствует более глубокому пониманию свойств физических систем и является источником новых задач. Действительно, при рассмотрении систем из многих частиц, как правило, исследуются их статистические и термодинамические свойства. При этом требуется, зная свойства отдельных атомов, описать свойства всей системы. Напротив, в теории квантовой информации наибольшее внимание уделяется *динамическим* свойствам *одиночных* квантовых систем. Мы надеемся, что данный подход покажется вам полезным, и после прочтения этой главы вы будете продолжать думать о физике «алгоритмически».

Задача 7.1 (эффективная временная разметка). Предложите эффективную схему (состоящую из $O(\text{poly}(n))$ -элементов), которая осуществляет циклическую перестановку всех диагональных элементов в матрице плотности размера $2^n \times 2^n$, за исключением элемента $|0^n\rangle\langle 0^n|$.

Задача 7.2 (вычисления с линейной оптикой). Предположим, что, выполняя квантовые вычисления с одиночными фотонами, вместо двойственного представления (подразд. 7.4.1) мы используем *унарное* представление, так что 2^n кубитовых базисных состояний представлены как $|00\dots 01\rangle$, $|00\dots 010\rangle$, $|00\dots 0100\rangle, \dots, |10\dots 0\rangle$.

1. Покажите, что произвольное унитарное n -кубитовое преобразование этих состояний можно реализовать, используя только светоделители и фазовращатели (т. е. без нелинейных сред).
2. Постройте схему, состоящую из светоделителей и фазовращателей, которая реализует алгоритм Дойча–Йожа для одного кубита.
3. Постройте схему, состоящую из светоделителей и фазовращателей, которая реализует квантовый алгоритм поиска для двух кубитов.
4. Докажите, что для реализации унитарного преобразования общего вида потребуется схема из экспоненциального по n числа элементов.

Задача 7.3 (управление через гамильтониан Джейнса–Каммингса). Для того, чтобы выполнять квантовые вычисления, нужно уметь управлять динамикой небольших квантовых систем через какую-то внешнюю *классическую* степень свободы. Замечательно, что для атомных состояний такое управление можно осуществлять при помощи оптических импульсов, причем суммарные атомные состояния сохраняют когерентность достаточно долго. В данной задаче мы установим, при каких условиях возможно такое управление. Приведем сначала выражение для гамильтониана Джейнса–Каммингса, описывающего взаимодействие одиночного атома с одной модой электромагнитного поля:

$$H = a^\dagger \sigma_- + a \sigma_+, \quad (7.175)$$

где σ_\pm — атомные операторы, а a и a^\dagger — операторы поля.

1. Рассмотрим матричный элемент

$$A_n = \langle n | U | \alpha \rangle, \quad (7.176)$$

где $U = e^{i\theta H}$, $|\alpha\rangle$ — когерентное состояние, $|n\rangle$ — состояние с n фотонами. Заметим, что A_n является *оператором*, действующим на атомные состояния. Проверьте, что

$$A_n = e^{-|\alpha|^2} \frac{|\alpha|^2}{n!} \begin{bmatrix} \cos(\theta\sqrt{n}) & \frac{i\sqrt{n}}{\alpha} \sin(\theta\sqrt{n}) \\ \frac{i\alpha}{\sqrt{n+1}} \sin(\theta\sqrt{n+1}) & \cos(\theta\sqrt{n+1}) \end{bmatrix}. \quad (7.177)$$

(*Указание.* Используйте результаты упр. 7.17.)

- 2.** Предположим, что α достаточно большое. Без потери общности можно считать α вещественным. Рассмотрим распределение вероятностей

$$p_n = e^{-x} \frac{x^n}{n!} \quad (7.178)$$

со средним значением $\langle n \rangle = x$ и стандартным отклонением $\sqrt{\langle n^2 \rangle - \langle n \rangle^2} = \sqrt{x}$. Используя замену переменных $n = x - L\sqrt{x}$ и формулу Стирлинга

$$n! \approx \sqrt{2\pi n} n^n e^{-n} \quad (7.179)$$

покажите, что

$$p_L \approx \frac{e^{-L^2/2}}{\sqrt{2\pi}}. \quad (7.180)$$

- 3.** Наиболее важными является оператор A_n при $n = |\alpha|^2$. Пусть $n = \alpha^2 + L\alpha$. Для

$$a = y \sqrt{\frac{1}{y^2} + \frac{L}{y}} \quad \text{и} \quad b = y \sqrt{\frac{1}{y^2} + \frac{L}{y} + 1}, \quad (7.181)$$

где $y = 1/\alpha$, покажите, что

$$A_L \approx \frac{e^{-L^2/4}}{(2\pi)^{1/4}} \begin{bmatrix} \cos a\varphi & ia \sin a\varphi \\ (i/b) \sin b\varphi & \cos b\varphi \end{bmatrix}, \quad (7.182)$$

где $\varphi = \alpha/\theta$. Проверьте также, что

$$\int_{-\infty}^{\infty} A_L^\dagger A_L dL = I. \quad (7.183)$$

- 4.** Идеальное унитарное преобразование атомных состояний можно записать в виде

$$U = \begin{bmatrix} \cos a\theta & i \sin a\theta \\ i \sin a\theta & \cos a\theta \end{bmatrix}. \quad (7.184)$$

Насколько A_L близко к U ? Попробуйте оценить степень совпадения

$$\mathcal{F} = \min_{|\psi\rangle} \int_{-\infty}^{\infty} |\langle\psi|U^\dagger A_L|\psi\rangle|^2 dL, \quad (7.185)$$

разлагая ее в ряд Тейлора по y .

Задача 7.4 (вычисления на двухуровневых атомах в ловушке). При реализации СНОТ в подразд. 7.6.3 мы в целях упрощения рассматривали трехуровневые атомы. В данной задаче демонстрируется, как можно обойтись двумя уровнями, правда за счет некоторых дополнительных усложнений.

Обозначим через $\mathcal{T}_{\hat{n}}^{\text{син},j}(\theta)$ операцию, реализуемую действующим на j -ю частицу лазерным импульсом с длительностью $\theta\sqrt{N}/\eta\Omega$ и с частотой, соответствующей синей боковой полосе $\omega = \Omega + \omega_z$. Аналогичную операцию для красной боковой полосы обозначим через $\mathcal{T}_{\hat{n}}^{\text{красн},j}(\theta)$. Направление \hat{n} задает ось вращения, лежащую в плоскости $\hat{x} - \hat{y}$, и определяется фазой лазерного излучения. Если из контекста ясно, о каком атоме идет речь, индекс j будет опускаться. В явном виде операция $\mathcal{T}_{\hat{n}}^{\text{син},j}(\theta)$ записывается следующим образом:

$$\mathcal{T}_{\hat{n}}^{\text{син}}(\theta) = \exp \left[\left(e^{i\varphi}|00\rangle\langle 11| + e^{-i\varphi}|11\rangle\langle 00| + e^{i\varphi}\sqrt{2}|01\rangle\langle 12| + e^{-i\varphi}\sqrt{2}|12\rangle\langle 01| + \dots \right) \frac{i\theta}{2} \right], \quad (7.186)$$

где $\hat{n} = \hat{x} \cos \varphi + \hat{y} \sin \varphi$, а состояния обозначаются как |атом, поле). Коэффициент $\sqrt{2}$ возникает из-за того, что для бозонных состояний $a^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle$.

- Покажите что $\mathcal{T}_{\hat{j}}^{\text{красн},j}(\pi)$ переставляет местами внутреннее и колебательное состояния атома j , при условии, что начальным колебательным состоянием было $|0\rangle$.
- Найдите значение θ , при котором $\mathcal{T}_{\hat{n}}^{\text{син}}(\theta)$, действуя на любое состояние в вычислительном подпространстве, порожденном векторами $|00\rangle$, $|01\rangle$, $|10\rangle$ и $|11\rangle$, при любом \hat{n} оставляет его в этом подпространстве.
- Покажите, что если $\mathcal{T}_{\hat{n}}^{\text{син}}(\varphi)$ сохраняет вычислительное подпространство, то при любом выборе угла поворота β и оси α оператор $U = \mathcal{T}_{\alpha}^{\text{син}}(-\beta)\mathcal{T}_{\hat{n}}^{\text{син}}(\theta)\mathcal{T}_{\alpha}^{\text{син}}(\beta)$ также сохраняет вычислительное подпространство.
- Найдите значения α и β , при которых оператор U диагонален и имеет следующий вид:

$$\begin{bmatrix} e^{-i\pi/\sqrt{2}} & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\pi/\sqrt{2}} \end{bmatrix}. \quad (7.187)$$

5. Покажите, что с помощью элемента (7.187) и однокубитовых операций можно реализовать элемент CNOT, в котором два кубита представлены внутренними состояниями двух атомов. Можете ли вы подобрать последовательность импульсов, реализующую CNOT, если не требовать, чтобы начальное колебательное состояние было $|0\rangle$?

Краткое содержание главы

- **Четыре фундаментальных условия для проведения квантовых вычислений:** (1) Представление кубитов, (2) Управляемая унитарная эволюция, (3) Приготовление начального состояния кубитов, (4) Измерение конечного состояния кубитов.
- **Одиночные фотоны** являются хорошим представлением кубитов, если логические состояния 0 и 1 используется как $|01\rangle$ и $|10\rangle$. Однако обычные нелинейные оптические среды, в которых может иметь место сильное фотон-фотонное взаимодействие, неизбежно поглощают или рассеивают свет.
- **КЭД в резонаторах** позволяет обеспечить сильное взаимодействие между одиночными атомами и одиночными фотонами. Атом служит промежуточным звеном в фотон-фотонном взаимодействии.
- **Ионы в ловушке.** Кубиты представлены состояниями ядерных и электронных спинов. При низких температурах спиновыми состояниями можно управлять с помощью лазерных импульсов. Взаимодействие спинов с трансляционной фононной модой позволяет реализовать двухкубитовые логические элементы.
- **Ядерные спины** представляют собой почти идеальные кубиты, а отдельные молекулы были бы почти идеальными квантовыми компьютерами, если бы нам удалось контролировать и измерять состояния их ядерных спинов. Метод ядерного магнитного резонанса позволяет это сделать с использованием больших ансамблей молекул, находящихся при комнатной температуре. Однако, из-за отсутствия эффективной процедуры приготовления начального состояния выходной сигнал оказывается очень слабым.

История и дополнительная литература

Замечательное обсуждение проблем, связанных с построением квантового компьютера, можно найти в работе Дивинченцо [123], на которой основан рис. 7.1. В ней также формулируются пять условий реализации квантового компьютера, напоминающие условия из разд. 7.2.

Простой квантовый гармонический осциллятор (разд. 7.3) является основой квантовой механики; его описание можно найти в любом стандартном учебнике, см. например [346]. Общие необходимые и достаточные условия для квантового вычисления, приведенные в подразд. 7.3.3, обсуждались в работе Ллойда [252].

Оптический квантовый компьютер, которому посвящен разд. 7.4, описывается формализмом квантовой оптики, вошедшим во многие учебники, например [261, 159]. Детали, касающиеся элементарной оптики и оптических приборов, таких как поляризаторы, светофильтры, фотодетекторы и др., можно найти, например, в учебнике [370]. Светофильтр, работающий в режиме одиночных фотонов, изучался Кампосом, Салехом и Тихом [105], а изящная аналогия между $SU(2)$ и парой связанных гармонических осцилляторов была впервые описана Швингером [346]. Двойственное представление кубита предложено Юрком и применено в работе Чанга и Ямамото [111] для описания квантового компьютера (с использованием нелинейной среды Керра), реализующего алгоритм Дойча-Йожа (как в упр. 7.13). Квантовый оптический элемент Фредкина был описан Ямамотой, Китагавой и Игетой [427], а также Мильбурном [282]. Методика генерации и детектирования одиночных фотонов, необходимая для оптического квантового компьютера, обсуждалась Имамоглу и Ямамото [197], и Квайетом, Штейнбергом, Чао, Эбергардом и Петровым [231]. Аналогичный механизм с применением электронной оптики, в котором вместо керровского взаимодействия использовалось кулоновское взаимодействие, рассматривался Китагавой и Уэда [232]. В работе Ватанабе и Ямамото [423] изучались фундаментальные ограничения, касающиеся свойств традиционных нелинейных оптических материалов в режиме одиночных фотонов вдали от резонанса. Идея использования линейных оптических элементов для моделирования квантовых логических элементов принадлежит Серфу, Адами и Квайету [77]. В важной более ранней работе Река, Цайлингера, Бернштейна и Бертани [345] описаны похожие конструкции, но эти авторы не связывали их явно с квантовыми вычислениями. Квайет, Митчелл, Швингерт и Уайт [222] построили схему, моделирующую квантовый алгоритм поиска Гровера с использованием линейных оптических элементов, но в которой требуемые ресурсы растут экспоненциально с увеличением размера входа. По поводу энергии, расходуемой при передаче информации по оптическим каналам связи на различные расстояния, см. работу Миллера [283].

Книга Аллена и Эберли [7] — прекрасный учебник по двухуровневым атомам и оптическому резонансу. Эксперимент, описанный в подразд. 7.5.4, выполнен Тюршетом, Худом, Ламжем, Мабучи и Кимблем [385]. Подробные комментарии можно найти в диссертации Тюршета [389]. Одиночные фотонны, использованные в этом эксперименте, получили название «летающих кубитов». Другой метод, в котором кубиты были представлены атомными состояниями, а атомы пропускались через оптические резонаторы, был предложен Домокосом, Реймоном, Бруном и Арошем [131]. Этот метод основан на идеи использования одиночных атомов для ввода когерентного состояния внутрь резонатора, принадлежащей Давидовичу, Маали, Бруну, Реймону и Арошу [130, 128].

Идея использования ионов в ловушке для квантовых вычислений была предложена Сираком и Цоллером [112]. Изложение этой идеи в подразд. 7.6.1 в значительной мере опирается на работы Стина [373] и Уайнленда, Монро, Итено, Либфрида, Кинга и Меекгофа [420]. Теорема Ирншоу является следствием уравнения Лапласа, см. оригинальную работу [134] или современный учебник по электромагнетизму, например Рамо, Уиннери и ван Дуцера [344]. Рис. 7.8 позаимствован из работы [373] (Figure 6). Рис. 7.7 взят из работы [420]. Эксперимент, описанный в подразд. 7.6.4, был выполнен группой Монро, Меекгофа, Кинга, Итено и Уайнленда [289]. Рис. 7.15 является копией оригинального снимка Уайнленда [420]. Брюэр, Деву и Калленбах [40] предложили использовать длинные цепочки из планарных ионных микроловушек для построения многокубитовых квантовых компьютеров. Ловушка такого вида изображена на рис. 7.12. Нагревание и другие процессы, приводящие к потере когерентности для ионов в ловушке, рассмотрены в теоретической работе Джеймса [198]. Влияние потери когерентности на квантовые вычисления методом ионов в ловушке, а также поправки к двухуровневому приближению довольно глубоко изучены Пленио и Найтом [323].

Дивинченцо впервые предложил использовать ядерные спины для квантовых вычислений [124] и заметил, что хорошо и давно известная последовательность импульсов ENDOR (electron nucleon double resonance) реализует элемент СНОТ. Однако, вопрос о том, как использовать для квантовых вычислений ансамбль ядер при комнатной температуре, оставался открытым до появления работ Кори, Фами и Хавела [81], а также Гершенфельда и Чанга [160], в которых было введено понятие эффективно чистых состояний. Проблема модификации квантовых алгоритмов, возникающая при использовании измерений, усредненных по ансамблю, была решена в работе [160] (подразд. 7.7.3). В качестве учебников по ЯМР мы можем порекомендовать книги Эрнста, Боденгаузена и Вокауна [135] и Шлихтера [364]. Критические замечания, касающиеся квантовых вычислений методом ЯМР, можно найти в работе Уоррена [410]; в этой же работе автор описывает преимущества метода электронного парамагнитного резонанса (ЭПР). Временная разметка представлена в работе Нилла, Чанга и Лафлама [210]. Вопросам реализации логических элементов методом ЯМР и построения схемы для приготовления состояния Белла (подразд. 7.7.4) посвящены работы Чанга, Гершенфельда, Кубинека и Леунга [83]. Реализация алгоритма Гровера (подразд. 7.7.4) представлена в работе Чанга, Гершенфельда и Кубинека [82], из которой позаимствован рис. 7.20. Линден, Капс и Фриман [249] заметили, что элемент обмена может быть полезен для квантовых вычислений методом ЯМР, и предложили последовательность импульсов для его реализации. Данные на рис. 7.18, демонстрирующие использование логической разметки для трех спинов, взяты из работы Вандерзипена, Яннони, Шервуда и Чанга [408]. Обобщение идеи квантовых вычислений с помощью ЯМР на случай кристаллических решеток было сделано в работе Ямагучи и Ямamoto [429]. Молекулы, изображенные на рис. 7.21, были использованы в работах (а) Чанга, Вандерзипена, Жу, Леунга и Ллойда [109]; (б) Кори, Масса, Прайса, Нилла, Лафлама, Зурека и Хавела [95]; (в) Сомару, Ченга, Хавела.

ла, Лафлама и Кори [375]; (г) Вандерзипена, Яннони, Шервуда и Чанга [408]; (д) Нильсена, Нилла и Лафлама [306]; (е) Леунга, Вандерзипена, Жу, Шервуда, Яннони, Кубинека и Чанга [273]. Кроме того, некоторые квантовые алгоритмы были реализованы на небольших молекулах в работах Джоунса, Моска и Хансена [200, 201]. Оптимальная схема логической разметки, в которой достигается энтропийный предел, была разработана Шульманом и Вазирани [377].

Многие авторы отмечали недостатки метода ЯМР как способа реализации квантовых вычислений. Возможно, они наиболее полно рассмотрены в работе Шака и Кейвса [347], а также в более ранней работе Баунштейна, Кейвса, Йожа, Линдена, Попеску и Шака [35], технические заключения которых (не касающиеся впрочем метода ЯМР) были обоснованы в работах Видала и Таррacha [402] и Зычковского, Городецкого, Санпера и Левенштейна [433]. Эти вопросы обсуждались также в работе Линдена и Попеску [263].

Существует очень много вариантов реализации квантового компьютера и упомянуть о каждом из них здесь невозможно. Мы укажем лишь небольшое число работ, отсылая читателя к литературе, процитированной в этих работах. Множество вариантов реализации, включая использование полимерных систем, предложил Ллойд [251]. Накамура, Пашкин и Цай [307] осуществили управление кубитами, представленными отдельными куперовскими парами, а также наблюдали осцилляции Раби в такой системе. Представление кубита с помощью магнитного потока через сверхпроводящий контур изучалось в работе Моойа, Орландо, Левитова, Тяна, ван дер Валя и Ллойда [291]. Плацман и Дикман предложили использовать в качестве кубитов электроны на поверхности жидкого гелия [315]. Представление кубита с помощью суммарного спина электронов в квантовой точке (разд. 7.8) описано в работе Лосса и Дивинченцо [239]. Из этой же работы взята идея упр. 7.52. Ссылки на литературу о времени когерентности для квантовых точек приведена в работе Хауберса, Суиткеса, Маркуса, Кампмана и Госкарда [194]. Реализация квантового компьютера, в которой используются спины электронов в квантовых точках, управляемые методами КЭДР, обсуждается в работе Имамоглу, Ошалома, Буркарда, Дивинченцо, Лосса, Шервина и Смолла [196]. Квантовый компьютер на ядерных спинах примесей ^{31}P , прикрепленных к кремниевой подложке, был предложен Кейном [208]. Аналогичная конструкция, но для спинов электронов в кремний-германиевых гетероструктурах рассматривалась Врайеном, Яблоновичем, Вангом, Джангом, Баландиным, Ройчудхури, Мором и Дивинченцо [409]. Наконец, Бреннен, Кейвс, Йессен и Дойч [36] предложили реализацию квантовых вычислений на основе нейтральных атомов, удерживаемых в оптической решетке с частотой света, далекой от резонансных линий атомов.

При экспериментальной реализации квантовой телепортации в качестве кубитов использовались одиночные фотоны и ядерные спины, см. разд. «История и дополнительная литература» в конце гл. 1. В контексте настоящей главы следует отметить одну из таких реализаций, предложенную Фурусавой, Зоренсоном, Браунштейном, Фухсом, Кимблем и Польциком [155], поскольку в ней для представления квантовой информации используется не конечномерное, а бесконечномерное гильбертово пространство, так что базисные состо-

яния параметризованы *непрерывными переменными* (аналогично координате и импульсу в подразд. 7.3.2). Первоначально этот подход был предложен в работе Вайдмана [397] и затем развит в работе Браунштейна и Кимбля [56]. Представление с непрерывными переменными было использовано при рассмотрении сверхплотного кодирования Браунштейном и Кимблем [58], исправления ошибок в квантовых вычислениях Браунштейном [70] и независимо Ллойдом и Слотином [269] и для вычислений в работе Ллойда и Браунштейна [235].

Часть III

Квантовая информация

Глава 8

КВАНТОВЫЙ ШУМ И КВАНТОВЫЕ ПРЕОБРАЗОВАНИЯ

До настоящего момента мы в основном имели дело с динамикой *замкнутых* квантовых систем, т. е. квантовых систем, которые не испытывают никаких нежелательных взаимодействий с внешним миром. К каким бы замечательным заключениям мы не пришли, относительно тех задач обработки информации, которые в *принципе* можно решить при помощи таких идеальных систем, эти заключения омрачаются тем фактом, что в реальном мире не существует абсолютно замкнутых систем, разве что Вселенная в целом. Реальные системы находятся в нежелательном взаимодействии с внешним миром, которое проявляется в виде *шума* в системах квантовой обработки информации. Необходимо понимать и контролировать шумовые процессы, для того чтобы построить эффективную систему квантовой обработки информации. Этим проблемам и посвящена центральная часть III книги, которая открывается данной главой, где обсуждается *формализм квантовых преобразований* — эффективный набор средств, позволяющий описывать квантовый шум и поведение *открытых* квантовых систем.

В чем состоит различие между открытой и замкнутой системами? Качающийся маятник, такой же, как в некоторых механических часах, можно рассматривать как практически идеальную замкнутую систему. Маятник очень слабо взаимодействует с остальным миром — своей окружающей *средой* — в основном через трение. Тем не менее, чтобы адекватно описать полную динамику маятника, понять, почему в конце концов он останавливается, необходимо учесть тормозящее действие трения о воздух и несовершенство подвески маятника. Аналогичным образом никакая квантовая система не является абсолютно замкнутой, а уж тем более квантовые компьютеры, которые, чтобы выполнить определенный набор действий, должны быть аккуратно запрограммированы внешней системой. Например, если состояние кубита представляется двумя положениями электрона, то этот электрон будет взаимодействовать с другими

заряженными частицами, которые играют роль источника неконтролируемого шума, влияющего на состояние кубита. Открытая система есть не что иное, как система, по которой взаимодействует с некоторой другой окружающей системой, по которой мы хотели бы усреднить или чьей динамикой мы хотели бы пренебречь.

Математический формализм *квантовых преобразований* — это основной инструмент в нашем описании динамики открытых квантовых систем. Это очень мощный инструмент в том смысле, что он применим к широкому диапазону физических объектов. Его можно использовать не только для описания почти замкнутых систем, которые слабо связаны со своей средой, но и для систем с сильным взаимодействием со средой, а также для замкнутых систем, которые мгновенно открывают и подвергают измерению. Другим преимуществом квантовых преобразований применительно к квантовым вычислениям и квантовой информации является их исключительная приспособленность для описания *дискретных изменений состояния*, то есть переходов между начальным состоянием ρ и конечным состоянием ρ' без явной ссылки на течение времени. Этот дискретный подход отличается от традиционных методов (таких, как мастер-уравнения, уравнения Ланжевена и стохастические дифференциальные уравнения), используемых физиками для описания открытых квантовых систем, которые ближе к описанию системы в непрерывном времени.

Глава построена следующим образом. В начале (в разд. 8.1) обсуждается описание шума в классических системах. Знакомство с классическим шумом очень поможет при изучении квантовых преобразований и квантового шума. В разд. 8.2 вводится формализм квантовых преобразований с трех разных точек зрения; это позволит хорошо усвоить элементарную теорию квантовых преобразований. Несколько важных примеров шума проиллюстрированы в разделе 8.3 при помощи квантовых преобразований. Среди них деполяризация, затухание амплитуды и затухание фазы. Для описания квантового шума в отдельном кубите используется геометрический подход с применением сферы Блоха. В разд. 8.4 рассматриваются некоторые аспекты квантовых преобразований: как связать квантовые преобразования и другие методы, обычно используемые физиками для описания квантового шума (такие, как мастер-уравнения); как экспериментально определить динамику квантовой системы при помощи процедуры, называемой *томографией квантового процесса*; как при помощи квантовых преобразований объяснить тот факт, что мир вокруг нас кажется подчиняющимся законам классической физики, в то время как в действительности следует законам квантовой механики. Глава завершается разд. 8.5, где обсуждаются ограничения формализма квантовых преобразований как общего подхода к описанию шума в квантовых системах.

8.1 Классический шум и марковские процессы

Чтобы понять процедуру шума в квантовых системах, полезно вначале обратиться к рассмотрению шума в классических системах. Каким образом следует моделировать шум в классической системе? Чтобы понять, как это делается,

приведем простые примеры и посмотрим, чему они могут нас научить применительно к квантовому шуму.

Представьте себе бит, хранимый на жестком диске, присоединенном к обычному классическому компьютеру. Вначале он находится в состоянии 0 или 1, но весьма вероятно, что через длительное время побочные магнитные поля приведут к изменению его состояния. Пусть вероятность изменения состояния бита есть p , а вероятность того, что бит остался в прежнем состоянии, $(1 - p)$. Этот процесс изображен на рис. 8.1

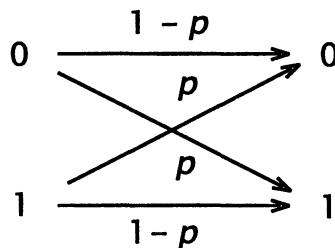


Рис. 8.1. Через продолжительное время состояние бита на жестком диске может измениться с вероятностью p

На самом деле, конечно, в окружающем пространстве присутствуют магнитные поля, которые могут изменить состояние бита. Чтобы выяснить вероятность переворота p , необходимо понять две вещи. Во-первых, потребуется модель, описывающая распределение магнитных полей в окружающем пространстве. Полагая, что пользователь жесткого диска не делает глупостей, таких, как размахивание около него сильным магнитом, можно построить реалистичную модель, измеряя магнитное поле в окружающей среде, похожей на ту, в которой будет работать этот жесткий диск. Во-вторых, необходима модель, описывающая взаимодействие окружающих магнитных полей с битами на диске. К счастью, такая модель уже существует и хорошо известна физикам — это уравнения Максвелла. Используя эти две модели, можно в принципе вычислить вероятность того, что состояние бита на диске изменится через некоторый определенный промежуток времени.

Выбор модели для окружающей среды и для взаимодействия системы со средой мы будем делать многократно, изучая шум как классический, так и квантовый. Взаимодействие с окружающей средой — это фундаментальный источник шума и в классических, и в квантовых системах. Часто непросто создать точную модель среды или взаимодействия система–среда, однако, разрабатывая модель и тщательно изучая наблюдаемые свойства системы, можно достичь высокой степени точности при моделировании шума в реальных физических системах.

Поведение бита на жестком диске можно кратко записать одним уравнением. Предположим, p_0 и p_1 — это начальные вероятности того, что бит находится в состояниях 0 или 1 соответственно. Пусть q_0 и q_1 — соответствующие вероятности после воздействия шума. Обозначим начальное состояние бита X , а

конечное — Y . Тогда, согласно правилу полной вероятности (Приложение 1), имеем

$$p(X = y) = \sum_x p(Y = y|X = x)p(X = x). \quad (8.1)$$

Условные вероятности $p(Y = y|X = x)$ называют *вероятностями переходов*, так как они характеризуют изменения, которые могут произойти в системе. Записывая эти уравнения в явном виде, для бита на жестком диске получим

$$\begin{bmatrix} q_0 \\ q_1 \end{bmatrix} = \begin{bmatrix} 1-p & p \\ p & 1-p \end{bmatrix} \begin{bmatrix} p_0 \\ p_1 \end{bmatrix}. \quad (8.2)$$

Рассмотрим более сложный пример шума в классической системе. Представьте, что мы пытаемся построить классическую схему для решения некоторой вычислительной задачи. К сожалению, для сборки схемы нам достались ненадежные детали. Наша несколько искусственная схема состоит из одного входного бита X , который проходит через два последовательно соединенных элемента *NOT* (НЕ), при этом получается промежуточный бит Y и окончательный бит Z . Естественно предположить, что правильное или ошибочное срабатывание второго элемента НЕ не зависит от того, правильно ли сработал первый. Такое предположение о том, что последовательные источники шума действуют независимо, физически осмысленно во многих ситуациях. Оно приводит к стохастическим процессам $X \rightarrow Y \rightarrow Z$ специального типа, называемым *марковскими процессами*. Физически предположение о марковском типе процессов соответствует тому, что окружение, вызывающее шум в первом элементе НЕ, считается действующим независимо от окружения, вызывающего шум во втором элементе. Это разумное предположение при условии, что элементы в пространстве сильно разнесены друг от друга.

Таким образом, шум в классических системах может быть описан при помощи теории стохастических процессов. Часто при анализе многоэтапных процессов марковские процессы являются хорошей моделью. Для одноэтапного процесса вероятности состояний на выходе \vec{q} связаны с вероятностями на входе \vec{p} уравнением

$$\vec{q} = E\vec{p}, \quad (8.3)$$

где E — матрица вероятностей перехода, которую будем называть *матрицей эволюции*. Таким образом, конечное состояние системы линейно связано с начальным. Это свойство линейности повторится при описании квантового шума, где матрицы плотности заменяют распределение вероятностей.

Какими свойствами должна обладать матрица эволюции E ? Наше требование состоит в том, чтобы при допустимом распределении вероятностей \vec{p} распределение $E\vec{p}$ тоже было допустимым. Это налагает два условия на E . Во-первых, все элементы E должны быть неотрицательны, это условие известно как требование *положительности*. Если бы оно не выполнялось, можно было бы получить отрицательные вероятности в $E\vec{p}$. Во-вторых, сумма элементов каждого столбца E должна быть равна 1, это условие известно как требование

полноты. Предположим, оно не выполняется. Допустим, например, что сумма элементов первого столбца не равна единице. Тогда, взяв \vec{p} с единицей в верхней позиции и всеми остальными элементами, равными нулю, увидим, что $E\vec{p}$ не оказывается допустимым распределением вероятностей.

Ключевые свойства классического шума можно сформулировать следующим образом: существует линейная связь между вероятностями на входе и выходе. Она описывается матрицей перехода с неотрицательными элементами (*положительность*), сумма которых по любому столбцу дает единицу (*полнота*). Системы с классическим шумом, действующим на протяжении нескольких этапов, описываются марковскими процессами при условии, что шум вызывается независимыми источниками. Каждое из этих ключевых свойств имеет важный аналог в теории квантового шума. Конечно, у квантового шума есть и некоторые неожиданные новые свойства.

8.2 Квантовые преобразования

8.2.1 Обзор

Формализм квантовых преобразований — главный инструмент для описания эволюции квантовых систем при самых разнообразных условиях, включая стохастические изменения квантовых состояний. В значительной степени марковские процессы таким же образом описывают стохастические изменения классических состояний. Подобно тому как классические состояния задаются векторами вероятностей, квантовые состояния можно описывать в терминах оператора плотности (матрицы плотности) ρ , свойства которого обсуждены в разд. 2.4. И так же, как классические состояния преобразуются в соответствии с формулой (8.3), квантовые состояния преобразуются согласно формуле

$$\rho' = \mathcal{E}(\rho). \quad (8.4)$$

Отображение \mathcal{E} в этом уравнении — это квантовое преобразование. Два простых примера квантовых преобразований, приведенные в гл. 2, — это унитарное преобразование и измерение, для которых $\mathcal{E}(\rho) = U\rho U^+$ и $\mathcal{E}_m(\rho) = M_m \rho M_m^+$ соответственно (см. ниже упр. 8.1 и 8.2). Квантовое преобразование заключает в себе динамическое изменение состояния, происходящее в результате некоторого физического процесса, ρ — это начальное состояние, а $\mathcal{E}(\rho)$ — конечное состояние по завершении процесса, возможно, с точностью до некоторого нормировочного множителя.

В следующих нескольких разделах будет развита общая теория квантовых преобразований, включающая унитарную эволюцию, измерение и даже более общие процессы. Будут обсуждены *три* различных подхода (рис. 8.2), все они эквивалентны. Первый основан на изучении динамики как следствия взаимодействия между системой и средой и схож с описанием классического шума в разд. 8.1. Это конкретный подход, и его легко связать с реальным миром. К сожалению, он страдает от одного недостатка — он математически неудобен.

Второй подход к пониманию квантовых преобразований, будучи полностью эквивалентным первому, преодолевает это неудобство, благодаря такому мощному математическому средству квантовых преобразований, как *представление операторной суммой*. Это довольно абстрактный метод, но он весьма полезен для вычислений и теоретических исследований. Третий подход, эквивалентный двум первым, описывает квантовые преобразования на языке набора физических аксиом, которым, как мы предполагаем, удовлетворяют динамические отображения в квантовой механике. Преимущество этого метода заключается в его общности, он показывает, что квантовая динамика описывается квантовыми преобразованиями при удивительно разнообразных внешних обстоятельствах. Однако он не представляет того *удобства* при вычислениях, которое обеспечивает второй подход и не обладает конкретностью первого. Вместе эти три подхода к квантовым преобразованиям являются мощным инструментом, при помощи которого можно понять природу квантового шума и его действие.

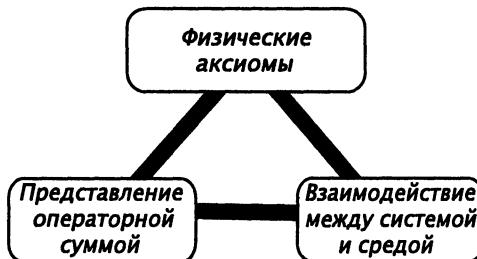


Рис. 8.2. Три подхода к квантовым преобразованиям, которые эквивалентны, но дают различные преимущества в зависимости от предполагаемого применения

Упражнение 8.1 (унитарная эволюция как квантовое преобразование). Чистое состояние эволюционирует при унитарном преобразовании как $|\psi\rangle \rightarrow U|\psi\rangle$. Покажите, что то же самое можно записать в виде $\rho \rightarrow \mathcal{E}(\rho) \equiv U\rho U^+$, для $\rho = |\psi\rangle\langle\psi|$.

Упражнение 8.2 (измерения как квантовые преобразования). Напомним (см.разд. 2.2.3), что квантовое измерение с возможными результатами m описывается набором измеряющих операторов M_m , таких что $\sum_m M_m^+ M_m = I$. Пусть ρ — состояние системы непосредственно перед измерением. Покажите, что для $\mathcal{E}_m(\rho) \equiv M_m \rho M_m^+$ состояние системы сразу после измерения можно представить как

$$\frac{\mathcal{E}_m(\rho)}{\text{tr}(\mathcal{E}_m(\rho))}. \quad (8.5)$$

Также покажите, что вероятность результата измерения равна $p(m) = \text{tr}(\mathcal{E}_m(\rho))$

8.2.2 Окружающая среда и квантовые преобразования

Динамика замкнутой квантовой системы описывается унитарным преобразованием. Умозрительно можно представить унитарное преобразование как черный

ящик, на вход которого подается исходное состояние, а на выходе получается результат, как показано на рис. 8.3, слева. Для наших целей внутреннее устройство ящика не существенно, его можно реализовать при помощи квантовой схемы, системы с некоторым гамильтонианом или каких-либо других средств.

Естественный способ описания динамики *открытой* квантовой системы — считать эту динамику следствием взаимодействия интересующей нас системы, которую будем называть *основной*, и *окружающей среды*. Вместе они образуют замкнутую квантовую систему (рис. 8.3, справа). Другими словами, предположим, имеется система, находящаяся в состоянии ρ , которую мы поместили в ящик, присоединенный к среде. Вообще говоря, окончательное состояние системы $\mathcal{E}(\rho)$ может не быть связанным унитарным преобразованием с исходным состоянием ρ . Мы *предполагаем* (пока), что исходное состояние системы — это прямое произведение $\rho \otimes \rho_{\text{окр.}}$. После преобразования U система больше не взаимодействует со средой и таким образом мы берем частичный след по окружению, чтобы получить приведенное состояние самой системы:

$$\mathcal{E}(\rho) = \text{tr}_{\text{env}} [U(\rho \otimes \rho_{\text{env}})U^\dagger]. \quad (8.6)$$

Конечно, если U не содержит никакого взаимодействия со средой, то $\mathcal{E}(\rho) = \tilde{U}\rho\tilde{U}^+$, где \tilde{U} — это часть U , которая действует на саму систему. Уравнение (8.6) — первое из трех эквивалентных *определений* квантовых преобразований.

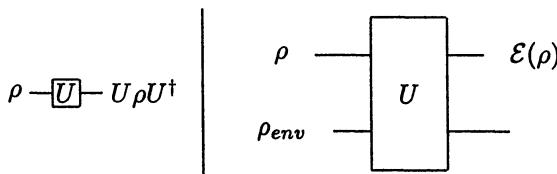


Рис. 8.3. Модели замкнутой (слева) и открытой (справа) квантовых систем.

В данном определении существенную роль играло предположение, что исходное состояние системы — прямое произведение. Вообще говоря, это неверно. Квантовая система всегда взаимодействует со средой, что приводит к увеличению корреляций, одним из проявлений которых является теплообмен между системой и средой. Предоставленная самой себе квантовая система будет релаксировать к состоянию с той же температурой, что и окружающая среда, т. е. между ними будет корреляция. Однако во многих случаях, представляющих практический интерес, резонно считать, что в начальный момент состояние системы и среды является прямым произведением. Когда экспериментатор приготавливает квантовую систему в определенном состоянии, он уничтожает все корреляции между системой и средой. В идеальном случае корреляции были бы полностью разрушены, а система находилась бы в чистом состоянии. Даже если этого нет, как мы увидим далее, формализм квантовых преобразований позволяет описывать динамику квантовой системы и в том случае, когда исходные состояния системы и окружающей среды не являются прямым произведением.

Другой важный вопрос: как задать U , если у среды фактически бесконечное число степеней свободы? Интересно отметить, что для адекватного описания любого возможного преобразования $\rho \rightarrow \mathcal{E}(\rho)$ оказывается достаточным описывать среду в гильбертовом пространстве размерности не более d^2 , если гильбертово пространство основной системы имеет размерность d . Также оказывается, что нет необходимости считать среду находящейся в смешанном состоянии в начальный момент, достаточно чистого состояния. Мы вернемся к этим вопросам в подразд. 8.2.3.

Приведем практический пример использования уравнения (8.6): рассмотрим квантовую цепь из двух кубитов (рис. 8.4), где U – элемент CNOT с основной системой, являющейся управляющим кубитом и окружающей средой, находящейся в начальный момент в состоянии $|\rho_{env}\rangle = |0\rangle\langle 0|$, в качестве управляемого кубита. Подставив эти выражения в уравнение (8.6), нетрудно заметить, что

$$\mathcal{E} = P_0\rho P_0 + P_1\rho P_1, \quad (8.7)$$

где $P_0 = |0\rangle\langle 0|$ и $P_1 = |1\rangle\langle 1|$ – проекционные операторы. Интуитивно ясно, как происходит такое преобразование: среда остается в состоянии $|0\rangle$, только если система находится в состоянии $|0\rangle$, в противном случае состояние среды меняется в $|1\rangle$. В следующем разделе мы выведем это уравнение в качестве примера представления операторной суммой.

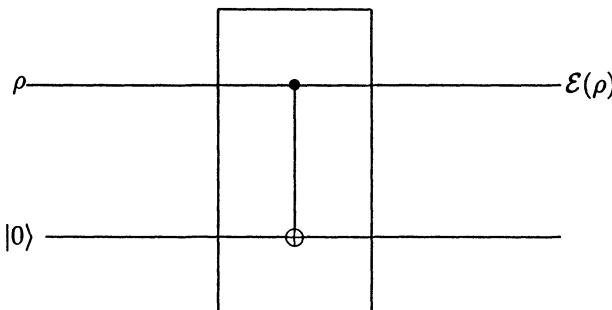


Рис. 8.4. Элемент CNOT как пример квантового преобразования одного кубита.

Мы описали квантовые преобразования как нечто, возникающее в результате взаимодействия основной системы с окружающей средой, однако стоит обобщить это определение, чтобы оно позволяло использовать отличающиеся пространства ввода и вывода. Например, рассмотрим один кубит A , который приготовлен в неизвестном состоянии ρ . Трехуровневая система («кутрит») B , в начальный момент приготовленная в некотором стандартном состоянии $|0\rangle$, начинает взаимодействовать с системой A посредством унитарного преобразования U , в результате чего полная система переходит в состояние $U(\rho \otimes |0\rangle\langle 0|)U^\dagger$. Теперь отбросим систему A , оставив систему B в некотором конечном состоянии ρ' . По определению квантовое преобразование \mathcal{E} , описывающее такой процесс, имеет вид

$$\mathcal{E}(\rho) = \rho' = \text{tr}_A(U(\rho \otimes |0\rangle\langle 0|)U^\dagger). \quad (8.8)$$

Заметим, что \mathcal{E} переводит операторы плотности исходной системы A в операторы плотности результирующей системы B . В дальнейшем по большей части будут обсуждаться квантовые преобразования «над» некоторой системой A , т. е. те, которые переводят операторы плотности системы A в операторы плотности системы A . Тем не менее иногда в приложениях оказывается полезным использовать более общее определение. Такое определение можно получить, назвав квантовыми преобразованиями класс отображений, которые возникают как результат следующей процедуры: некоторая исходная система подготовлена в некотором неизвестном квантовом состоянии ρ . Затем она приводится в контакт с другими системами, подготовленными в стандартных состояниях, при этом взаимодействие описывается некоторым унитарным оператором. После этого часть объединенной системы отбрасывается и остается одна окончательная система в некотором состоянии ρ' . Квантовое преобразование, определяющее такой процесс, просто переводит ρ в ρ' . Такое обобщение позволяет естественным образом сочетать несовпадающие пространства ввода и вывода в нашей трактовке квантовых преобразований представлением операторной суммой и в наших аксиоматических построениях. Все же в большинстве случаев можно упростить рассуждения предположением о том, что пространства ввода и вывода квантового преобразования совпадают, используя удобное разделение на «основную систему» и «среду», которое в общем случае, не имеет места. Иногда мы будем давать упражнения для демонстрации необходимых обобщений в случаях, когда пространства ввода и вывода различаются.

8.2.3 Представление операторной суммой

Квантовые преобразования могут быть представлены в элегантной форме, известной как *представление операторной суммой*, которая по существу повторяет уравнение (8.6) в терминах операторов в гильбертовом пространстве только основной системы. Главный результат мотивируется следующими простыми выкладками. Пусть $|e_k\rangle$ — ортонормированный базис в (конечномерном) пространстве состояний среды, а $\rho_{\text{окр}} = |e_0\rangle\langle e_0|$ — ее исходное состояние. Без потери общности можно считать, что начальное состояние среды чистое, так как, если оно смешанное, можно ввести дополнительную систему, очищающую состояние среды (см. разд. 2.5). Хотя эта дополнительная система фиктивная, она не влияет на динамику основной системы и может быть использована в качестве промежуточного шага в вычислениях. Уравнение (8.6) можно переписать в виде

$$\mathcal{E}(\rho) = \sum_k \langle e_k | U [\rho \otimes |e_0\rangle\langle e_0|] U^\dagger | e_k \rangle \quad (8.9)$$

$$= \sum_k E_k \rho E_k^\dagger, \quad (8.10)$$

где $E_k = \langle e_k | U | e_0 \rangle$ — оператор в пространстве состояний основной системы. Уравнение (8.10) называется представлением \mathcal{E} операторной суммой, а операторы E_k — элементами преобразования \mathcal{E} . Указанное представление важно, в оставшейся части книги мы неоднократно будем его использовать.

Элементы преобразования удовлетворяют важному ограничению, известному как *соотношение полноты*, аналогичному соотношению полноты для матрицы эволюции в описании классического шума. В классическом случае это соотношение полноты проистекает из условия нормировки распределения вероятности. В квантовом случае соотношение полноты возникает из аналогичного требования о том, что след $\mathcal{E}(\rho)$ равен единице:

$$1 = \text{tr}(\mathcal{E}(\rho)) \quad (8.11)$$

$$= \text{tr} \left(\sum_k E_k \rho E_k^\dagger \right) \quad (8.12)$$

$$= \text{tr} \left(\sum_k E_k^\dagger E_k \rho \right). \quad (8.13)$$

Так как это соотношение верно для всех ρ , должно выполняться тождество

$$\sum_k E_k^\dagger E_k = I. \quad (8.14)$$

Данное уравнение справедливо для *сохраняющих след* квантовых преобразований. Существуют также квантовые преобразования, не сохраняющие следа, для которых $\sum_k E_k^\dagger E_k \leq I$, но они описывают процессы, в которых дополнительная информация о происходящем приобретается при измерении (далее мы объясним это подробнее). Отображение \mathcal{E} вида (8.10), для которого $\sum_k E_k^\dagger E_k \leq I$, дает наше второе *определение* квантового преобразования. Ниже будет показано, что это определение по существу совпадает с первым (8.6) и фактически является несколько более общим, поскольку учитывает квантовые преобразования, не сохраняющие следа. Мы часто будем возвращаться к первому определению, а затем опять использовать второе: из контекста должно быть ясно, каким из определений мы пользуемся в каждом случае.

Упражнение 8.3. В нашем выводе представления операторной суммой неявно предполагалось, что пространства ввода и вывода преобразования совпадают. Предположим, составная система AB , находившаяся вначале в некотором неизвестном состоянии ρ , приводится в контакт с составной системой CD , находившейся вначале в некотором стандартном состоянии $|0\rangle$. Эти две системы влияют друг на друга посредством унитарного взаимодействия U . После взаимодействия мы отбрасываем системы A и D , получая состояние ρ' системы BC . Покажите, что отображение $\mathcal{E}(\rho) = \rho'$ удовлетворяет равенству

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger \quad (8.15)$$

для некоторого набора линейных операторов E_k , отображающих пространство состояний системы AB в пространство состояний системы BC , таких что $\sum_k E_k^+ E_k = I$.

Представление операторной суммой существенно, поскольку позволяет дать **внутренние характеристики динамики основной системы**. Такое представление описывает динамику основной системы без необходимости явно рассматривать свойства среды — все, что нам нужно знать, сосредоточено в операторах E_k , которые действуют только на основную систему. Это упрощает вычисления и часто способствует лучшему пониманию. Более того, многие различные взаимодействия со средой могут привести к одной и той же динамике основной системы. Если интересна именно динамика основной системы, то имеет смысл выбирать представление, которое не включает в себя несущественную информацию о других системах.

В конце этого подраздела исследуются свойства представления операторной суммой, и, в частности, его некоторые особенности. Так, будет дана его физическая интерпретация в терминах элементов преобразования E_k . Естественно возникает вопрос: как представление операторной суммой может быть определено для любой открытой квантовой системы (при условии, что, например, задано взаимодействие между системой и средой или какая-то иная информация)? Ответ на этот вопрос — вторая тема, которая будет затронута в заключительной части данного подраздела. Обратная задача — как построить модель открытой квантовой системы для любого представления операторной суммой — завершает этот подраздел.

Упражнение 8.4 (измерение). Предположим, имеется однокубитовая главная система, взаимодействующая с однокубитовой средой посредством преобразования

$$U = P_0 \otimes I + P_1 \otimes X, \quad (8.16)$$

где X — обычная матрица Паули (действующая на среду), а $P_0 \equiv |0\rangle\langle 0|$ и $P_1 \equiv |1\rangle\langle 1|$ — проекторы (действующие на систему). Найдите квантовое преобразование этого процесса в представлении операторной суммой, считая, что начальное состояние среды есть $|0\rangle$.

Упражнение 8.5 (переворот спина). То же, что в предыдущем упражнении, но

$$U = \frac{X}{\sqrt{2}} \otimes I + \frac{Y}{\sqrt{2}} \otimes X. \quad (8.17)$$

Найдите квантовое преобразование для этого процесса в представлении операторной суммой.

Упражнение 8.6 (композиция преобразований). Предположим, что \mathcal{E} и \mathcal{F} — преобразования одной квантовой системы. Покажите, что композиция $\mathcal{F} \circ \mathcal{E}$ — это квантовое преобразование в том смысле, что у него есть представление операторной суммой. Сформулируйте и докажите обобщение этого результата на случай, когда \mathcal{E} и \mathcal{F} не обязательно имеют совпадающие пространства ввода и вывода.

Физическая интерпретация представления операторной суммой

Существует занятная интерпретация, которую можно дать представлению операторной суммой. Представьте себе, что над средой в базисе $|e_k\rangle$ выполняется измерение после применения унитарного преобразования U . Применяя принцип неявного измерения, можно видеть, что такое измерение влияет только на состояние среды и не изменяет состояния основной системы. Пусть ρ_k — это состояние основной системы, соответствующее полученному результату k , т. е.

$$\rho_k \propto \text{tr}_E(|e_k\rangle\langle e_k|U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger|e_k\rangle\langle e_k|) = \langle e_k|U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger|e_k\rangle \quad (8.18)$$

$$= E_k \rho E_k^\dagger. \quad (8.19)$$

Нормируем ρ_k ,

$$\rho_k = \frac{E_k \rho E_k^\dagger}{\text{tr}(E_k \rho E_k^\dagger)} \quad (8.20)$$

и находим вероятность получения k :

$$p(k) = \text{tr}(|e_k\rangle\langle e_k|U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger|e_k\rangle\langle e_k|) \quad (8.21)$$

$$= \text{tr}(E_k \rho E_k^\dagger). \quad (8.22)$$

Следовательно,

$$\mathcal{E} = \sum_k p(k) \rho_k = \sum_k E_k \rho E_k^\dagger. \quad (8.23)$$

Эта формула дает красивую физическую интерпретацию квантовых преобразований с элементами $\{E_k\}$. Действие квантового преобразования эквивалентно взятию состояния ρ и случайной его замене на $E_k \rho E_k^\dagger / \text{tr}(E_k \rho E_k^\dagger)$ с вероятностью $\text{tr}(E_k \rho E_k^\dagger)$. В таком виде это очень похоже на понятие канала с шумом, используемое в классической теории информации. В этом смысле мы будем иногда называть некоторые квантовые преобразования, описывающие процессы квантового шума, квантовыми каналами с шумом.

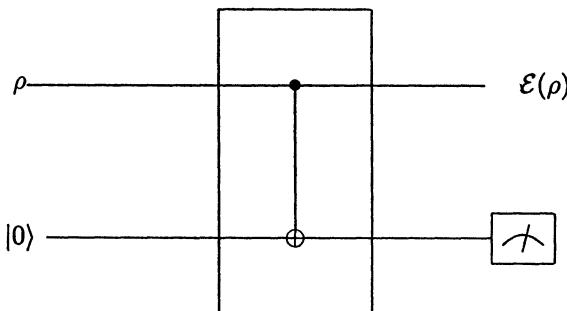


Рис. 8.5. Элемент CNOT как элементарная модель измерения отдельного кубита.

Простой пример (см. рис. 8.4) иллюстрирует такую интерпретацию представления операторной суммой. Предположим, мы выбрали состояния $|e_k\rangle = |0_E\rangle$ и $|1_E\rangle$, где использован индекс E , чтобы подчеркнуть, что данные состояния относятся к среде. Это можно интерпретировать как справедливое измерение в базисе кубита среды (рис. 8.5). Выполнение такого измерения не изменяет, конечно, состояния основной системы. Используя индексы P для обозначения основной системы, действие CNOT можно раскрыть как

$$U = |0_P 0_E\rangle\langle 0_P 0_E| + |0_P 1_E\rangle\langle 0_P 1_E| + |1_P 1_E\rangle\langle 1_P 0_E| + |1_P 0_E\rangle\langle 1_P 1_E|, \quad (8.24)$$

следовательно,

$$E_0 = \langle 0_E | U | 0_E \rangle = |0_P\rangle\langle 0_P|, \quad (8.25)$$

$$E_1 = \langle 1_E | U | 0_E \rangle = |1_P\rangle\langle 1_P|, \quad (8.26)$$

и, таким образом, имеем

$$\mathcal{E}(\rho) = P_0 \rho P_0 + P_1 \rho P_1 \quad (8.27)$$

в соответствии с уравнением (8.7).

Измерение и представление операторной суммой

Если имеется описание открытой квантовой системы, то можно найти представление ее динамики операторной суммой? Впрочем, ответ нам уже известен: имея унитарное преобразование для системы и среды и базис состояний $|e_k\rangle$ среды, элементы преобразования мы определяем выражением:

$$E_k \equiv \langle e_k | U | e_0 \rangle. \quad (8.28)$$

Можно еще больше обобщить этот результат, если разрешить выполнять измерения над составной системой (система — среда) после унитарного взаимодействия, которые позволяют приобрести информацию о квантовом состоянии. Оказывается, такая физическая возможность естественным образом связана с не сохраняющими след квантовыми преобразованиями, т. е. отображениями $\mathcal{E}(\rho) = \sum_k E_k \rho E_k^+$, такими, что $\sum_k E_k^+ E_k \leq I$.

Пусть основная система в начальный момент находится в состоянии ρ , для удобства будем обозначать ее буквой Q . К системе Q присоединена окружающая ее система E . Предположим, что Q и E в начальный момент — независимые системы и что E в начальный момент находится в некотором стандартном состоянии σ . Таким образом, начальное состояние объединенной системы можно представить как

$$\rho^{QE} = \rho \otimes \sigma. \quad (8.29)$$

Мы считаем, что взаимодействие между системами описывается унитарным оператором U . После выключения взаимодействия над объединенной системой осуществляется проективное измерение, описываемое проекторами P_m . Случай, когда измерение не производится, соответствует специальному выбору,

когда существует только один возможный результат измерения $m = 0$, соответствующий проектору $P_0 \equiv I$.

Эта ситуация проиллюстрирована на рис. 8.6. Наша цель — определить конечное состояние Q' как функцию начального состояния ρ . Конечное состояние QE задается выражением

$$\frac{P_m U(\rho \otimes \sigma) U^\dagger P_m}{\text{tr}(P_m U(\rho \otimes \sigma) U^\dagger P_m)}, \quad (8.30)$$

если был получен результат измерения m . После взятия следа по E конечное состояние Q определяется как

$$\frac{\text{tr}_E(P_m U(\rho \otimes \sigma) U^\dagger P_m)}{\text{tr}(P_m U(\rho \otimes \sigma) U^\dagger P_m)}. \quad (8.31)$$

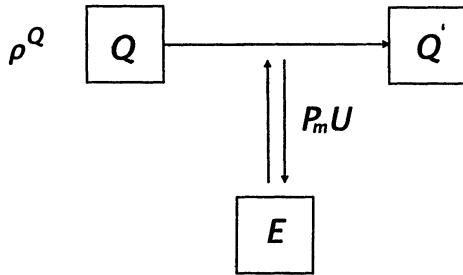


Рис. 8.6. Модель система — среда квантовых преобразований

Это представление конечного состояния зависит от начального состояния среды σ , взаимодействия U и измеряющего оператора P_m . Определим отображение

$$\mathcal{E}(\rho) \equiv \text{tr}_E(P_m U(\rho \otimes \sigma) U^\dagger P_m), \quad (8.32)$$

так что конечное состояние $Q = \mathcal{E}_m(\rho) / \text{tr}(\mathcal{E}_m(\rho))$. Заметим, что $\text{tr}(\mathcal{E}_m(\rho))$ — это вероятность получить m в результате измерения. Пусть $\sigma = \sum_j q_j |j\rangle \langle j|$ — диагонализация для σ . Введем ортонормированный базис $|e_k\rangle$ для системы E . Заметим, что

$$\mathcal{E}(\rho) = \sum_{jk} q_j \text{tr}_E(|e_k\rangle \langle e_k| P_m U(\rho \otimes |j\rangle \langle j|) U^\dagger P_m |e_k\rangle \langle e_k|) \quad (8.33)$$

$$= \sum_{jk} E_{jk} \rho E_{jk}^\dagger, \quad (8.34)$$

где

$$E_{jk} \equiv \sqrt{q_j} \langle e_k | P_m U | j \rangle. \quad (8.35)$$

Это уравнение является обобщением уравнения (8.10) и позволяет явным образом вычислить операторы, входящие в представление операторной суммой

для \mathcal{E}_m , при условии, что начальное состояние σ системы E и взаимодействие между E и Q известны. Квантовые преобразования \mathcal{E}_m можно представлять как описание некоторого процесса измерения, обобщающее описание измерения, данное в гл. 2.

Упражнение 8.7. Предположим, что вместо того, чтобы выполнять проективное измерение составной системы (основная система + среда), мы произвели измерение общего вида, описываемое операторами измерения $\{M_m\}$. Найдите представление операторной суммой для соответствующих квантовых преобразований \mathcal{E}_m основной системы и покажите, что соответствующие вероятности получения различных результатов измерения равны $\text{tr}(\mathcal{E}_m(\rho))$.

*Модели система – среда для произвольного представления
операторной суммой*

Мы показали, что взаимодействующие квантовые системы естественным образом приводят к использованию представления квантовых преобразований операторной суммой. А насчет обратной задачи? Существуют ли «разумные» модельные среды и взаимодействия, приводящие к квантовому преобразованию, соответствующему данному набору операторов $\{E_k\}$? Под «разумным» взаимодействием мы подразумеваем то, что это либо унитарная эволюция, либо проективное измерение. Здесь мы обсудим, как построить такую систему. Наша конструкция предназначена только для квантовых преобразований, отображающих пространство ввода в то же самое пространство вывода, но распространение ее на более общий случай тривиально. В частности, мы покажем, что для любого, сохраняющего или не сохраняющего след квантового преобразования \mathcal{E} с элементами $\{E_k\}$, существуют модельная среда E , находящаяся в начальный момент в чистом состоянии $|e_0\rangle$, и модельная динамика, определяемая унитарным оператором U и проектором P в E , так что

$$\mathcal{E}(\rho) = \text{tr}_E(PU(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger P). \quad (8.36)$$

Чтобы убедиться в этом, предположим сначала, что \mathcal{E} — это сохраняющее след квантовое преобразование с представлением операторной суммой, генерируемым элементами преобразования $\{E_k\}$, удовлетворяющими соотношению полноты $\sum_k E_k^\dagger E_k = I$, поэтому необходимо только найти подходящий унитарный оператор U , чтобы смоделировать эту динамику. Пусть $|e_k\rangle$ — ортонормированный базис для E , так что индекс k задает взаимнооднозначное соответствие с операторами E_k . Заметим, что, по определению, в E такой базис существует: мы пытаемся найти *модельную* среду, приводящую к динамике, описываемой элементами преобразования $\{E_k\}$. Определим оператор U со следующим действием на состояния вида $|\psi\rangle|e_0\rangle$:

$$U|\psi\rangle|e_0\rangle \equiv \sum_k E_k |\psi\rangle|e_k\rangle, \quad (8.37)$$

где $|e_0\rangle$ — некоторое стандартное состояние модельной среды.

Заметим, что для произвольных состояний $|\psi\rangle$ и $|\varphi\rangle$ основной системы справедливо уравнение

$$\langle\psi|\langle e_0|U^\dagger U|\varphi\rangle|e_0\rangle = \sum_k \langle\psi|E_k^\dagger E_k|\varphi\rangle = \langle\psi|\varphi\rangle \quad (8.38)$$

вследствие соотношения полноты. Таким образом, оператор U можно расширить до унитарного оператора, действующего на всем пространстве объединенной системы. Легко проверить, что

$$\text{tr}_E(U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger) = \sum_k E_k \rho E_k^\dagger, \quad (8.39)$$

так что данная модель реализует квантовое преобразование \mathcal{E} с элементами $\{E_k\}$. Этот результат проиллюстрирован во вставке 8.1.

Не сохраняющие след квантовые преобразования можно легко моделировать, используя схожие идеи (упр. 8.8). Более интересное обобщение этой конструкции возникает в случае набора квантовых преобразований $\{\mathcal{E}_m\}$, соответствующих возможным результатам измерения, вследствие чего квантовое преобразование $\sum_m \mathcal{E}_m$ сохраняет след, поскольку сумма вероятностей различных исходов равна единице и $1 = \sum_m p(m) = \text{tr}[(\sum_m \mathcal{E}_m)(\rho)]$ для всех возможных начальных состояний ρ (см упражнение 8.9)

Упражнение 8.8 (квантовые преобразования, не сохраняющие след). Объясните, как построить унитарный оператор для модели системы — окружающая среда не сохраняющего след квантового преобразования, введя в набор элементов преобразования E_k дополнительный оператор E_∞ , выбранный таким образом, что при суммировании по всему множеству k (включая $k = \infty$) получается $\sum_k E_k^\dagger E_k = I$.

Упражнение 8.9 (модель измерений). Если дан набор квантовых преобразований $\{\mathcal{E}_m\}$, таких, что $\sum_m \mathcal{E}_m$ сохраняет след, то можно построить модель измерений, приводящую к этому набору квантовых преобразований. Пусть для каждого m E_{mk} — набор элементов преобразования \mathcal{E}_m . Введем систему среды E с ортонормированным базисом $|m, k\rangle$, находящимся во взаимооднозначном соответствии с набором индексов элементов преобразования. Аналогично предыдущему построению определим оператор U следующим образом:

$$U|\psi\rangle|e_0\rangle = \sum_{mk} |\psi\rangle|m, k\rangle. \quad (8.40)$$

Далее определим проекторы $P_m = \sum_k |m, k\rangle\langle m, k|$ на системе окружающей среды E . Покажите, что после применения U к $\rho \otimes |e_0\rangle\langle e_0|$, измерение P_m дает результат m с вероятностью $\text{tr}(\mathcal{E}_m(\rho))$, а соответствующее состояние основной системы после измерения будет иметь вид $\mathcal{E}_m(\rho) \text{tr}(\mathcal{E}_m(\rho))$.

8.2.4 Аксиоматический подход к квантовым преобразованиям

До настоящего момента нашим основным мотивом для изучения квантовых преобразований было то, что они предоставляют элегантный способ изучения

систем, взаимодействующих с окружающей средой. Теперь мы собираемся перейти к другой точке зрения — попытаемся записать физически осмыслиенные аксиомы, которым, как мы надеемся, должны удовлетворять квантовые преобразования. Эта точка зрения более абстрактна, чем подход, использованный нами ранее и основанный на явной модели системы-среда, но он также чрезвычайно эффективен вследствие абстрактности.

Вставка 8.1. Реализация квантовых преобразований

Используя сохраняющее след квантовое преобразование, выраженное в представлении операторной суммой $\mathcal{E}(\rho) = \sum_k E_k \rho E_k^+$, можно сконструировать для него физическую модель следующим образом. С учетом формулы (8.10) U должно удовлетворять условию

$$E_k = \langle e_k | U | e_0 \rangle, \quad (8.41)$$

где U — некоторый унитарный оператор, а $|e_k\rangle$ — ортонормированные базисные векторы системы среды. Такой U удобно представить в виде блочной матрицы:

$$U = \begin{bmatrix} [E_1] & \cdot & \cdot & \cdot & \cdots \\ [E_2] & \cdot & \cdot & \cdot & \cdots \\ [E_3] & \cdot & \cdot & \cdot & \cdots \\ [E_4] & \cdot & \cdot & \cdot & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{bmatrix} \quad (8.42)$$

в базисе $|e_k\rangle$. Заметим, что элементы преобразования E_k определяют только первую колонку блоков этой матрицы (в отличие от других ситуаций здесь удобно, чтобы первый индекс соответствовал состояниям среды, а второй — основной системы). Определение оставшейся части матрицы остается за нами, мы просто выбираем эти элементы таким образом, чтобы U был унитарным. Заметим, что в соответствии с результатами гл. 4, U может быть реализован квантовой схемой.

Метод, к которому мы собираемся перейти, состоит в следующем. Прежде всего мы намереваемся забыть все, что узнали о квантовых преобразованиях и начать заново определять квантовые преобразования в соответствии с набором аксиом, которые обоснуем физически. Сделав это, докажем, что отображение \mathcal{E} удовлетворяет этим аксиомам в том и только в том случае, если может быть представлено операторной суммой, тем самым установив недостающую связь между абстрактными аксиоматическими формулировками и нашими предыдущими рассуждениями.

Мы определяем квантовое преобразование \mathcal{E} как отображение из множества операторов плотности исходного пространства Q_1 во множество операторов плотности результирующего пространства Q_2 , удовлетворяющее следующим

трем аксиоматическим свойствам (заметим, что для простоты обозначений мы считаем $Q_1 = Q_2 = Q$):

- A1. Во-первых, $\text{tr}(\mathcal{E}(\rho))$ — вероятность того, что процесс, представляемый \mathcal{E} , вообще произойдет; здесь ρ — начальное состояние. Следовательно, $0 \leq \text{tr}(\mathcal{E}(\rho)) \leq 1$ для любого состояния ρ .
- A2. Во-вторых, \mathcal{E} — линейное отображение на множестве матриц плотности, т. е. для вероятностей $\{p_i\}$ имеем

$$\mathcal{E}\left(\sum_i p_i \rho_i\right) = \sum_i p_i \mathcal{E}(\rho_i). \quad (8.43)$$

- A3. В третьих, \mathcal{E} — вполне положительное отображение. Это значит, что, если \mathcal{E} отображает операторы плотности системы Q_1 в операторы плотности системы Q_2 , то $\mathcal{E}(A)$ должно быть неотрицательно определенным для любого положительного оператора A . Более того, если ввести дополнительную систему R произвольной размерности, должен быть верным следующий факт: $(\mathcal{I} \otimes \mathcal{E})(A)$ положительно для любого неотрицательно определенного оператора A составной системы RQ_1 , где \mathcal{I} обозначает тождественное отображение системы R .

Первое свойство введено для математического удобства. Чтобы рассматривать измерения, удобно условиться, что \mathcal{E} не обязательно сохраняет след матрицы плотности, т.е. $\text{tr}(\rho) = 1$. Более того, примем, что \mathcal{E} должно быть определено таким образом, что $\text{tr}(\mathcal{E}(\rho))$ равен вероятности получения описываемого \mathcal{E} результата измерения. Например, предположим, что мы осуществляли проективное измерение в базисе отдельного кубита. Тогда для описания этого процесса используются два квантовых преобразования, определяемые тождествами $\mathcal{E}_0(\rho) \equiv |0\rangle\langle 0|\rho|0\rangle\langle 0|$ и $\mathcal{E}_1(\rho) \equiv |1\rangle\langle 1|\rho|1\rangle\langle 1|$. Обратите внимание, что вероятности соответствующих результатов измерения равны $\text{tr}(\mathcal{E}_0(\rho))$ и $\text{tr}(\mathcal{E}_1(\rho))$. Используя эту договоренность, получим правильно нормированное конечное состояние

$$\frac{\mathcal{E}(\rho)}{\text{tr}[\mathcal{E}(\rho)]}. \quad (8.44)$$

В случае, если процесс детерминированный, т. е. никакого измерения не выполняется, это сводится к требованию $\text{tr}(\mathcal{E}(\rho)) = 1 = \text{tr}(\rho)$ для всех ρ . Как обсуждалось выше, в этом случае можно сказать, что квантовое преобразование сохраняет след, поскольку \mathcal{E} дает полное описание квантового процесса. В то же время, если существует такое ρ , что $\text{tr}(\mathcal{E}(\rho)) < 1$, то квантовое преобразование не сохраняет след, так как \mathcal{E} не предоставляет полного описания процессов, которые могут произойти с системой (т. е. с некоторой вероятностью может получиться другой результат измерения). *Физическое* квантовое преобразование удовлетворяет требованию, что вероятности никогда не превышают единицы, т.е. $\text{tr}(\mathcal{E}(\rho)) \leq 1$.

Второе свойство также проистекает из физического требования к квантовым преобразованиям. Предположим, вход ρ квантового преобразования получается случайным выбором состояния из ансамбля $\{\rho_i, p_i\}$ квантовых состояний, то есть $\rho = \sum_i p_i \rho_i$. Тогда можно было бы ожидать, что результирующее состояние $\mathcal{E}(\rho)/\text{tr}(\mathcal{E}(\rho)) = \mathcal{E}(\rho)/p(\mathcal{E})$ соответствует случайной выборке из ансамбля $\{p(i|\mathcal{E}), \mathcal{E}(\rho_i)/\text{tr}(\mathcal{E}(\rho_i))\}$, где $p(i|\mathcal{E})$ — вероятность того, что было приготовлено состояние ρ_i , при условии, что процесс \mathcal{E} осуществился. Следовательно,

$$\mathcal{E}(\rho) = p(\mathcal{E}) \sum_i p(i|\mathcal{E}) \frac{\mathcal{E}(\rho_i)}{\text{tr}[\mathcal{E}(\rho_i)]}, \quad (8.45)$$

где $p(\mathcal{E}) = \text{tr}(\mathcal{E}(\rho))$ — вероятность того, что с состоянием ρ произошел процесс, описываемый \mathcal{E} . По правилу Байеса (Приложение 1) имеем

$$p(i|\mathcal{E}) = p(\mathcal{E}|i) \frac{p_i}{p(\mathcal{E})} = \frac{\text{tr}[\mathcal{E}(\rho_i)] p_i}{p(\mathcal{E})}, \quad (8.46)$$

тогда формула (8.45) сводится к (8.43).

Третье свойство также возникает из важного физического требования, что не только $\mathcal{E}(\rho)$ должно быть допустимой матрицей плотности (с точностью до нормировки), если таковой является ρ , но, более того, если $\rho = \rho_{RQ}$ — матрица плотности некоторого объединения систем R и Q , а \mathcal{E} действует только на Q , то $\mathcal{E}(\rho_{RQ})$ должно также приводить к допустимой матрице плотности (с точностью до нормировки) составной системы. Соответствующий пример дан во вставке 8.2. Формально предположим, что мы ввели вторую (конечномерную) систему R . Пусть \mathcal{I} обозначает тождественное отображение для системы R . Тогда отображение $\mathcal{I} \otimes \mathcal{E}$ должно преобразовывать неотрицательно определенные операторы в неотрицательно определенные операторы.

Вставка 8.2. Вполне положительный или положительный

Операция транспонирования над отдельным кубитом является примером, показывающим, почему важно, чтобы квантовые преобразования были вполне положительны. По определению это отображение соответствует транспонированию оператора плотности в выбранном базисе:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \xrightarrow{\mathcal{T}} \begin{bmatrix} a & c \\ b & d \end{bmatrix}. \quad (8.47)$$

Данное отображение положительно на операторах плотности одного отдельного кубита. Предположим, однако, что кубит — часть системы из двух кубитов, исходно находившихся в начальный момент в запутанном состоянии

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}, \quad (8.48)$$

а оператор транспонирования применяется к первому из этих двух кубитов, в то время как второй изменяется тривиальным образом. Тогда оператор плотности системы после преобразования примет вид

$$\frac{1}{2} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \quad (8.49)$$

Вычисления показывают, что собственные значения этого оператора равны $1/2, 1/2, 1/2$ и $-1/2$, т. е. это — недопустимый оператор плотности. Таким образом, операция транспонирования — пример положительного отображения, которое не вполне положительно, т. е. оно сохраняет положительность операторов основной системы, но теряет это свойство, если его применить к системам, которые включают в себя основную систему как подсистему.

Может показаться удивительным, что этих трех аксиом достаточно для определения квантовых преобразований. Тем не менее следующая теорема показывает, что они эквивалентны ранее использовавшимся моделям систем-окружающая среда и определению в терминах представления операторной суммой.

Теорема 8.1. Отображение \mathcal{E} удовлетворяет аксиомам A1, A2 и A3 в том и только в том случае, если

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger \quad (8.50)$$

для некоторого набора операторов $\{E_i\}$, которые отображают исходное гильбертово пространство в результирующее гильбертово пространство, и $\sum_i E_i^\dagger E_i \leq I$.

Доказательство.

Положим $\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger$. Очевидно, что \mathcal{E} линейно, поэтому для проверки того, что \mathcal{E} — квантовое преобразование, необходимо доказать только то, что оно вполне положительно. Пусть A — любой неотрицательно определенный оператор, действующий на пространство состояний расширенной системы RQ , а $|\psi\rangle$ — некоторое состояние RQ . Определив $|\varphi_i\rangle = (I_R \otimes E_i^\dagger)|\psi\rangle$, получим

$$\langle \psi | (I_R \otimes E_i) A (I_R \otimes E_i^\dagger) |\psi\rangle = \langle \varphi_i | A | \varphi_i \rangle \quad (8.51)$$

$$\geq 0 \quad (8.52)$$

вследствие того, что неотрицательно определенный оператор A . Следовательно,

$$|\psi\rangle(\mathcal{I} \otimes \mathcal{E})(A)|\psi\rangle = \sum_i \langle \varphi_i | A | \varphi_i \rangle \geq 0, \quad (8.53)$$

и, таким образом, для любого неотрицательно определенного оператора A оператор $(\mathcal{I} \otimes \mathcal{E})(A)$ тоже неотрицательно определенный, как и требовалось доказать. Требование $\sum_i E_i^+ E_i \leq I$ обеспечивает то, что вероятности меньше или равны 1. Этим завершается первая часть доказательства.

Предположим далее, что \mathcal{E} удовлетворяет аксиомам А1, А2 и А3. Наша цель найти представление \mathcal{E} операторной суммой. Предположим, мы ввели систему R той же размерности, что и исходная квантовая система Q . Пусть $|i_R\rangle$ и $|i_Q\rangle$ — ортонормированные базисы для R и Q . Удобно использовать один индекс i для обоих базисов и это, конечно, можно сделать, так как R и Q имеют одинаковую размерность. Определим общее состояние $|\alpha\rangle$ системы RQ формулой

$$|\alpha\rangle \equiv \sum_i |i_R\rangle |i_Q\rangle. \quad (8.54)$$

Состояние $|\alpha\rangle$ — с точностью до нормировочного множителя — максимально запутанное состояние систем R и Q . Такая интерпретация $|\alpha\rangle$ как максимально запутанного состояния может помочь в понимании дальнейшего построения. Далее, определим оператор σ на пространстве состояний RQ выражением

$$\sigma \equiv (\mathcal{I}_R \otimes \mathcal{E})(|\alpha\rangle\langle\alpha|). \quad (8.55)$$

Можно представлять его как результат действия квантового преобразования \mathcal{E} на одну половину максимально запутанного состояния системы RQ . Теперь продемонстрируем замечательный факт, что оператор σ полностью определяет квантовое преобразование \mathcal{E} . То есть, чтобы узнать, как \mathcal{E} действует на произвольное состояние системы Q , достаточно знать, как оно действует лишь на одно состояние, максимально запутанное с другой системой!

Прием, который позволяет восстановить \mathcal{E} по σ состоит в следующем. Положим, $|\psi\rangle = \sum_j \psi_j |j_Q\rangle$ — некоторое состояние системы Q . Определим соответствующее состояние $|\tilde{\psi}\rangle$ системы R уравнением

$$|\tilde{\psi}\rangle \equiv \sum_j \psi_j^* |j_R\rangle. \quad (8.56)$$

Заметим, что

$$\langle \tilde{\psi} | \sigma | \tilde{\psi} \rangle = \langle \tilde{\psi} | \left(\sum_{ij} |i_R\rangle \langle j_R| \otimes \mathcal{E}(|i_Q\rangle \langle j_Q|) \right) | \tilde{\psi} \rangle \quad (8.57)$$

$$= \sum_{ij} \psi_i \psi_j^* \mathcal{E}(|i_Q\rangle \langle j_Q|) \quad (8.58)$$

$$= \mathcal{E}(|\psi\rangle \langle \psi|). \quad (8.59)$$

Пусть $\sigma = \sum_i |s_i\rangle\langle s_i|$ — некоторое разложение σ , причем векторы $|s_i\rangle$ ненормированы. Определим отображение

$$E_i(|\psi\rangle) \equiv \langle \tilde{\psi} | s_i \rangle. \quad (8.60)$$

Легко показать, что это — линейное отображение, т.е. E_i — линейный оператор на пространстве состояний Q . Более того, имеем

$$\sum_i E_i |\psi\rangle\langle\psi| E_i^\dagger = \langle \tilde{\psi} | s_i \rangle \langle s_i | \tilde{\psi} \rangle \quad (8.61)$$

$$= \langle \tilde{\psi} | \sigma | \tilde{\psi} \rangle \quad (8.62)$$

$$= \mathcal{E}(|\psi\rangle\langle\psi|). \quad (8.63)$$

Тогда

$$\mathcal{E}(|\psi\rangle\langle\psi|) = \sum_i E_i |\psi\rangle\langle\psi| E_i^\dagger \quad (8.64)$$

для всех чистых состояний $|\psi\rangle$ системы Q . Из линейности следует, что

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger. \quad (8.65)$$

Условие $\sum_i E_i^\dagger E_i \leq I$ вытекает непосредственно из аксиомы **A1**, связывающей след $\mathcal{E}(\rho)$ с вероятностью. ■

Неопределенность в представлении операторной суммой

Мы видели, что представление операторной суммой дает очень общее описание динамики открытой квантовой системы. Однозначно ли такое описание?

Рассмотрим квантовые преобразования \mathcal{E} и \mathcal{F} , действующие на отдельный кубит, в представлении операторной суммой $\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$ и $\mathcal{F}(\rho) = \sum_k F_k \rho F_k^\dagger$, где элементы преобразований \mathcal{E} и \mathcal{F} определены формулами

$$E_1 = \frac{I}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad E_2 = \frac{Z}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad (8.66)$$

и

$$F_1 = |0\rangle\langle 0| = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad F_2 = |1\rangle\langle 1| = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}. \quad (8.67)$$

Эти квантовые преобразования выглядят совершенно по-разному. Интересно то, что \mathcal{E} и \mathcal{F} , в действительности — это *одно и то же квантовое преобразование*. Чтобы убедиться в этом, заметим, что $F_1 = (E_1 + E_2)/\sqrt{2}$ и $F_2 = (E_1 - E_2)/\sqrt{2}$. Следовательно, имеем

$$\mathcal{F}(\rho) = \frac{(E_1 + E_2)\rho(E_1^\dagger + E_2^\dagger) + (E_1 - E_2)\rho(E_1^\dagger - E_2^\dagger)}{2} \quad (8.68)$$

$$= E_1 \rho E_1^\dagger + R_2 \rho E_2^\dagger \quad (8.69)$$

$$= \mathcal{E}(\rho). \quad (8.70)$$

Этот пример показывает, что элементы преобразования, возникающие в представлении операторной суммой, неоднозначны.

Неоднозначность в этом представлении очень интересна. Предположим, мы подбросили «честную монету» и в зависимости от того, что выпало, применили к системе одно из унитарных преобразований квантовой системы I или Z . Этот процесс соответствует первому представлению \mathcal{E} операторной суммой. Второе представление \mathcal{E} операторной суммой (обозначенное выше \mathcal{F}) соответствует проведению проективного измерения в базисе $\{|0\rangle, |1\rangle\}$ с неизвестным результатом. Эти два, очевидно, совершенно разных физических процесса приводят к одной и той же динамике основной системы.

В каком случае два набора элементов дают одно и то же квантовое преобразование? Ответ на этот вопрос важен, по меньшей мере, по двум причинам. Во-первых, с физической точки зрения неопределенность в выборе представления позволяет более глубоко понять, как разные физические процессы приводят к одинаковой динамике системы. Во-вторых, эта неопределенность имеет решающее значение для правильного понимания квантового исправления ошибок.

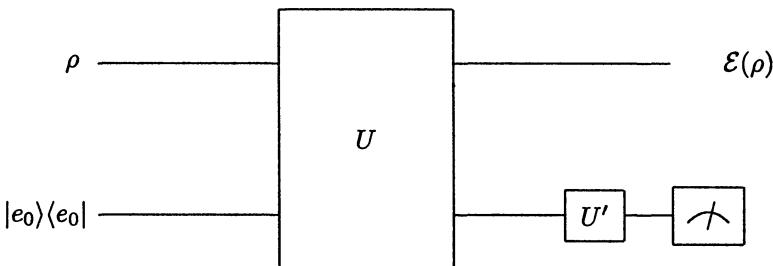


Рис. 8.7. Происхождение унитарной неопределенности представления операторной суммой.

Интуитивно ясно, что должна существовать большая свобода в представлении операторной суммой. Рассмотрим сохраняющее след квантовое преобразование \mathcal{E} , которое описывает динамику некоторой системы, такой, например, как на рис. 8.3, справа. Было показано, что элементы преобразования $E_k = \langle e_k | U | e_0 \rangle$ для \mathcal{E} можно связать с ортонормированным базисом среды. Предположим, к взаимодействию U мы добавили дополнительное унитарное действие U' только на среду (рис. 8.7). Очевидно, это не изменит состояния основной системы. Какие элементы преобразования соответствуют этому новому процессу $(I \otimes U')U$? Имеем

$$F_k = \langle e_k | (I \otimes U')U | e_0 \rangle \quad (8.71)$$

$$= \sum_j [I \otimes \langle e_k | U' | e_j \rangle] \langle e_j | U | e_0 \rangle \quad (8.72)$$

$$= \sum_j U'_{kj} E_j, \quad (8.73)$$

где мы использовали тот факт, что $\sum_j |e_j\rangle\langle e_j| = I$, а U'_{kj} — элементы матрицы U' в базисе $|e_k\rangle$. Оказывается, такой произвол в представлении операторной

суммой, получающейся из этой физически понятной картины, заключает в себе всю суть свободы, доступной в данном представлении операторной суммой, что доказывается следующей теоремой.

Теорема 8.2 (унитарная неопределенность представления операторной суммой). Предположим, $\{E_1, \dots, E_m\}$ и $\{F_1, \dots, F_n\}$ — элементы преобразований для \mathcal{E} и \mathcal{F} соответственно. Добавив нулевые операторы к более короткому списку элементов преобразования, можно достичь равенства $m = n$. Причем $\mathcal{E} = \mathcal{F}$ тогда и только тогда, когда существуют такие комплексные числа u_{ij} , что $E_i = \sum_j u_{ij} F_j$, а u_{ij} — элементы унитарной матрицы размера $m \times m$.

Доказательство.

Ключ к доказательству содержится в теореме 2.6. Согласно последней, два набора векторов $|\psi_i\rangle$ и $|\psi_j\rangle$ генерируют одинаковые операторы только в том случае, если

$$|\psi_i\rangle = \sum_j u_{ij} |\varphi_j\rangle, \quad (8.74)$$

где u_{ij} — унитарная матрица из комплексных чисел, и мы заполним меньший набор состояний $|\psi_i\rangle$ или $|\psi_j\rangle$ нулевыми состояниями так, чтобы в этих двух множествах было одинаковое количество элементов. Этот результат позволяет охарактеризовать свободу в выборе представления операторной суммой. Положим, $\{E_i\}$ и $\{F_i\}$ — два набора элементов одного и того же квантового преобразования и $\sum_i E_i \rho E_i^\dagger = \sum_j F_j \rho F_j^\dagger$ для любого ρ . Введем следующие определения:

$$|e_i\rangle \equiv \sum_k |k_R\rangle (E_i |k_Q\rangle), \quad (8.75)$$

$$|f_j\rangle \equiv \sum_k |k_R\rangle (F_j |k_Q\rangle). \quad (8.76)$$

Из определения σ (уравнение (8.55)), следует, что $\sigma = \sum_i |e_i\rangle \langle e_i| = \sum_i |f_i\rangle \langle f_i|$, а значит, существует унитарная матрица u_{ij} , так что

$$|e_i\rangle = \sum_j u_{ij} |f_j\rangle. \quad (8.77)$$

Но для произвольного $|\psi\rangle$ имеем

$$E_i |\psi\rangle = \langle \tilde{\psi} | e_i \rangle \quad (8.78)$$

$$= \sum_j u_{ij} \langle \tilde{\psi} | f_j \rangle \quad (8.79)$$

$$= \sum_k u_{ij} F_j |\psi\rangle. \quad (8.80)$$

Следовательно, можно написать

$$E_i = \sum_j u_{ij} F_j. \quad (8.81)$$

И наоборот, предположим, что E_i и F_i связаны унитарным преобразованием вида $E_i = \sum_j u_{ij} F_j$. Простые выкладки показывают, что квантовое преобразование с элементами $\{E_i\}$ совпадает с преобразованием с элементами $\{F_j\}$. Теорема доказана. ■

Теорему 8.2 можно использовать для ответа на другой интересный вопрос: какой максимальный размер среды может потребоваться, чтобы обеспечить данное квантовое преобразование?

Теорема 8.3. Любое квантовое преобразование \mathcal{E} системы с гильбертовым пространством размерности d можно представить операторной суммой, содержащей самое большое d^2 элементов,

$$\mathcal{E} = \sum_{k=1}^M E_k \rho E_k^\dagger, \quad (8.82)$$

где $1 \leq M \leq d^2$.

Эта теорема имеет простое доказательство, мы предоставим читателю возможность сделать это самостоятельно.

Упражнение 8.10. Докажите теорему 8.3, используя неопределенность представления операторной суммой. Пусть $\{E_j\}$ — множество элементов преобразования \mathcal{E} . Определим матрицу как $W_{jk} \equiv \text{tr}(E_j^\dagger E_k)$. Покажите, что эта матрица эрмитова и ее ранг не превышает d^2 , а следовательно, существует унитарная матрица u , такая что $u W u^\dagger$ диагональна и содержит самое большое d^2 ненулевых элементов. Используйте u , чтобы определить для \mathcal{E} новый набор из $\leq d^2$ ненулевых элементов преобразования $\{F_j\}$.

Упражнение 8.11. Предположим, \mathcal{E} — квантовое преобразование, отображающее d -мерное пространство ввода в d' -мерное пространство вывода. Покажите, что \mathcal{E} может быть описано при помощи dd' элементов преобразования $\{E_k\}$.

Такая неопределенность в представлении операторной суммой удивительно полезна. Мы будем ее использовать, например, при изучении квантовой коррекции ошибок (гл. 10). Мы увидим, что определенные наборы операторов в представлении операторной суммой позволяют получить более полезную информацию о квантовых процессах коррекции ошибок, и нам надлежит исследовать эту проблему. Как обычно, наличие нескольких способов понимания процесса дает возможность более глубоко заглянуть в суть происходящего.

8.3 Примеры квантового шума и квантовых преобразований

В данном разделе мы рассмотрим некоторые конкретные примеры квантового шума и квантовых преобразований. Они иллюстрируют мощь разрабатываемого нами формализма. Они также важны для понимания практических следствий шума в квантовых системах и того, как можно контролировать шум при помощи таких методик как исправление ошибок.

Начнем (подразд. 8.3.1) с обсуждения того, как можно описать измерение квантовым преобразованием и, в частности, рассмотрим преобразования, соответствующие взятию следа и частичного следа. Затем мы перейдем к описанию шума, начиная с демонстрации графического метода для квантовых преобразований на отдельном кубите. Этот метод используется в оставшейся части раздела для иллюстрации элементарных процессов классической ошибки и переворота фазы (подразд. 8.3.3), а также для обсуждения деполяризующего канала (подразд. 8.3.4), затухания амплитуды (подразд. 8.3.5) и затухания фазы (подразд. 8.3.6). Затухание амплитуды и фазы — это идеализированные модели шума, которые заключают в себе многие из наиболее важных особенностей шумов, происходящих в квантовомеханических системах, и мы рассмотрим не только их абстрактную математическую формулировку, но и появление этих процессов в реальных квантовых системах.

8.3.1 След и частичный след

Одно из основных применений формализма квантовых преобразований — описание измерения. Квантовое преобразование можно использовать для описания как вероятности получить некоторый конкретный результат измерения над квантовой системой, так и изменения состояния системы, связанного с измерением.

Простейшим преобразованием, связанным с измерением, является взятие следа $\rho \rightarrow \text{tr}(\rho)$; можно показать, что оно является квантовым преобразованием, следующим образом. Пусть H_Q — некоторое исходное гильбертово пространство с ортонормированным базисом $|1\rangle \dots |d\rangle$, а H'_Q — одномерное результирующее пространство с базисным вектором $|0\rangle$. Определим $\mathcal{E}(\rho)$ как

$$\mathcal{E}(\rho) \equiv \sum_{i=1}^d |0\rangle\langle i|\rho|i\rangle\langle 0|, \quad (8.83)$$

т.е. \mathcal{E} — квантовое преобразование согласно теореме 8.1. Заметим, что $\mathcal{E}(\rho) = \text{tr}(\rho)|0\rangle\langle 0|$, поэтому с точностью до несущественного множителя $|0\rangle\langle 0|$, квантовое преобразование совпадает со следом.

Еще более полезным результатом является то, что взятие частичного следа — тоже квантовое преобразование. Предположим, имеется объединенная система QR , и мы хотим взять след по системе R . Пусть $|j\rangle$ — базис системы R . Зададим линейный оператор $E_i : H_{QR} \rightarrow H_Q$ соотношением

$$E_i \left(\sum_j \lambda_j |q_j\rangle |j\rangle \right) \equiv \lambda_i |q_i\rangle, \quad (8.84)$$

где λ_j — комплексные числа, а $|q_j\rangle$ — произвольные состояния системы Q . Определим \mathcal{E} как квантовое преобразование с элементами $\{E_i\}$, т. е.

$$\mathcal{E}(\rho) \equiv \sum_i E_i \rho E_i^\dagger. \quad (8.85)$$

В соответствии с 8.1, это — квантовое преобразование из системы QR в систему Q . Заметим, что

$$\mathcal{E}(\rho \otimes |j\rangle\langle j'|) = \rho \delta_{j,j'} = \text{tr}_R(\rho \otimes |j\rangle\langle j'|), \quad (8.86)$$

где ρ — любой эрмитов оператор на пространстве состояний системы Q , а $|j\rangle$ и $|j'\rangle$ — векторы, принадлежащие ортонормированному базису системы R . Из линейности \mathcal{E} и tr_R следует, что $\mathcal{E} = \text{tr}_R$.

8.3.2 Геометрическая картина квантового преобразования одного кубита

Существует элегантный геометрический метод для изображения квантовых преобразований одного кубита. Этот метод позволяет достичь интуитивного понимания поведения квантовых преобразований в терминах действия, производимого ими на сфере Блоха. Обратимся к упр. 2.27, где было показано, что состояние отдельного кубита всегда может быть записано в представлении Блоха:

$$\rho = \frac{I + \vec{r} \cdot \vec{\sigma}}{2}, \quad (8.87)$$

где \vec{r} — трехкомпонентный действительный вектор. В явном виде получим

$$\rho = \frac{1}{2} \begin{bmatrix} 1 + r_z & r_x - ir_y \\ r_x + ir_y & 1 - r_z \end{bmatrix}. \quad (8.88)$$

В таком представлении оказывается, что произвольное, сохраняющее след квантовое преобразование эквивалентно отображению вида

$$\vec{r} \xrightarrow{\mathcal{E}} \vec{r}' = M\vec{r} + \vec{c}, \quad (8.89)$$

где M — действительная матрица 3×3 , а \vec{c} — постоянный вектор. Это *аффинное отображение*, переводящее сферу Блоха в себя. Чтобы в этом убедиться, предположим, что операторы E_i , генерирующие представление \mathcal{E} операторной суммой, имеют вид

$$E_i = \alpha_i I + \sum_{k=1}^3 a_{ik} \sigma_k. \quad (8.90)$$

Тогда несложно проверить, что

$$M_{jk} = \sum_l \left[a_{lj} a_{lk}^* + a_{lj}^* a_{lk} \left(|\alpha_l|^2 - \sum_p a_{lp} a_{lp}^* \right) \delta_{jk} + i \sum_p \varepsilon_{jpk} (\alpha_l a_{lp}^* - \alpha_l^* a_{lp}) \right] \quad (8.91)$$

$$c_k = 2i \sum_l \sum_{jp} \varepsilon_{jpk} a_{lj} a_{lp}^*, \quad (8.92)$$

здесь использовалось соотношение полноты $\sum_i E_i^+ E_i = I$ для упрощения выражения для \tilde{c} .

Смысъ аффинного отображения, задаваемого уравнением (8.89), станет яснее, если рассмотреть полярное разложение матрицы $M = U|M|$, где U унитарная матрица. Из того, что M действительна, следует, что $|M|$ действительна и эрмитова, т.е. $|M|$ — симметрическая матрица. Далее, так как M действительна, можно считать, что U также действительна и, таким образом, является ортогональной матрицей: $U^T U = I$, где T обозначает операцию транспонирования. Следовательно, можно записать

$$M = OS, \quad (8.93)$$

где O — действительная ортогональная матрица с детерминантом 1, представляющая собственное вращение, а S — действительная симметрическая матрица. Тогда уравнение (8.89) — это просто последовательные выполнения деформации сферы Блоха вдоль главных осей, определяемой S , собственного вращения, связанного с O , и перемещения, обусловленного \tilde{c} .

Упражнение 8.12. Почему можно считать, что в разложении (8.93) детерминант O равен 1?

Упражнение 8.13. Покажите, что унитарные преобразования соответствуют вращению сферы Блоха.

Упражнение 8.14. Покажите, что $\det(S)$ не обязательно положительный.

8.3.3 Каналы с классической ошибкой и переворотом фазы .

Описанную выше геометрическую картину можно использовать для визуализации некоторых важных квантовых преобразований отдельных кубитов, которые нам понадобятся ниже для теории исправления ошибок. Канал с *классической ошибкой* переворачивает состояние кубита из $|0\rangle$ в $|1\rangle$ (и наоборот) с вероятностью $(1 - p)$. Элементы этого преобразования следующие:

$$E_0 = \sqrt{p}I = \sqrt{p} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad E_1\sqrt{1-p}X = \sqrt{1-p} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \quad (8.94)$$

Действие канала с классической ошибкой проиллюстрировано на рис. 8.8.

При помощи геометрической картины очень просто проверить известные факты об этом квантовом преобразовании. Например, легко убедиться, что величина $\text{tr}(\rho^2)$ для отдельного кубита равна $(1 + |r|^2)/2$, где $|r|$ — норма блоховского вектора. Сжатие сферы Блоха, проиллюстрированное на рис. 8.8, не может увеличить нормы блоховского вектора, и, таким образом, мы сразу же делаем вывод, что для канала с классической ошибкой $\text{tr}(\rho^2)$ может только уменьшиться. Это — не единственный пример применения геометрической картины. Как только она станет достаточно привычной, ею можно пользоваться для лучшего понимания свойств квантовых преобразований отдельного кубита.

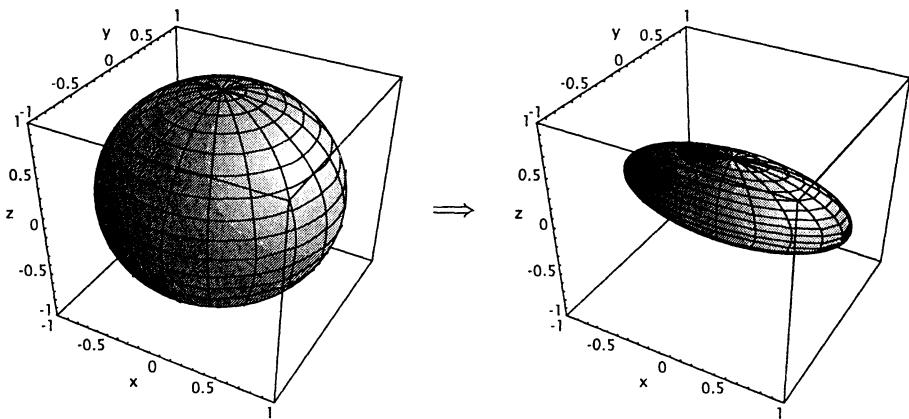


Рис. 8.8. Действие канала с классической ошибкой на блоховской сфере при $p = 0,3$. Сфера слева соответствует набору всех чистых состояний, а деформированная сфера справа — состояниям после прохождения через канал. Обратите внимание на то, что состояния на оси \hat{x} не изменяются, тогда как плоскость $(\hat{y} - \hat{z})$ равномерно сжимается в $(1 - 2p)$ раз

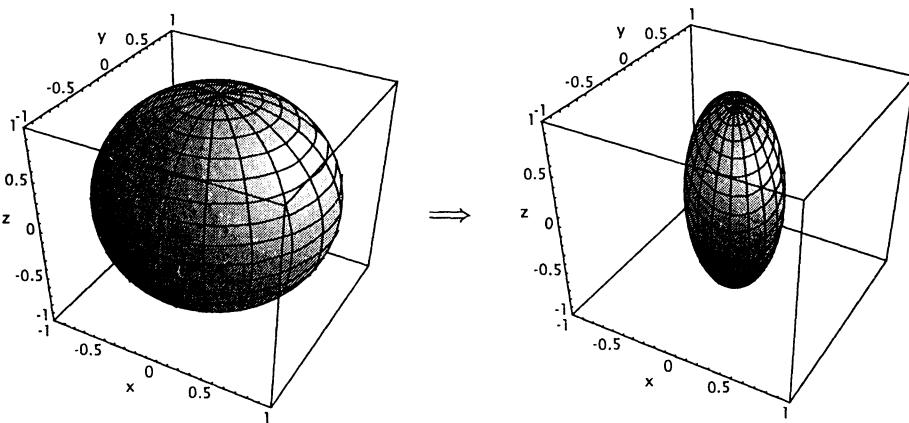


Рис. 8.9. Действие канала с переворотом фазы на блоховской сфере при $p = 0,3$. Обратите внимание на то, что состояния на оси \hat{z} не изменяются, тогда как плоскость $\hat{x} - \hat{y}$ равномерно сжимается в $(1 - 2p)$ раз.

У канала с переворотом фазы следующие элементы преобразования:

$$E_0 = \sqrt{p}I = \sqrt{p} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad E_1 = \sqrt{1-p}Z = \sqrt{1-p} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \quad (8.95)$$

Действие канала с переворотом фазы проиллюстрировано на рис. 8.9. В качестве частного случая канала с переворотом фазы рассмотрим квантовое преобразование, возникающее при $p = 1/2$. Используя произвол в представлении операторной суммой, это преобразование можно записать в виде

$$\rho \rightarrow \mathcal{E}(\rho) = P_0\rho P_0 + P_1\rho P_1, \quad (8.96)$$

где $P_0 = |0\rangle\langle 0|$ и $P_1 = |1\rangle\langle 1|$ соответствуют измерению кубита в базисе $\{|0\rangle, |1\rangle\}$ с неизвестным результатом измерения. При помощи приведенного алгоритма легко показать, что соответствующее отображение на сфере Блоха имеет вид

$$(r_x, r_y, r_z) \rightarrow (0, 0, r_z). \quad (8.97)$$

Геометрически блоховский вектор проецируется на ось \hat{z} , а его \hat{x} и \hat{y} компоненты теряются.

Канал с *фазовой ошибкой* имеет следующие элементы преобразования:

$$E_0 = \sqrt{p}I = \sqrt{p} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad E_1 = \sqrt{1-p}Y = \sqrt{1-p} \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}. \quad (8.98)$$

Это — комбинация переворота фазы и классической ошибки, так как $Y = iXZ$. Действие канала с фазовой ошибкой показано на рис. 8.10.

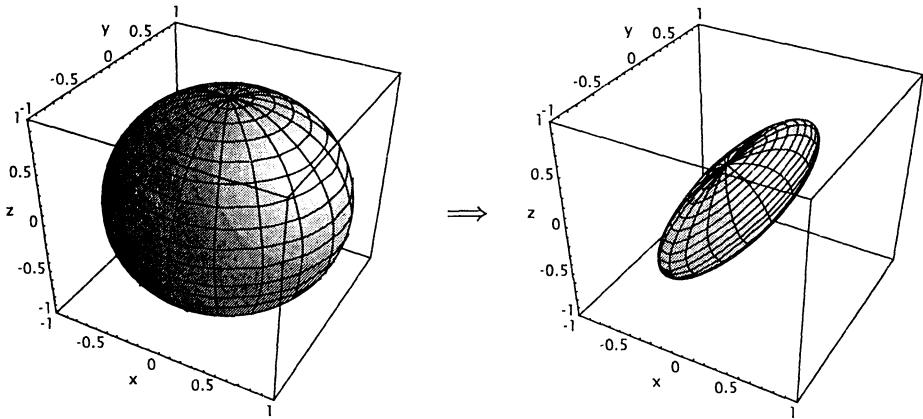


Рис. 8.10. Действие канала с фазовой ошибкой на блоховской сфере при $p = 0,3$. Обратите внимание, что состояния на оси \hat{y} не изменяются, в то время как плоскость $(\hat{x} - \hat{z})$ равномерно сжимается в $(1 - 2p)$ раз.

Упражнение 8.15. Предположим, что над отдельным кубитом производится проективное измерение в базисе $|+\rangle, |-\rangle$, где $|\pm\rangle \equiv (|0\rangle \pm |1\rangle)/\sqrt{2}$. В случае, если результат измерения не известен, матрица плотности эволюционирует в соответствии с уравнением

$$\rho \rightarrow \mathcal{E}(\rho) = |+\rangle\langle +| \rho |+\rangle\langle +| + |-\rangle\langle -| \rho |-\rangle\langle -. \quad (8.99)$$

Проиллюстрируйте это преобразование на сфере Блоха.

Упражнение 8.16. Графическая интерпретация квантовых преобразований одного кубита была выведена для преобразований, сохраняющих след. Найдите в явном виде пример не сохраняющего след квантового преобразования, которое невозможно описать как последовательные деформацию, вращение и смещение блоховской сферы.

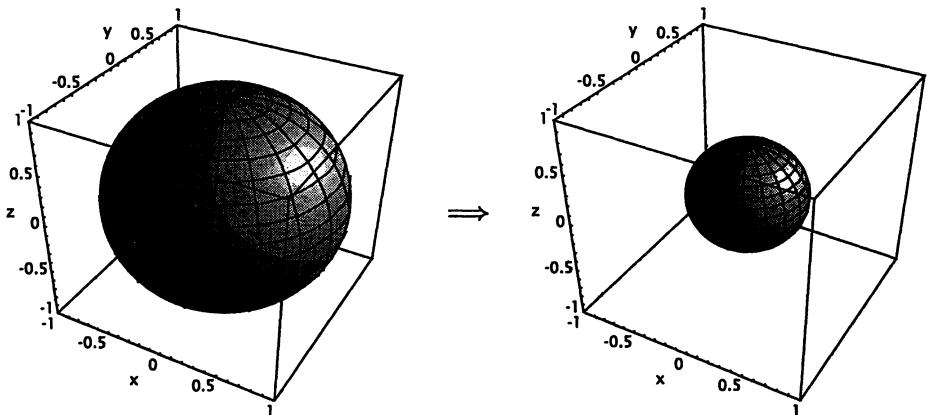


Рис. 8.11. Действие деполяризующего канала на блоховской сфере для $p = 0,5$. Обратите внимание на то, что вся сфера равномерно сжимается как функция p

8.3.4 Деполяризующий канал

Деполяризующий канал является важным примером квантового шума. Представьте, что мы берем отдельный кубит и с вероятностью p этот кубит **деполяризуется**. Т.е. он заменяется на полностью смешанное состояние $I/2$. С вероятностью $(1 - p)$ кубит остается неизменным. Состояние квантовой системы после воздействия такого шума имеет вид

$$\mathcal{E}(\rho) = \frac{pI}{2} + (1 - p)\rho. \quad (8.100)$$

Действие деполяризующего канала на блоховской сфере изображено на рис. 8.11.

Квантовая схема, моделирующая действие деполяризующего канала, показана на рис. 8.12. Верхняя линия схемы — это вход деполяризующего канала, а две нижние являются «средой» для моделируемого канала. Мы используем среду с двумя входами в смешанном состоянии. Идея заключается в том, что третий кубит, находившийся в начальный момент времени в состоянии $|0\rangle$ с вероятностью $(1 - p)$ и в состоянии $|1\rangle$ с вероятностью p , действует как переключатель: от него зависит, поменяются или нет местами полностью смешанное состояние $I/2$, хранимое во втором кубите, и содержимое первого кубита.

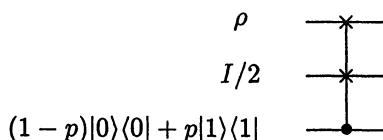


Рис. 8.12. Схема, моделирующая деполяризующий канал.

Выражение (8.100) не имеет вида операторной суммы. Заметим, что для любого ρ справедливо уравнение

$$\frac{I}{2} = \frac{\rho + X\rho X + Y\rho Y + Z\rho Z}{4} \quad (8.101)$$

и, тогда подставив $I/2$ в (8.100), получим уравнение

$$\mathcal{E}(\rho) = \left(1 - \frac{3p}{4}\right)\rho + \frac{p}{4}(X\rho X + Y\rho Y + Z\rho Z), \quad (8.102)$$

показывающее, что элементы преобразования деполяризующего канала есть $\{\sqrt{1-3p}/4I, \sqrt{p}X/2, \sqrt{p}Y/2, \sqrt{p}Z/2\}$. Укажем в этой связи, что часто бывает удобно параметризовать деполяризующий канал по-другому, например:

$$\mathcal{E}(\rho) = (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z), \quad (8.103)$$

т.е. состояние ρ не меняется с вероятностью $(1-p)$, а каждое преобразование X, Y или Z происходит с вероятностью $p/3$.

Упражнение 8.17. Проверьте (8.101) следующим образом. Определив

$$\mathcal{E}(A) \equiv \frac{A + XAX + YAY + ZAZ}{4}, \quad (8.104)$$

покажите, что

$$\mathcal{E}(I) = I; \quad \mathcal{E}(X) = \mathcal{E}(Y) = \mathcal{E}(Z) = 0. \quad (8.105)$$

Теперь используйте представление на сфере Блоха для матриц плотности отдельного кубита для проверки уравнения (8.101).

Деполяризующий канал можно, конечно, обобщить на квантовые системы с размерностью большей, чем 2. Для d -мерной квантовой системы деполяризующий канал снова заменяет состояние на полностью смешанное состояние I/d с вероятностью p и оставляет его неизменным в противном случае. Соответствующее квантовое преобразование выглядит как

$$\mathcal{E}(\rho) = \frac{pI}{d} + (1-p)\rho. \quad (8.106)$$

Упражнение 8.18. Для $k \geq 1$ покажите, что $\text{tr}(\rho^k)$ не может увеличиться от действия деполяризующего канала.

Упражнение 8.19. Найдите представление операторной суммой для обобщенного деполяризующего канала, действующего в d -мерном гильбертовом пространстве.

8.3.5 Затухание амплитуды

Важным приложением квантовых преобразований является описание *диссипации энергии* — явления, связанного с потерями энергии в квантовых системах.

Как изменяется состояние атома, который спонтанно излучает фотон? Каким образом спиновая система достигает равновесия с окружающей средой при высокой температуре? Каково состояние фотона в интерферометре или резонаторе при наличии рассеяния и затухания?

Каждый из этих процессов обладает своими особенностями, но их общее поведение хорошо описывается квантовым преобразованием, известным как **затухание амплитуды**, которое мы можем получить, если рассмотрим следующий сценарий. Предположим, имеется одна оптическая мода в квантовом состоянии $a|0\rangle + b|1\rangle$ — суперпозиция нуля и одного фотона. Рассеяние фотона из этой моды можно представить как результат действия поставленного на пути фотона полупрозрачного зеркала — светофильтра. Как было показано в подразд. 7.4.2, такой светофильтр приводит к тому, что фотон взаимодействует с другой оптической модой (представляющей среду) в соответствии с унитарным преобразованием $B = \exp[\theta(a^+b - ab^+)]$, где a, a^+ и b, b^+ — операторы рождения и уничтожения фотонов в этих двух модах. Состояние системы после светофильтра в предположении, что среда не содержала вначале фотонов, можно представить как $B|0\rangle(a|0\rangle + b|1\rangle) = a|0\rangle + b(\cos\theta|01\rangle + \sin\theta|10\rangle)$ в соответствии с (7.34). Взяв след по окружающей среде, получим квантовое преобразование

$$\mathcal{E}_{AD}(\rho) = E_0\rho E_0 + E_1\rho E_1, \quad (8.107)$$

где $E_k = \langle k|b|0\rangle$ имеют вид

$$E_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix}, \quad E_1 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix}. \quad (8.108)$$

Это — элементы преобразования «затухание амплитуды», причем $\gamma = \sin^2\theta$ можно считать вероятностью испускания фотона.

Обратите внимание на то, что невозможно создать линейную комбинацию E_0 и E_1 , приводящую к элементу преобразования, пропорциональному единичному (сравните с упр. 8.23). Преобразование E_1 заменяет состояние $|1\rangle$ на $|0\rangle$, что соответствует физическому процессу излучения системой кванта энергии в среду. Преобразование E_0 оставляет состояние $|0\rangle$ неизменным, но уменьшает амплитуду состояния $|1\rangle$. С физической точки зрения это происходит потому, что среда не получила квант энергии, так что среде теперь «кажется», что система находится в состоянии $|0\rangle$, а не $|1\rangle$.

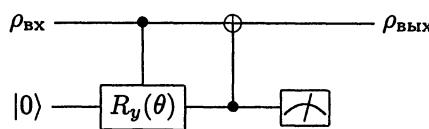


Рис. 8.13. Схема, моделирующая затухание амплитуды

Упражнение 8.20 (схема, моделирующая затухание амплитуды). Покажите, что схема, изображенная на рис. 8.13, моделирует квантовое преобразование «затухание амплитуды» при $\sin^2(\theta/2) = \gamma$.

Упражнение 8.21 (затухание амплитуды гармонического осциллятора). Предположим, что наша основная система — гармонический осциллятор — взаимодействует со средой, моделируемой другим гармоническим осциллятором посредством гамильтониана

$$H = \chi(a^\dagger b + b^\dagger a), \quad (8.109)$$

где a и b — операторы уничтожения для соответствующих гармонических осцилляторов в соответствии с определениями в разд. 7.3.

- Пусть $U = \exp(-iH\Delta t)$. Обозначим собственные состояния $b^\dagger b$ как $|k_b\rangle$ и выберем вакуумное состояние $|0_b\rangle$ в качестве начального состояния среды. Покажите, что элементы преобразования $E_k = \langle k_b|U|0_b\rangle$ имеют вид

$$E_k = \sum_n \sqrt{\binom{n}{k}} \sqrt{(1-\gamma)^{n-k}\gamma^k} |n-k\rangle\langle n|, \quad (8.110)$$

где $\gamma = 1 - \cos^2(\chi\Delta t)$ — вероятность потери одного кванта энергии, а состояния $|n\rangle$ — собственные для $a^\dagger a$.

- Покажите, что элементы E_k определяют сохраняющее след квантовое преобразование.

Упражнение 8.22 (затухание амплитуды для матрицы плотности отдельного кубита). Для состояния общего вида отдельного кубита

$$\rho = \begin{bmatrix} a & b \\ b^* & c \end{bmatrix} \quad (8.111)$$

покажите, что затухание амплитуды приводит к состоянию

$$\mathcal{E}_{AD}(\rho) = \begin{bmatrix} 1 - (1-\gamma)(1-a) & b\sqrt{1-\gamma} \\ b^*\sqrt{1-\gamma} & c(1-\gamma) \end{bmatrix}. \quad (8.112)$$

Упражнение 8.23 (затухание амплитуды для кубитов в двойственном представлении). Предположим, состояние отдельного кубита представлено при помощи двух кубитов в виде

$$|\psi\rangle = a|01\rangle + b|10\rangle. \quad (8.113)$$

Покажите, что преобразование $\mathcal{E}_{AD} \otimes \mathcal{E}_{AD}$, будучи примененным к такому состоянию, задает процесс, который можно описать элементами преобразования

$$E_0^{\text{dr}} = \sqrt{1-\gamma}I, \quad (8.114)$$

$$E_1^{\text{dr}} = \sqrt{\gamma} [|00\rangle\langle 01| + |00\rangle\langle 10|], \quad (8.115)$$

т. е. с кубитом либо ничего (E_0^{dr}) не происходит, либо он преобразуется (E_1^{dr}) в состояние $|00\rangle$, ортогональное $|\psi\rangle$. Это — простой код обнаружения ошибок, а также *основа надежности* кубита в двойственном представлении, которая обсуждалась в разд. 7.4.

Упражнение 8.24 (спонтанное излучение как затухание амплитуды). Одиночный атом, взаимодействующий с одной модой электромагнитного излучения, способен к спонтанному излучению (см.подразд. 7.6.1). Чтобы убедиться в том, что этот процесс — просто затухание амплитуды, возьмите унитарное преобразование, получаемое из взаимодействия Джейнса–Каммингса (уравнение 7.77), при расстройке $\delta = 0$ и выведите квантовое преобразование, взяв след по полю.

Общей характеристикой квантового преобразования является набор состояний, остающихся инвариантными при этом преобразовании. Например, мы видели, что в случае канала с переворотом фазы сохраняется неизменной ось \hat{z} на сфере Блоха; она соответствует состояниям вида $p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1|$ для произвольной вероятности p . В случае затухания амплитуды остается инвариантным только основное состояние $|0\rangle$. Это — естественное следствие предположения, что начальное состояние среды $|0\rangle$, как если бы она была при нулевой температуре.

Какие квантовые преобразования описывают эффект диссипации в среде при конечной температуре? Этот процесс \mathcal{E}_{GAD} , называемый *обобщенное затухание амплитуды*, определяется для отдельного кубита следующими элементами преобразования:

$$E_0 = \sqrt{p} \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix}, \quad (8.116)$$

$$E_1 = \sqrt{p} \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix}, \quad (8.117)$$

$$E_2 = \sqrt{1-p} \begin{bmatrix} \sqrt{1-\gamma} & 0 \\ 0 & 1 \end{bmatrix}, \quad (8.118)$$

$$E_3 = \sqrt{1-p} \begin{bmatrix} 0 & 0 \\ \sqrt{\gamma} & 0 \end{bmatrix}, \quad (8.119)$$

при этом стационарное состояние, удовлетворяющее условию $\mathcal{E}_{\text{GAD}}(\rho_{\infty}) = \rho_{\infty}$, имеет вид

$$\rho_{\infty} = \begin{bmatrix} p & 0 \\ 0 & 1-p \end{bmatrix}. \quad (8.120)$$

Обобщенное затухание амплитуды описывает процесс T_1 -релаксации, вызываемый взаимодействием спинов с окружающей их решеткой — большой системой, находящейся в тепловом равновесии, часто при температуре гораздо более высокой, чем спиновая. Эта ситуация актуальна для ЯМР-квантовых вычисле-

ний, где становятся важными некоторые свойства \mathcal{E}_{GAD} , описанные во вставке 8.3.

Вставка 8.3. Обобщенное затухание амплитуды и эффективно чистые состояния

Понятие об «эффективно чистых состояниях», введенное в разд. 7.7, оказалось полезным в ЯМР-реализациях квантовых компьютеров. Эти состояния ведут себя как чистые под действием унитарной эволюции и измерений бесследовых наблюдаемых. Как они проявлят себя под действием квантовых преобразований? Вообще говоря, эффективность этих состояний разрушается неунитарными преобразованиями матриц плотности, но удивительным образом такие состояния могут «правильно» вести себя при обобщенном затухании амплитуды.

Рассмотрим эффективно чистое состояние отдельного кубита $\rho = (1-p)I + (2p-1)|0\rangle\langle 0|$. Очевидно, измерение бесследовой наблюдаемой, произведенное над $U\rho U^\dagger$ приводит к результату, пропорциональному получающемуся при измерении в чистом состоянии $U|0\rangle\langle 0|U^\dagger$. Предположим, ρ — стационарное состояние \mathcal{E}_{GAD} . Интересно, что в этом случае имеем

$$\mathcal{E}_{GAD}(U\rho U^\dagger) = (1-p)I + (2p-1)\mathcal{E}_{AD}(U\rho U^\dagger). \quad (8.121)$$

Таким образом при обобщенном затухании амплитуды эффективно чистое состояние может оставаться таким и, более того, «чистая» часть ρ ведет себя так, как если бы она испытывала затухание амплитуды из-за резервуара с нулевой температурой!

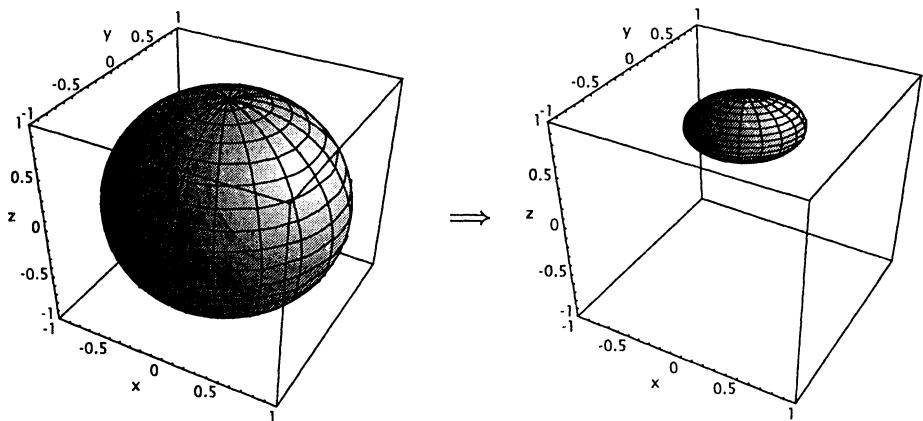


Рис. 8.14. Действие канала с затуханием амплитуды на блоховской сфере при $p = 0,8$. Обратите внимание на то, что вся сфера сжимается к северному полюсу — состоянию $|0\rangle$.

Упражнение 8.25. Если определена температура T кубита в предположении, что при равновесии вероятности находжения в состояниях $|0\rangle$ и $|1\rangle$ удовле-

творяют распределению Больцмана, т. е. $p_0 = e^{-E_0/k_B T}/Z$ и $p_1 = e^{-E_1/k_B T}/Z$, где E_0 и E_1 — соответственно, энергия состояния $|0\rangle$ и $|1\rangle$, а $Z = e^{-E_0/k_B T} + e^{-E_1/k_B T}$, то какая температура соответствует состоянию ρ_∞ ?

Можно визуализировать эффект затухания амплитуды в блоховском представлении как преобразование вектора Блоха

$$(r_x, r_y, r_z) \rightarrow \left(r_x \sqrt{1 - \gamma}, r_y \sqrt{1 - \gamma}, \gamma + r_z(1 - \gamma) \right). \quad (8.122)$$

Если γ заменить зависящей от времени функцией типа $1 - e^{-t/T_1}$ (здесь t — время, а T_1 — некоторая константа, характеризующая скорость процесса), как обычно происходит в реальных физических процессах, то мысленно можно представить результат затухания амплитуды как *поток* на сфере Блоха, который перемещает каждую точку единичного шара в сторону фиксированной точки на северном полюсе где находится состояние $|0\rangle$ (рис. 8.14).

Аналогично обобщенное затухание амплитуды приводит к преобразованию

$$(r_x, r_y, r_z) \rightarrow \left(r_x \sqrt{1 - \gamma}, r_y \sqrt{1 - \gamma}, \gamma(2p - 1) + r_z(1 - \gamma) \right). \quad (8.123)$$

Сравнив (8.122) и (8.123), становится очевидно, что обычное затухание амплитуды и обобщенное затухание амплитуды отличаются только положением фиксированной точки потока; конечное состояние находится на оси \hat{z} в точке $(2p - 1)$, которая соответствует смешанному состоянию.

8.3.6 Затухание фазы

Затухание фазы — это чисто квантовомеханический процесс шума, который описывает потерю квантовой информации без потери энергии. Физически он описывает, например, процесс, при котором фотон случайным образом рассеивается при распространении по волноводу, или когда электронные состояния в атоме испытывают возмущение вследствие взаимодействия с удаленными электрическими зарядами. Собственные состояния энергии квантовой системы не меняются со временем, но они накапливают фазу, пропорциональную собственному значению. Когда система эволюционирует в течение некоторого точно не известного промежутка времени, часть информации о квантовой фазе — *относительная фаза* между собственными состояниями энергии — теряется.

Вот очень простая модель квантового шума такого типа. Предположим, имеется кубит $|\psi\rangle = a|0\rangle + b|1\rangle$, к которому применяется оператор вращения $R_z(\theta)$, причем угол вращения θ случаен. Случайность может быть следствием, например, детерминистического взаимодействия со средой, которая никогда больше не будет взаимодействовать с системой и, таким образом, неявно измеряется (см. разд. 4.4). Мы будем называть такое случайное воздействие R_z *сбоем фазы*. Предположим, что угол сбоя фазы θ хорошо описывается как случайное число с гауссовым распределением со средним значением 0 и дисперсией 2λ .

Конечное состояние в этом процессе задается матрицей плотности, получаемой усреднением по θ

$$\rho = \frac{1}{\sqrt{4\pi\lambda}} \int_{-\infty}^{+\infty} R_z(\theta) |\psi\rangle\langle\psi| R_z^\dagger(\theta) e^{-\theta^2/4\lambda} d\theta \quad (8.124)$$

$$= \begin{bmatrix} |a|^2 & ab^* e^{-\gamma} \\ a^* b e^{-\gamma} & |b|^2 \end{bmatrix}. \quad (8.125)$$

Случайный сбой фазы приводит к тому, что ожидаемое значение недиагональных элементов матрицы плотности экспоненциально затухает до нуля со временем. Это характеристическое свойство затухания фазы.

Другой способ вывести квантовое преобразование, соответствующее затуханию фазы, — рассмотреть взаимодействие между двумя гармоническими осцилляторами — аналогично тому, как выводилось затухание амплитуды в предыдущем подразделе, но, на этот раз, с гамильтонианом взаимодействия

$$H = \chi a^\dagger a (b + b^\dagger). \quad (8.126)$$

Обозначив $U = \exp(-iH\Delta t)$, рассматривая только состояния $|0\rangle$ и $|1\rangle$ осциллятора a в качестве нашей системы и, считая, что начальное состояние второго осциллятора (среды) — $|0\rangle$, можно видеть, что взятие следа по среде приводит к элементам преобразования $E_k = \langle k_b | U | 0 \rangle$, которые равны

$$E_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{bmatrix}, \quad (8.127)$$

$$E_1 = \begin{bmatrix} 0 & 0 \\ 0 & \sqrt{\lambda} \end{bmatrix}, \quad (8.128)$$

где $\lambda = 1 - \cos^2(\chi\Delta t)$ можно интерпретировать как вероятность того, что фотон был упруго рассеян средой. Как это было в случае затухания амплитуды, E_0 оставляет $|0\rangle$ неизменным, но уменьшает амплитуду состояния $|1\rangle$; тем не менее в отличие от затухания амплитуды, операция E_1 разрушает $|0\rangle$ и уменьшает амплитуду состояния $|1\rangle$, но не превращает его в $|0\rangle$.

Применив теорему 8.2 об унитарной неопределенности квантовых преобразований, можно видеть, что унитарная комбинация E_0 и E_1 приводит к новому набору элементов преобразования для затухания фазы:

$$\tilde{E}_0 = \sqrt{\alpha} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad (8.129)$$

$$\tilde{E}_1 = \sqrt{1-\alpha} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad (8.130)$$

где $\alpha = (1 + \sqrt{1-\lambda})/2$. Таким образом, квантовое преобразование, соответствующее затуханию фазы, *точно* совпадает с каналом с переворотом фазы, который мы встречали в подразд. 8.3.3!

Так как затухание фазы — то же самое, что канал с переворотом фазы, нам известно, как его отображать на блоховской сфере (см. рис. 8.9). Это соответствует преобразованию вектора Блоха

$$(r_x, r_y, r_z) \rightarrow \left(r_x \sqrt{1 - \lambda}, r_y \sqrt{1 - \lambda}, r_z \right), \quad (8.131)$$

которое приводит к сжатию сферы в эллипсоид. Затухание фазы часто называют « T_2 » (или «спин-спин»)-релаксацией по историческим причинам, где $e^{-t/2T_2} = \sqrt{1 - \lambda}$. Как функция времени, величина затухания увеличивается, что соответствует потоку всех точек единичного шара внутрь в направлении оси \hat{z} . Заметим, что состояния на оси \hat{z} остаются инвариантными.

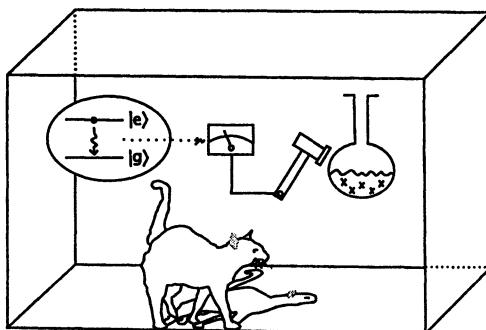
Исторически затухание фазы считалось процессом, физической причиной которого является случайный сбой фазы или рассеяние. Только после того, как обнаружилась его связь с каналом с переворотом фазы, была разработана квантовая коррекция таких ошибок, поскольку считалось, что фазовые ошибки непрерывны и их нельзя описывать дискретным образом. Фактически фазовые ошибки с одним кубитом можно всегда считать возникающими в результате процесса, в котором с кубитом либо ничего не происходит с вероятностью α , либо с вероятностью $(1 - \alpha)$ кубит переворачивается оператором Паули Z . Хотя истинный физический процесс может быть другим, для преобразования, происходящего с кубитом за промежуток времени, больший, чем характерное время случайного процесса, разницы нет никакой.

Вставка 8.4. Кот Шредингера

Когда я слышу о коте Шредингера, я хватаюсь за пистолет.

Стивен Хокинг.

Судьба печально известного кота Шредингера такова: его жизнь или смерть определяются автоматическим устройством, которое разбивает ампулу с ядом и убивает кота, если обнаруживается, что распалось возбужденное состояние атома (см. рисунок).



Шредингер задался вопросом: что произойдет, если атом находился в смешанном состоянии? Кот жив или мертв? Почему смешанные состояния, подобные упомянутому выше, не встречаются в повседневной жизни? Разгадка заключается в том, что такие состояния совершенно невероятны в реальном мире, поскольку макроскопические смешанные состояния очень чувствительны к потере когерентности. Пусть атом представляет отдельный кубит. Составная система вначале находится в состоянии $|\text{жив}\rangle|1\rangle$. Предположим, по истечении времени полураспада атома состояние будет равновероятной суперпозицией $|\text{жив}\rangle(|0\rangle + |1\rangle)/\sqrt{2}$ (это упрощение реальной физической картины, которая слишком сложна, чтобы в нее здесь углубляться). Установка убивает кота, если атом оказывается в состоянии $|0\rangle$; в противном случае кот остается живым. Это приводит к состоянию $|\psi\rangle = [|\text{мертв}\rangle|0\rangle + |\text{жив}\rangle|1\rangle]/\sqrt{2}$, в котором состояние кот оказывается запутанным с состоянием атомом. Казалось бы, это означает, что кот одновременно и жив и мертв, однако давайте рассмотрим матрицу плотности этого состояния

$$\rho = |\psi\rangle\langle\psi| \quad (8.132)$$

$$\begin{aligned} &= \frac{1}{2} \left[|\text{жив}, 1\rangle\langle\text{жив}, 1| + |\text{мертв}, 0\rangle\langle\text{мертв}, 0| \right. \\ &\quad \left. + |\text{жив}, 1\rangle\langle\text{мертв}, 0| + |\text{мертв}, 0\rangle\langle\text{жив}, 1| \right]. \end{aligned} \quad (8.133)$$

На практике невозможно полностью изолировать кота и атом в их ящике, и, таким образом, информация о смешанном состоянии будет просачиваться во внешний мир. Например, тепло тела кота может пройти сквозь стенки и явиться некоторым показателем его состояния. Такие эффекты можно смоделировать как затухание фазы, которое экспоненциально подавляет последние два (недиагональных) члена в ρ . В первом приближении, можно смоделировать систему кот — атом как простой гармонический осциллятор. Важный результат, касающийся потери когерентности такой системой, заключается в том, что когерентность между состояниями с большой разностью энергий теряется быстрее, чем между состояниями с меньшей разностью (упр. 8.31). Таким образом, ρ быстро перейдет в практически диагональное состояние, которое соответствует ансамблю состояний кот — атом, представляющих или живого, или мертвого кота, а не суперпозицию этих двух состояний.

Затухание фазы — один из наиболее тонких и важных процессов при исследовании квантовых вычислений и квантовой информации. Он стал предметом обширных изысканий и обсуждений, особенно в связи с тем, что мир вокруг нас представляется классическим и смешанные состояния не встречаются в нашей повседневной жизни. Именно затухание фазы ответственно за это отсутствие смешанных состояний в больших системах (упражнение 8.31). Пионер кванто-

вой механики Шредингер был, по-видимому, первым, кто сформулировал эту проблему, и сделал это в особенно острой форме (см. вставку 8.4).

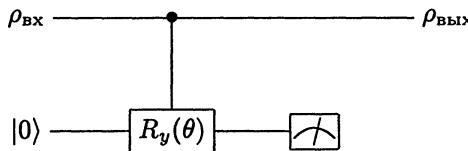


Рис. 8.15. Модельная схема для затухания фазы. По верхнему проводу идет входной бит в неизвестном состоянии, а по нижнему — вспомогательный кубит, используемый для моделирования среды.

Упражнение 8.26 (схема, моделирующая затухание фазы). Покажите, что схема, приведенная на рис. 8.15, может моделировать квантовое преобразование «затухание фазы», если правильно выбрать θ .

Упражнение 8.27 (затухание фазы — канал с переворотом фазы). Запишите унитарное преобразование, связывающее элементы преобразования (8.127)–(8.128) с элементами (8.129)–(8.130), т. е. найдите u такое, что и $\tilde{E}_k = \sum_j u_{ij} E_j$.

Упражнение 8.28 (модель схемы затухания фазы на одном элементе CNOT). Покажите, что один элемент CNOT может быть использован как модель для затухания фазы, если начальное состояние среды смешанное, причем величина затухания будет определяться вероятностями состояний в смеси.

Упражнение 8.29 (унитальность). Квантовый процесс \mathcal{E} *унитален*, если $\mathcal{E}(I) = I$. Покажите, что деполяризующий канал и канал с затуханием фазы унитальны, а канал с затуханием амплитуды — нет.

Упражнение 8.30 ($T_2 \leq T_1$). Скорость релаксации T_2 фазовой когерентности характеризует экспоненциальное затухание недиагональных элементов матрицы плотности кубита, тогда как T_1 — скорость затухания диагональных элементов (см. уравнение (7.144)). При затухании амплитуды *обе* скорости T_1 и T_2 отличны от нуля. Покажите, что при затухании амплитуды $T_1 = T_2$, а также, что если имеют место амплитудное и фазовое затухания, то $T_2 \leq T_1$.

Упражнение 8.31 (экспоненциальная чувствительность к затуханию фазы). Используя (8.126), покажите, что элемент $\rho_{nm} = \langle n|\rho|m\rangle$ матрицы плотности гармонического осциллятора экспоненциально затухает как $e^{-\lambda(n-m)^2}$ с некоторой константой λ в результате затухания фазы.

8.4 Применения квантовых преобразований

Формализм квантовых преобразований имеет многочисленные применения. В этом разд. мы опишем два из них. В подразд. 8.4.1 рассматривается теория *мастер-уравнения* — картина квантового шума, дополнительная к формализму квантовых преобразований. *Мастер-уравнение* описывает квантовый шум в *непрерывном времени*, в терминах дифференциальных уравнений. Этот подход

к квантовому шуму чаще всего используется физиками. В 8.4.2 мы опишем *томографию квантового процесса* — метод экспериментального определения динамики квантовой системы.

8.4.1 Мастер-уравнения

В самых разнообразных дисциплинах встречаются открытые системы, для изучения которых можно использовать многие методы помимо квантовых преобразований. В этом разделе мы кратко опишем один из таких методов — подход *мастер-уравнений*.

Динамика открытых квантовых систем хорошо изучена в сфере квантовой оптики. Основной целью в этом контексте, является описание временной эволюции открытой системы при помощи дифференциального уравнения, которое адекватно описывает неунитарное поведение. Такое описание предоставляется мастер-уравнением, которое в самом общем случае может быть записано в *форме Линдблада*:

$$\frac{d\rho}{dt} = -\frac{i}{\hbar}[H, \rho] + \sum_j \left[2L_j \rho L_j^\dagger - \{L_j^\dagger L_j, \rho\} \right], \quad (8.134)$$

где $\{x, y\} = xy + yx$ обозначает антикоммутатор, H — гамильтониан системы (эрмитов оператор, соответствующий когерентной части динамики), а L_j — *операторы Линдблада*, представляющие взаимодействие системы со средой. Дифференциальное уравнение записано в приведенной выше форме, чтобы обеспечить то, что процесс вполне положителен в смысле, аналогичном использованному для описания квантовых преобразований. Также принято считать, что состояние системы и среды в начальный момент является фактическим. Кроме того, вывод мастер-уравнения некоторого процесса обычно начинают с гамильтониана модели системы-среда, а затем, чтобы определить L_j , используют приближения Борна и Маркова. Заметим, что в формализме мастер-уравнения в любой момент времени выполняется равенство $\text{tr}(\rho(t)) = 1$.

В качестве примера уравнения Линдблада рассмотрим двухуровневую атомную систему, взаимодействующую с вакуумом и способную к спонтанному излучению. Когерентная часть эволюции атома описывается гамильтонианом $H = -\hbar\omega\sigma_z/2$. $\hbar\omega$ — это разность энергий атомных уровней. Спонтанное излучение приводит к тому, что атом, находившийся в возбужденном состоянии, переходит, излучая фотон, в основное состояние $|0\rangle$. Это излучение описывается оператором Линдблада $\sqrt{\gamma}\sigma_-$, где $\sigma_- = |0\rangle\langle 1|$ — понижающий атомный оператор, а γ — скорость спонтанного излучения. Мастер-уравнение, описывающее этот процесс, имеет вид

$$\frac{d\rho}{dt} = -\frac{i}{\hbar}[H, \rho] + \gamma \left[2\sigma_- \rho \sigma_+ - \sigma_+ \sigma_- \rho - \rho \sigma_+ \sigma_- \right], \quad (8.135)$$

где $\sigma_+ \equiv \sigma_-^\dagger$ — повышающий атомный оператор.

Чтобы решить это уравнение полезно перейти к представлению взаимодействия, т. е. сделать замену переменных:

$$\tilde{\rho}(t) \equiv e^{iHt} \rho(t) e^{-iHt}. \quad (8.136)$$

Тогда уравнение движения для $\tilde{\rho}$ выглядит как

$$\frac{d\tilde{\rho}}{dt} = \gamma [2\tilde{\sigma}\tilde{\rho}\tilde{\sigma}_+ - \tilde{\sigma}_+\tilde{\sigma}_-\tilde{\rho} - \tilde{\rho}\tilde{\sigma}_+\tilde{\sigma}_-], \quad (8.137)$$

где

$$\tilde{\sigma} \equiv e^{iHt} \sigma_- e^{-iHt} = e^{-i\omega t} \sigma_-, \quad (8.138)$$

$$\tilde{\sigma}_+ \equiv e^{iHt} \sigma_+ e^{-iHt} = e^{i\omega t} \sigma_+. \quad (8.139)$$

Окончательное уравнение движения имеет следующий вид:

$$\frac{d\tilde{\rho}}{dt} = \gamma [2\sigma_- \tilde{\rho} \sigma_+ - \sigma_+ \sigma_- \tilde{\rho} - \tilde{\rho} \sigma_+ \sigma_-]. \quad (8.140)$$

Это уравнение легко решить, используя блоховское векторное представление $\tilde{\rho}$. Решение определяется формулами

$$\lambda_x = \lambda_x(0) e^{-\gamma t}, \quad (8.141)$$

$$\lambda_y = \lambda_y(0) e^{-\gamma t}, \quad (8.142)$$

$$\lambda_z = \lambda_z(0) e^{-2\gamma t} + 1 - e^{-2\gamma t}. \quad (8.143)$$

Обозначив $\gamma' = 1 - \exp(-2t\gamma)$, можно легко проверить, что такая эволюция эквивалентна уравнению

$$\tilde{\rho} = \mathcal{E}(\tilde{\rho}(0)) \equiv E_0 \tilde{\rho}(0) E_0^\dagger + E_1 \tilde{\rho}(0) E_1^\dagger, \quad (8.144)$$

где

$$E_0 \equiv \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1 - \gamma'} \end{bmatrix}, \quad (8.145)$$

$$E_1 \equiv \begin{bmatrix} 0 & \sqrt{\gamma'} \\ 0 & 0 \end{bmatrix} \quad (8.146)$$

— элементы, задающие квантовое преобразование \mathcal{E} . Обратите внимание, что следствием этого преобразования является затухание амплитуды (сравните с уравнением (8.108)). Рассмотренная ситуация — частный случай спин-бозонной модели, в которой маленькая конечномерная квантовая система взаимодействует с резервуаром простых гармонических осцилляторов. В физике она важна при описании взаимодействия атомов с электромагнитным излучением, как например, в квантовом резонаторе, атомной или ионной ловушке.

Подход мастер-уравнения менее общий, чем формализм квантовых преобразований. Решив мастер-уравнение, можно определить временную зависимость матрицы плотности. Знание ее, в свою очередь означает, что результат может быть выражен как квантовое преобразование в представлении операторной суммой

$$\rho(t) = \sum_k E_k(t) \rho(0) E_k^\dagger(t), \quad (8.147)$$

где $E_k(t)$ — зависящие от времени элементы преобразования, определяемые из решения мастер-уравнения. Однако квантовый процесс, выраженный в терминах представления операторной суммой, не обязательно можно записать в виде мастер-уравнения. Например, квантовые преобразования могут описывать не марковскую динамику просто потому, что они характеризуют только изменения состояния, а не непрерывную эволюцию во времени. Тем не менее каждый подход занимает свое место. Фактически даже квантовые преобразования не дают *самого общего описания*; в разд. 8.5 мы рассмотрим некоторые процессы, которые нельзя представить квантовыми преобразованиями.

8.4.2 Томография квантовых процессов

Квантовые преобразования дают прекрасную математическую модель для открытых квантовых систем, их легко себе представить (по крайней мере для кубитов), но какое отношение они имеют к экспериментально измеримым величинам? Какие измерения должен проделать экспериментатор, чтобы определить динамику квантовой системы? Для классической системы эта элементарная задача известна как *идентификация системы*. Здесь будет показано, как осуществить аналогичное действие над конечномерной квантовой системой, т. е. — *томографию квантового процесса*.

Чтобы понять томографию процесса, вначале необходимо рассмотреть другую процедуру. Это так называемая *томография квантового состояния* — метод экспериментального определения неизвестного квантового состояния. Предположим, имеется неизвестное состояние отдельного кубита ρ . Как можно экспериментально определить ρ ?

Если дана единственная копия ρ , то измерить ее невозможно. Главная проблема состоит в том, что никакое квантовое измерение не способно гарантированно отличить неортогональные квантовые состояния, такие, как $|0\rangle$ и $(|0\rangle + |1\rangle)/\sqrt{2}$. Тем не менее можно определить ρ , если есть большое количество экземпляров ρ . Например, если ρ — квантовое состояние, полученное в результате некоторого эксперимента, можно просто повторить эксперимент много раз, чтобы получить много копий состояния ρ .

Предположим, имеется много копий однокубитовой матрицы плотности ρ . Множество $I/\sqrt{2}, X/\sqrt{2}, Y/\sqrt{2}, Z/\sqrt{2}$ образует ортонормированный набор матриц по отношению к скалярному произведению Гильберта–Шмидта, т. е. ρ можно разложить следующим образом:

$$\rho = \frac{\text{tr}(\rho)I + \text{tr}(X\rho)X + \text{tr}(Y\rho)Y + \text{tr}(Z\rho)Z}{2}. \quad (8.148)$$

Вспомним, однако, что выражения вида $\text{tr}(A\rho)$ имеют смысл средних значений наблюдаемых. Например, чтобы определить $\text{tr}(Z\rho)$, следует измерить наблюдаемую Z большое количество раз m и получить z_1, z_2, \dots, z_m , равные $+1$ или -1 . Эмпирическое среднее этих значений $\sum_i z_i/m$ — это оценка действительного значения $\text{tr}(Z\rho)$. Можно использовать центральную предельную теорему, чтобы определить, насколько хороша эта оценка при больших m , когда она становится практически гауссовой со средним значением, равным $\text{tr}(Z\rho)$, и со стандартным отклонением $\Delta(Z)/\sqrt{m}$, где $\Delta(Z)$ — стандартное отклонение одного измерения Z , которое ограничено сверху единицей, так что стандартное отклонение нашей оценки $\sum_i z_i/m$ не превышает $1/\sqrt{m}$.

Подобным же образом с большой степенью надежности можно оценить величины $\text{tr}(X\rho)$ и $\text{tr}(Y\rho)$ в пределе большого размера выборки, и, таким образом, получить хорошее приближение для ρ . Обобщение этой процедуры на случай большего, чем один, числа кубитов несложно, по крайней мере в принципе. Аналогично случаю с одним кубитом произвольную матрицу плотности n кубит можно разложить как

$$\rho = \sum_{\vec{v}} \frac{\text{tr}(\sigma_{v_1} \otimes \sigma_{v_2} \otimes \cdots \otimes \sigma_{v_n} \rho) \sigma_{v_1} \otimes \sigma_{v_2} \otimes \cdots \otimes \sigma_{v_n}}{2^n}, \quad (8.149)$$

где суммирование выполняется по векторам $\vec{v} = (v_1, \dots, v_n)$ с элементами v_i , выбранными из множества $0, 1, 2, 3$. Проводя измерения наблюдаемых, которые являются произведениями матриц Паули, можно оценить каждый член этой суммы и, таким образом, получить оценку для ρ .

Мы описали, как осуществить томографию состояния для системы, составленной из кубитов. А что, если не кубитовая система? Не вызывает удивления то, что приведенный выше метод легко обобщить на такие системы. Мы не будем здесь этим заниматься, а отошлем читателя к разделу «История и дополнительная литература» в конце главы.

Теперь мы знаем, как осуществить томографию квантового состояния. Попытаемся использовать этот способ для томографии квантового процесса? Экспериментальная методика может быть описана следующим образом. Предположим, пространство состояний системы имеет размерность d , например для одного кубита $d = 2$. Мы выбираем d^2 чистых квантовых состояний $|\psi_1\rangle, \dots, |\psi_{d^2}\rangle$ так, что соответствующие матрицы плотности $|\psi_1\rangle\langle\psi_1|, \dots, |\psi_{d^2}\rangle\langle\psi_{d^2}|$ образуют базисный набор пространства матриц. Более детально выбор такого набора будет объяснен ниже. Для каждого j мы подготовим квантовую систему в состоянии $|\psi_j\rangle$, а затем подвернем ее процессу \mathcal{E} , томографию которого мы собираемся осуществить. После того, как процесс завершится, мы используем томографию квантового состояния, чтобы определить получаемое состояние $\mathcal{E}(|\psi_j\rangle\langle\psi_j|)$. Встав на позицию пуриста, можно сказать, что все сделано, поскольку в принципе квантовое преобразование \mathcal{E} теперь определяется линейным расширением на все состояния.

На практике, конечно, мы бы хотели иметь способ определения удобного представления \mathcal{E} из экспериментально доступных данных. Опишем общую

процедуру, позволяющую это сделать, разработанную специально для случая одного кубита. Нашей целью является определение множества элементов преобразования $\{E_i\}$ для \mathcal{E}

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger. \quad (8.150)$$

Однако эксперименты дают числа, а не операторы, являющиеся теоретическим понятием. Чтобы определить E_i исходя из измеримых параметров, удобно рассмотреть эквивалентное описание \mathcal{E} , используя *фиксированный* набор операторов \tilde{E}_i , которые образуют базис на множестве операторов в пространстве состояний, так что

$$E_i = \sum_m e_{im} \tilde{E}_m \quad (8.151)$$

для некоторых комплексных чисел e_{im} . Уравнение (8.150) может быть переписано в виде

$$\mathcal{E}(\rho) = \sum_{mn} \tilde{E}_m \rho \tilde{E}_n^\dagger \chi_{mn}, \quad (8.152)$$

где $\chi_{mn} \equiv \sum_i e_{ime} e_{in}^*$ — элементы матрицы, которая, по определению, положительна и эрмитова. Это выражение, известное как *представление χ -матрицей*, показывает, что \mathcal{E} можно полностью описать матрицей комплексных чисел χ , если зафиксирован набор операторов \tilde{E}_i .

Вообще χ будет содержать $d^4 - d^2$ независимых действительных параметров, потому что линейное отображение пространства $d \times d$ матриц в себя описывается d^4 независимыми параметрами, но имеется еще d^2 дополнительных ограничений, связанных с тем, что ρ должна оставаться эрмитовой со следом, равным единице, т. е. выполняется соотношение полноты

$$\sum_i E_i^\dagger E_i = I, \quad (8.153)$$

что дает d^2 связей. Мы покажем, как экспериментально определить χ , а затем, как восстановить представление операторной суммой в виде (8.150), зная матрицу χ .

Пусть ρ_j , $1 \leq j \leq d^2$ — фиксированный линейно-независимый базис в пространстве матриц $d \times d$, т. е. любая матрица $d \times d$ может быть однозначно записана как линейная комбинация ρ_j . Удобным выбором является множество операторов $|n\rangle\langle m|$. С экспериментальной точки зрения конечное состояние $\mathcal{E}(|n\rangle\langle m|)$ может быть получено, если приготовить исходные состояния $|n\rangle$, $|m\rangle$, $|+\rangle = (|n\rangle + |m\rangle)/\sqrt{2}$ и $|-\rangle = (|n\rangle - |m\rangle)/\sqrt{2}$ и образовать линейную комбинацию $\mathcal{E}(|n\rangle\langle n|)$, $\mathcal{E}(|m\rangle\langle m|)$, $\mathcal{E}(|+\rangle\langle +|)$ и $\mathcal{E}(|-\rangle\langle -|)$ следующим образом:

$$\mathcal{E}(|n\rangle\langle m|) = \mathcal{E}(|+\rangle\langle -|) + i\mathcal{E}(|-\rangle\langle -|) - \frac{1+i}{2}\mathcal{E}(|n\rangle\langle n|) - \frac{1+i}{2}\mathcal{E}(|m\rangle\langle m|). \quad (8.154)$$

Затем при помощи томографии квантового состояния можно определить $\mathcal{E}(\rho_j)$ для каждого ρ_j .

Более того, каждую $\mathcal{E}(\rho_j)$ можно выразить как линейную комбинацию базисных состояний

$$\mathcal{E}(\rho_j) = \sum_k \lambda_{jk} \rho_k, \quad (8.155)$$

а, поскольку $\mathcal{E}(\rho_j)$ известно из томографии состояния, λ_{jk} можно определить при помощи стандартных алгоритмов линейной алгебры. Продолжая преобразования, можно написать

$$\tilde{E}_m \rho_j \tilde{E}_n^\dagger = \sum_k \beta_{jk}^{mn} \rho_k, \quad (8.156)$$

где β_{jk}^{mn} — комплексные числа, которые также можно вычислить при помощи стандартных алгоритмов из линейной алгебры, зная операторы \tilde{E}_m и ρ_j . Используя последние два выражения и (8.152), получим следующее уравнение:

$$\sum_k \sum_{mn} \chi_{mn} \beta_{jk}^{mn} \rho_k = \sum_k \lambda_{jk} \rho_k. \quad (8.157)$$

Из линейной независимости ρ_k следует, что для каждого k имеет место выражение

$$\sum_{mn} \beta_{jk}^{mn} \chi_{mn} = \lambda_{jk}. \quad (8.158)$$

Это необходимое и достаточное условие того, что матрица χ дает правильное квантовое преобразование \mathcal{E} . Можно считать χ и λ векторами, а β — матрицей $d^4 \times d^4$ со столбцами, нумеруемыми парами mn , и строками — парами jk . Покажем, каким образом можно получить χ . Пусть κ — обобщенное обратное матрицы β , удовлетворяющее соотношению

$$\beta_{jk}^{mn} \sum_{st,xy} \beta_{jk}^{st} \kappa_{st}^{xy} \beta_{xy}^{mn}. \quad (8.159)$$

Большинство компьютерных программ для вычислений с матрицами способны находить такие обобщенные обратные. Теперь мы докажем, что χ , определенная формулой

$$\chi_{mn} \equiv \sum_{jk} \kappa_{jk}^{mn} \lambda_{jk}, \quad (8.160)$$

удовлетворяет соотношению (8.158).

Сложность состоит в том, что, вообще говоря, χ не задается однозначно уравнением (8.158). Для удобства перепишем эти уравнения в матричной форме:

$$\beta \vec{\chi} = \vec{\lambda}, \quad (8.161)$$

$$\vec{\chi} \equiv \kappa \vec{\lambda}. \quad (8.162)$$

Из построения, которое привело к уравнению (8.152) нам известно, что существует по меньшей мере одно решение уравнения (8.161), которое мы назовем

$\vec{\chi}'$. Следовательно, $\vec{\lambda} = \beta\vec{\chi}'$. Обобщенное обратное удовлетворяет равенству $\beta\kappa\beta = \beta$. Умножая определение $\vec{\chi}$ слева на β , получим

$$\beta\vec{\chi} = \beta\kappa\vec{\lambda} \quad (8.163)$$

$$= \beta\kappa\beta\vec{\chi}' \quad (8.164)$$

$$= \beta\vec{\chi}' \quad (8.165)$$

$$= \vec{\lambda}. \quad (8.166)$$

Следовательно, χ , заданное (8.162), удовлетворяет равенству (8.161), что мы и хотели показать.

Определив χ , можно сразу получить представление \mathcal{E} операторной суммой следующим образом. Пусть унитарная матрица U^+ диагонализует χ

$$\chi_{mn} = \sum_{xy} U_{mx} d_x \delta_{xy} U_{ny}^*. \quad (8.167)$$

Легко убедиться, что

$$E_i = \sqrt{d_i} \sum_k U_{ji} \tilde{E}_j \quad (8.168)$$

— элементы преобразования \mathcal{E} . Тогда можно сказать, что алгоритм состоит из следующих шагов: λ определяется экспериментально при помощи томографии состояний, которая в свою очередь задает χ уравнением $\vec{\chi} = \kappa\lambda$, что дает полное описание \mathcal{E} , в том числе набор элементов преобразования E_i .

В случае однокубитового квантового процесса необходимо определить лишь 12 параметров (вставка 8.5). Томография двухкубитового квантового «черного ящика» \mathcal{E}_2 гораздо сложнее. В этом случае следует найти 240 параметров для того, чтобы полностью описать квантовое преобразование, действующее на систему! Очевидно, что их нахождение было бы довольно серьезным предприятием. Однако, как и в случае с одним кубитом, существует относительно прямой метод реализации компьютерной программы, которая автоматизирует вычисление при условии, что экспериментальные методики проведения томографии состояния и приготовления состояний доступны в лаборатории.

Вставка 8.5. Томография процесса в случае одного кубита

Общий метод томографии процесса можно упростить в случае преобразований одного кубита, получив явные формулы, которые можно использовать для обработки экспериментальных данных. Эти упрощения становятся возможными благодаря выбору фиксированных операторов \tilde{E}_i , коммутационные свойства которых позволяют определить χ -матрицу прямым матричным умножением. В случае одного кубита мы используем следующие обозначения:

$$\tilde{E}_0 = I, \quad (8.169)$$

$$\tilde{E}_1 = X, \quad (8.170)$$

$$\tilde{E}_2 = -iY, \quad (8.171)$$

$$\tilde{E}_3 = Z. \quad (8.172)$$

В χ содержится 12 параметров, которые задают произвольное однокубитовое квантовое преобразование \mathcal{E} . Эти параметры могут быть измерены в четырех сериях экспериментов. В качестве конкретного примера предположим, что приготовлены состояния $|0\rangle$, $|1\rangle$, $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ и $|-\rangle = (|0\rangle + i|1\rangle)/\sqrt{2}$, и четыре матрицы

$$\rho'_1 = \mathcal{E}(|0\rangle\langle 0|), \quad (8.173)$$

$$\rho'_4 = \mathcal{E}(|1\rangle\langle 1|), \quad (8.174)$$

$$\rho'_2 = \mathcal{E}(|+\rangle\langle +|) - i\mathcal{E}(|-\rangle\langle -|) - (1-i)(\rho'_1 + \rho'_4)/2, \quad (8.175)$$

$$\rho'_3 = \mathcal{E}(|+\rangle\langle +|) + i\mathcal{E}(|-\rangle\langle -|) - (1+i)(\rho'_1 + \rho'_4)/2 \quad (8.176)$$

определяются при помощи томографии состояния. Они соответствуют $\rho'_j = \mathcal{E}(\rho_j)$, где

$$\rho_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad (8.177)$$

$\rho_2 = \rho_1 X$, $\rho_3 = X \rho_1$ и $\rho_4 = X \rho_1 X$. Из (8.156) и уравнений (8.169)–(8.172) можно определить β , и аналогично ρ'_j определяет λ . Однако благодаря специальному выбору базиса, используя представление \tilde{E}_i матрицами Паули, можно выразить матрицу β как кронекеровское произведение $\beta = \Lambda \otimes \Lambda$, где

$$\Lambda = \frac{1}{2} \begin{bmatrix} I & X \\ X & -I \end{bmatrix}, \quad (8.178)$$

так что χ удобно выразить в терминах блочных матриц.

$$\chi = \Lambda \begin{bmatrix} \rho'_1 & \rho'_2 \\ \rho'_3 & \rho'_4 \end{bmatrix} \Lambda. \quad (8.179)$$

Мы показали, как динамика квантовой системы может быть экспериментально определена при помощи регулярной процедуры. Данная методика томографии квантового процесса аналогична шагу идентификации системы в классической теории управления и играет схожую роль для понимания и управления квантовыми системами с шумом.

Упражнение 8.32. Объясните, как обобщить квантовую томографию процесса на случай не сохраняющих след квантовых преобразований, возникающих, например, при исследовании процесса измерения.

Упражнение 8.33 (задание квантового процесса). Предположим, мы хотим точно задать произвольное квантовое преобразование \mathcal{E} одного кубита, описывая, как преобразуется набор точек $\{\vec{r}_k\}$ на сфере Блоха. Докажите, что это множество должно содержать не менее четырех точек.

Упражнение 8.34 (томография процесса для двух кубитов). Покажите, что матрица χ_2 , описывающая действие «черного ящика» на двух кубитах, может быть выражена следующим образом:

$$\chi_2 = \Lambda_2 \bar{\rho}' \Lambda_2, \quad (8.180)$$

где $\Lambda_2 = \Lambda \otimes \Lambda$, Λ определена во вставке 8.5, а $\bar{\rho}'$ — блочная матрица из 16 измеренных матриц плотности:

$$\bar{\rho}' = P^T \begin{bmatrix} \rho'_{11} & \rho'_{12} & \rho'_{13} & \rho'_{14} \\ \rho'_{21} & \rho'_{22} & \rho'_{23} & \rho'_{24} \\ \rho'_{31} & \rho'_{32} & \rho'_{33} & \rho'_{34} \\ \rho'_{41} & \rho'_{42} & \rho'_{43} & \rho'_{44} \end{bmatrix} P; \quad (8.181)$$

здесь $\rho'_{nm} = \mathcal{E}(\rho_{nm})$, $\rho_{nm} = T_n |00\rangle \langle 00| T_m$, $T_1 = I \otimes I$, $T_2 = I \otimes X$, $T_3 = X \otimes I$, $T_4 = X \otimes X$ и $P = I \otimes [(\rho_{00} + \rho_{12} + \rho_{21} + \rho_{33}) \otimes I]$ — матрица перестановки.

Упражнение 8.35 (пример томографии процесса). Рассмотрим «черный ящик» на одном кубите с неизвестной динамикой \mathcal{E}_1 . Предположим, что следующие четыре матрицы плотности получены из экспериментальных измерений, произведенных в соответствии с уравнениями (8.173)-(8.176):

$$\rho'_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad (8.182)$$

$$\rho'_2 = \begin{bmatrix} 0 & \sqrt{1-\gamma} \\ 0 & 0 \end{bmatrix}, \quad (8.183)$$

$$\rho'_3 = \begin{bmatrix} 0 & 0 \\ \sqrt{1-\gamma} & 0 \end{bmatrix}, \quad (8.184)$$

$$\rho'_4 = \begin{bmatrix} \gamma & 0 \\ 0 & 1-\gamma \end{bmatrix}, \quad (8.185)$$

где γ — численный параметр. Из этих соотношений можно сделать несколько существенных выводов: основное состояние $|0\rangle$ остается инвариантным под действием \mathcal{E}_1 , возбужденное состояние $|1\rangle$ частично переходит в основное, а смешанные состояния затухают. Определите χ -матрицу этого процесса.

8.5 Ограничения формализма квантовых преобразований

Существуют ли интересные квантовые системы, чья динамика не описывается квантовыми преобразованиями? В этом разделе мы сконструируем искусственный пример такой системы и попытаемся выяснить обстоятельства, при которых это возможно.

Предположим, один кубит приготовлен в некотором неизвестном квантовом состоянии ρ , что подразумевает выполнение над ним определенной процедуры в лаборатории. Пусть среди степеней свободы лаборатории есть один кубит, который как побочный эффект процедуры приготовления оказывается в состоянии $|0\rangle$, если состояние ρ находится в нижней половине блоховской сферы, и в состоянии $|1\rangle$, если ρ — в верхней половине. Тогда состояние системы после приготовления имеет вид

$$\rho \otimes |0\rangle\langle 0| \otimes \text{остальные степени свободы}, \quad (8.186)$$

если ρ находится в нижней половине блоховской сферы, и

$$\rho \otimes |1\rangle\langle 1| \otimes \text{остальные степени свободы}, \quad (8.187)$$

если ρ лежит в верхней половине блоховской сферы.

Как только приготовление состояния завершено, система начинает взаимодействовать со средой, в данном случае со степенями свободы лаборатории. Предположим, взаимодействие происходит так, что приводит к преобразованию СНОТ над основной системой и дополнительным кубитом лабораторной системы. Таким образом, если в начальный момент вектор Блоха системы находился в нижней половине сферы Блоха, то в результате этого процесса он остается неизменным, если же он был в верхней половине сферы Блоха — он поворачивается в ее нижнюю половину.

Очевидно, этот процесс не является аффинным отображением, действующим на сфере Блоха и тогда в соответствии с результатами, полученными в подразд. 8.3.2, *не может быть квантовым преобразованием*. Из этого примера нужно извлечь следующий урок: *эволюция квантовой системы, которая взаимодействует со степенями свободы, использованными для ее приготовления, по завершении приготовления не будет адекватно описываться в рамках формализма квантовых преобразований*. Важно было получить это заключение, поскольку оно показывает, что существуют физически разумные условия, при которых формализм квантовых преобразований неадекватно описывает процессы, происходящие в квантовых системах. Необходимо иметь это в виду, например, в приложениях процедуры томографии квантовых процессов, обсуждавшейся в предыдущем разделе.

Тем не менее в оставшейся части книги мы будем работать в рамках формализма квантовых преобразований. Он предоставляет мощный и довольно общий метод описания динамики квантовых систем. Этот метод особенно эффективен в задачах, связанных с квантовой обработкой информации. Изучение

квантовой обработки информации за рамками формализма квантовых преобразований представляет интерес для дальнейших исследований.

Задача 8.1 (от формы Линдблада к квантовым преобразованиям). Используя обозначения подразд. 8.4.1, решите в явном виде дифференциальное уравнение

$$\dot{\rho} = -\frac{\lambda}{2}(\sigma_+\sigma_- \rho + \rho \sigma_+ \sigma_- - 2\sigma_- \rho \sigma_+) \quad (8.188)$$

относительно $\rho(t)$. Выразите отображение $\rho(0) \rightarrow \rho(t)$ как $\rho(t) = \sum_k E_k(t)\rho(0)E_k^\dagger(t)$.

Задача 8.2 (телеportация как квантовое преобразование). Предположим, у Алисы есть один кубит, обозначенный как система 1, который она хочет передать Бобу. К сожалению, она и Боб пользуются только одной несовершенно запутанной парой кубитов. Половину пары, принадлежащую Алисе, назовем системой 2, а половину, принадлежащую Бобу — системой 3. Предположим, Алиса проводит измерение, описываемое набором квантовых преобразований \mathcal{E}_m , с результатом m над системами 1 и 2. Покажите, что это индуцирует квантовое преобразование $\tilde{\mathcal{E}}_m$, связывающее начальное состояние системы 1 с конечным состоянием системы 3, и что телепортация осуществляется, если Боб сможет обратить это преобразование, используя такое сохраняющее след квантовое преобразование \mathcal{R}_m , что

$$\mathcal{R}_m \left(\frac{\tilde{\mathcal{E}}_m(\rho)}{\text{tr}[\tilde{\mathcal{E}}_m(\rho)]} \right) = \rho, \quad (8.189)$$

где ρ — начальное состояние системы 1.

Задача 8.3 (случайные унитарные каналы). Может показаться, что все унитарные каналы, т. е. те, для которых $\mathcal{E}(I) = I$, появляются в результате усреднения по случайным унитарным преобразованиям, т. е., $\mathcal{E}(\rho) = \sum_k p_k U_k \rho U_k^\dagger$, где U_k — унитарные операторы, а p_k образуют распределение вероятности. Покажите, что, хотя это и верно для одного кубита, это неверно для большего размера систем.

Краткое содержание главы:

- Представление операторной суммой. Поведение открытой квантовой системы может быть представлено в виде

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger, \quad (8.190)$$

где E_k — элементы преобразования, причем $\sum_k E_k^\dagger E_k = I$, если квантовое преобразование сохраняет след.

- Модели среды для квантовых преобразований.** Сохраняющее след квантовое преобразование всегда можно получить как результат унитарного взаимодействия системы с заранее не скоррелированной средой, и наоборот. Не сохраняющие след квантовые преобразования можно трактовать подобным образом, если ввести дополнительное проективное измерение, производимое над объединением системы и среды, которое дает разные результаты, соответствующие разным, не сохраняющим след квантовым преобразованиям.
- Томография квантового процесса.** Квантовое преобразование d -мерной квантовой системы можно полностью определить экспериментально, измеряя матрицы плотности, получаемые из d^2 чистых состояний на входе.
- Элементы важных преобразований одного кубита:**

Деполяризующий канал	$\sqrt{1 - \frac{3p}{4}} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \sqrt{\frac{p}{4}} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$ $\sqrt{\frac{p}{4}} \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sqrt{\frac{p}{4}} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Затухание амплитуды	$\begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix}, \quad \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix}$
Затухание фазы	$\begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 \\ 0 & \sqrt{\gamma} \end{bmatrix}$
Переворот фазы	$\sqrt{p} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \sqrt{1-p} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Классическая ошибка	$\sqrt{p} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \sqrt{1-p} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Фазовая ошибка	$\sqrt{p} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \sqrt{1-p} \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$

История и дополнительная литература

Квантовый шум — важное явление, возникающее в разных ситуациях, и на эту тему выпущена обширная литература. Мы ограничимся ссылками только на малую выборку источников. Одна из первых монографий по квантовому шуму в математическом контексте принадлежит Дэвису [114]. Калдейра и Леггет [89] предприняли одно из первых и наиболее полных исследований важной модели, известной как *спин-бозонная* модель, используя подход, основанный на Фейнмановских интегралах по траекториям. Гардинер [159] изучал квантовый шум в контексте квантовой оптики. Позднее квантооптическое сообщество развило подход *квантовых траекторий* к квантовому шуму. Обзоры по этой теме можно найти в статьях Цоллера и Гардинера [432], а также Пленио и Найта [324].

По квантовым преобразованиям существует большое количество источников. Упомянем лишь несколько ключевых работ, особенно выделим книгу Крауса [229], содержащую ссылки на более ранние источники по данному вопросу. Гелльвиг и Краус [187, 188], а также Чои [85] выпустили статьи, оказавшие большое влияние на развитие этого направления. Линдблад [246] установил связь между формализмом квантовых преобразований и теорией непрерывной временной квантовой эволюции, введя то, что сейчас называется формой Линдблада. Шумахер [348] и Кейвс [78] написали отличные обзоры по формализму квантовых преобразований применительно к квантовой коррекции ошибок.

Томография квантового состояния была предложена Богелем и Рискеном [407]. Леонгардт [241] написал обзор, содержащий ссылки на другие работы. На значение томографий квантовых процессов было указано в работе Тюршета, Худа, Ланжа, Мабучи и Кимбла [385]. Теория была разработана независимо Чангом и Нильсеном [96], а также Пойатосом, Сираком и Цоллером [314]. Ранее Джонс [202] обрисовал основные идеи томографии квантового процесса.

Печальная путаница возникла с термином «потеря когерентности»¹. Исторически он использовался лишь для обозначения процесса затухания фазы, в частности Зуреком [438]. Зурек и другие исследователи осознали, что затухание фазы имеет исключительную роль при переходе от квантовой к классической физике; для определенных видов взаимодействия со средой оно происходит во временных масштабах гораздо более быстрых, чем любой процесс затухания амплитуды и может, таким образом, быть гораздо более важным в определении потери квантовой когерентности. Основным положением этих исследований было появление классичности из-за взаимодействия со средой. Тем не менее использование термина «потеря когерентности» в контексте квантовых вычислений и квантовой информации относится к *любому процессу шума* в квантовом устройстве. В этой книге мы предпочитаем более общий термин «*квантовый шум*» и стремимся его использовать, хотя иногда *потеря когерентности* находит себе подходящее место в контексте.

Более детальное обсуждение некоторых из ограничений формализма кван-

¹Имеется в виду английский термин «decoherence». — Прим. ред.

товых преобразований (и, в частности, предположения о том, что состояние системы и среды в начальный момент является произведением) дано Ройером [340].

Задача 8.2 принадлежит Нильсену и Кейвсу [301]. Задача 8.3 появилась у Ландау и Стритера [268] как часть глубокого исследования экстремальных точек выпуклого множества дважды стохастических преобразований.

Глава 9

МЕРЫ РАЗЛИЧИЯ КВАНТОВОЙ ИНФОРМАЦИИ

Что означает утверждение, что два набора информации похожи? Что понимать под тем, что информация сохраняется в некотором процессе? Эти вопросы являются центральными в теории обработки квантовой информации. В этой главе мы дадим количественные ответы на них, используя *меры различия*. Основываясь на этих двух вопросах, мы рассмотрим два широких класса мер, различая статические и динамические меры. Статические меры определяют, насколько близки два квантовых состояния, динамические — насколько сохраняется информация в некотором процессе. Мы начнем со статических мер и затем используем их в качестве основы для разработки динамических.

При введении мер различия как в классической, так и в квантовой механике существует определенный произвол. В теории квантовых вычислений и квантовой информации, используется несколько мер различия. В этой главе мы рассмотрим две наиболее широко используемые из них: *следовую метрику* и *степень совпадения*. В большинстве случаев их свойства почти одинаковы, однако иногда удобнее использовать какую-либо одну из них.

9.1 Меры различия классической информации

Поиск различий в распределениях вероятностей — скользкое дело.

Кристофер Фукс

Давайте начнем с интуитивно более понятных мер различия для классической информации. Сравним строки битов, например, 00010 и 10011. Один из способов определения расстояния между ними — *метрика Хэмминга*, которая определяется как число разрядов, различающихся в двух строках. Строки 00010 и 10011 различаются только в первом и последнем разрядах, так что расстояние между ними в метрике Хэмминга равно двум. К сожалению, метрика Хэмминга вводится только для дискретных состояний. В квантовой механике состояния непрерывны и эта метрика работать не будет.

Лучше начать изучение мер различия квантовой информации со сравнения классических распределений вероятностей. Источник классической информации обычно рассматривают как случайную величину, распределенную в соответствии с некоторым алфавитом. Например, неизвестный источник англий-

скогого текста может быть представлен как последовательность случайных букв латинского алфавита. Перед тем, как прочитать текст, мы можем сделать некоторые предположения об относительной частоте различных букв и о корреляциях между ними, например, можно предположить, что в английском тексте сочетание 'th' встречается гораздо чаще, чем 'zx'. Возможность характеризовать информацию с помощью распределения вероятностей подталкивает нас к тому, чтобы провести сравнение разных распределений.

Что означает утверждение, что два распределения вероятностей p_x и q_x с одним набором индексов x похожи друг на друга? Однозначный ответ на этот вопрос дать трудно, вместо этого мы определим две меры различия, каждая из которых широко используется при изучении квантовых вычислений и квантовой информации. Одной из этих мер является *следовая метрика*, которая определяется как

$$D(p_x, q_x) \equiv \frac{1}{2} \sum_x |p_x - q_x|. \quad (9.1)$$

Эта величина называется также L_1 метрикой, или метрикой Колмогорова. Мы предпочитаем термин «следовая метрика», потому что в квантовой механике аналогичная величина определяется через функцию следа. Она действительно является метрикой, так как симметрична ($D(x, y) = D(y, x)$) и удовлетворяет неравенству треугольника $D(x, z) \leq D(x, y) + D(y, z)$.

Упражнение 9.1. Найдите расстояние между распределениями вероятностей $(1, 0)$ и $(1/2, 1/2)$ в следовой метрике; между распределениями $(1/2, 1/3, 1/6)$ и $(3/4, 1/8, 1/8)$.

Упражнение 9.2. Покажите, что расстояние между распределениями вероятностей $(p, 1-p)$ и $(q, 1-q)$ в следовой метрике равно $|p - q|$.

Другой мерой различия, которую мы введем, является *степень совпадения*. Степень совпадения распределений вероятностей p_x и q_x определяется как

$$F(p_x, q_x) \equiv \sum_x \sqrt{p_x q_x}. \quad (9.2)$$

Степень совпадения сильно отличается от следовой метрики. Прежде всего, она не является метрикой, так как для одинаковых распределений $\{p_x\}$ и $\{q_x\}$, имеем $F(p_x, q_x) = \sum_x p_x = 1$. Позднее мы обсудим метрику, которую можно получить из степени совпадения. Геометрическая интерпретация степени совпадения дана на рис. 9.1. Степень совпадения — это скалярное произведение векторов единичной длины с компонентами $\sqrt{p_x}$ и $\sqrt{q_x}$.

Упражнение 9.3. Найдите степень совпадения для распределениями вероятностей $(1, 0)$ и $(1/2, 1/2)$; для распределений $(1/2, 1/3, 1/6)$ и $(3/4, 1/8, 1/8)$.

Следовая метрика и степень совпадения позволяют определять расстояние между двумя распределениями вероятностей. Но имеют ли они физический смысл? Для следовой метрики физический смысл, действительно, существует. Легко доказать, что

$$D(p_x, q_x) = \max_S |p(S) - q(S)| = \max_S \left| \sum_{x \in S} p_x - \sum_{x \in S} q_x \right|. \quad (9.3)$$

Здесь максимум берется по всем подмножествам S набора индексов x . Величина под знаком максимума — разность вероятностей события S , соответствующих первому и второму распределениям. При максимизации находится событие S , для которого сильнее всего различаются рассматриваемые распределения вероятностей, а следовая метрика показывает величину этого различия.

К сожалению, для степени совпадения нет такой простой интерпретации. Однако мы будем изучать степень совпадения, так как она полезна для различных математических целей. Не исключено, что ее физический смысл будет найден в будущем. Кроме того, существует тесная связь между степенью совпадения и следовой метрикой, и свойства одной из этих величин часто можно получить из свойств другой.

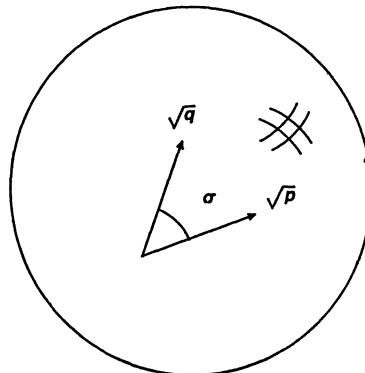


Рис. 9.1. Геометрическая интерпретация степени совпадения как скалярного произведения векторов $\sqrt{p_x}$ и $\sqrt{q_x}$ единичной длины ($1 = \sum_x (\sqrt{p_x})^2 = \sum_x (\sqrt{q_x})^2$)

Упражнение 9.4. Докажите соотношение (9.3).

Упражнение 9.5. Покажите, что в формуле (9.3) можно убрать знак модуля, т. е., что

$$D(p_x, q_x) = \max_S |p(S) - q(S)| = \max_S \left(\sum_{x \in S} p_x - \sum_{x \in S} q_x \right). \quad (9.4)$$

Следовая метрика и степень совпадения — статические меры различия. С их помощью можно определять расстояние между двумя постоянными распределениями вероятностей. Существует третья мера различия, которая является *динамической*, т. е. она позволяет определить, насколько меняется информация в некотором физическом процессе. Предположим, что некоторая случайная величина X передается по каналу с шумом. В канале происходит марковский процесс $X \rightarrow Y$ и на выходе получается другая случайная величина Y .

Для удобства предположим, что возможные значения величин X и Y одинаковы и мы будем обозначать их через x . Тогда вероятность того, что величина Y не равна X , $p(X \neq Y)$, и будет очевидной мерой того, насколько информация сохраняется в этом процессе.

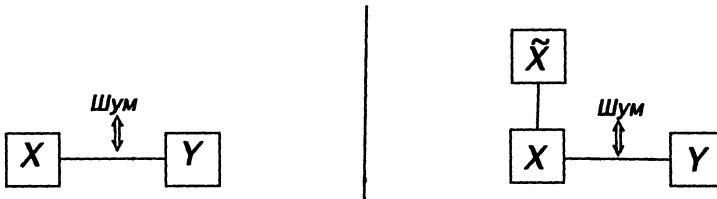


Рис. 9.2. Можно сделать копию \tilde{X} величины X , перед тем, как она под действием шума перейдет в Y в марковском процессе.

Эта динамическая мера различия может рассматриваться как специальный случай статической следовой метрики. Предположим, что перед передачей по каналу с шумом случайной величины X мы делаем ее копию $\tilde{X} = X$. После передачи получаем случайную величину Y , как показано на рис. 9.2. Насколько близка исходная, идеально коррелированная пара (\tilde{X}, X) к полученной (\tilde{X}, Y) ? Используя следовую метрику, находим:

$$D((\tilde{X}, X), (\tilde{X}, Y)) = \frac{1}{2} \sum_{xx'} |\delta_{xx'} p(X = x) - p(\tilde{X} = x, Y = x')| \quad (9.5)$$

$$\begin{aligned} &= \frac{1}{2} \sum_{x \neq x'} p(\tilde{X} = x, Y = x') \\ &\quad + \frac{1}{2} \sum_x |p(X = x) - p(\tilde{X} = x, Y = x)| \end{aligned} \quad (9.6)$$

$$\begin{aligned} &= \frac{1}{2} \sum_{x \neq x'} p(\tilde{X} = x, Y = x') \\ &\quad + \frac{1}{2} \sum_x (p(X = x) - p(\tilde{X} = x, Y = x)) \end{aligned} \quad (9.7)$$

$$= \frac{p(\tilde{X} \neq Y) + 1 - p(\tilde{X} = Y)}{2} \quad (9.8)$$

$$\begin{aligned} &= \frac{p(X \neq Y) + p(\tilde{X} \neq Y)}{2} \\ &= p(X \neq Y). \end{aligned} \quad (9.9) \quad (9.10)$$

Таким образом, как показано на рис. 9.3, вероятность ошибки в канале равна расстоянию между распределениями вероятностей (\tilde{X}, X) и (\tilde{X}, Y) в следовой метрике. Это важное утверждение будет основой аналогичного утверждения для квантовой информации. Его необходимо использовать, так как в

квантовой механике не существует *прямого* аналога вероятности $p(X \neq Y)$. Мы не можем говорить о совместном распределении вероятностей величин X и Y , так как они *не существуют одновременно*. Вместо этого, мы определим динамическую меру для квантовой информации способом, похожим на только что описанный, учитывая, что в квантовом процессе важно сохранение не классической корреляции, а квантовой запутанности состояний.

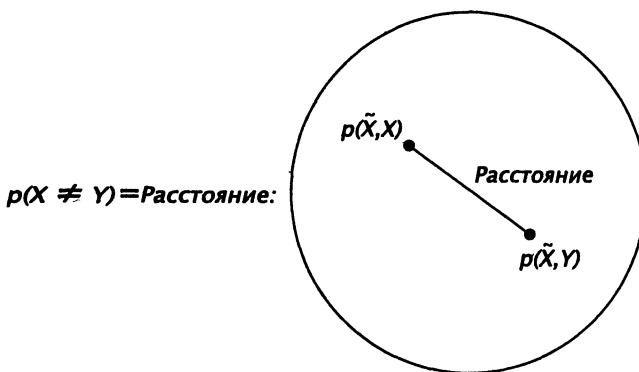


Рис. 9.3. Вероятность ошибки в канале равна расстоянию между распределениями вероятностей (\tilde{X}, X) и (\tilde{X}, Y) в следовой метрике $X \rightarrow \tilde{Y}$.

9.2 Насколько близки два квантовых состояния?

Насколько близки два квантовых состояния? Ниже мы опишем квантовые обобщения классических понятий следовой метрики и степени совпадения и детально обсудим свойства этих величин.

9.2.1 Следовая метрика

Начнем с определения *следовой метрики* для квантовых состояний ρ и σ

$$D(\rho, \sigma) \equiv \frac{1}{2} \operatorname{tr} |\rho - \sigma|, \quad (9.11)$$

где, как обычно, $|A| \equiv \sqrt{A^\dagger A}$. Заметим, что квантовая следовая метрика является обобщением классической, т. е., если состояния ρ и σ коммутируют, то в квантовой следовой метрике расстояние между ними равно расстоянию между их собственными значениями в классической следовой метрике. Действительно, если ρ и σ коммутируют, то существует некоторый ортонормированный базис $|i\rangle$, в котором они диагональны:

$$\rho = \sum_i r_i |i\rangle \langle i|; \quad \sigma = \sum_i s_i |i\rangle \langle i|. \quad (9.12)$$

Тогда

$$D(\rho, \sigma) = \frac{1}{2} \operatorname{tr} \left| \sum_i (r_i - s_i) |i\rangle\langle i| \right| \quad (9.13)$$

$$= D(r_i, s_i). \quad (9.14)$$

Упражнение 9.6. Найдите расстояние между матрицами плотности в следовой метрике

$$\frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1| \quad \text{и} \quad \frac{2}{3}|0\rangle\langle 0| + \frac{1}{3}|1\rangle\langle 1|; \quad (9.15)$$

между матрицами плотности

$$\frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1| \quad \text{и} \quad \frac{2}{3}|+\rangle\langle +| + \frac{1}{3}|-\rangle\langle -|, \quad (9.16)$$

где $|\pm\rangle \equiv (|0\rangle \pm |1\rangle)/\sqrt{2}$.

Лучше понять следовую метрику можно на примере одного кубита, представленного с помощью сферы Блоха. Пусть состояниям ρ и σ соответствуют блоховские векторы \vec{r} и \vec{s} ,

$$\rho = \frac{I + \vec{r} \cdot \vec{\sigma}}{2}, \quad \sigma = \frac{I + \vec{s} \cdot \vec{\sigma}}{2}. \quad (9.17)$$

(Здесь $\vec{\sigma}$ — вектор матриц Паули, не нужно путать его с состоянием σ .) Легко вычислить расстояние между состояниями σ и ρ в следовой метрике:

$$D(\rho, \sigma) = \frac{1}{2} \operatorname{tr} |\rho - \sigma| \quad (9.18)$$

$$= \frac{1}{4} \operatorname{tr} |(\vec{r} - \vec{s}) \cdot \vec{\sigma}|. \quad (9.19)$$

Так как $(\vec{r} - \vec{s}) \cdot \vec{\sigma}$ имеет собственные значения $\pm|\vec{r} - \vec{s}|$, след $|(\vec{r} - \vec{s}) \cdot \vec{\sigma}|$ есть $2|\vec{r} - \vec{s}|$ и

$$D(\rho, \sigma) = \frac{|\vec{r} - \vec{s}|}{2}, \quad (9.20)$$

т. е. расстояние между двумя состояниями одного кубита в следовой метрике равно половине обычного евклидового расстояния между их представлениями на сфере Блоха!

Это интуитивное геометрическое представление состояния кубита бывает полезно для понимания общих свойств следовой метрики. Свойства можно предсказать или опровергнуть, рассматривая простые примеры на блоховской сфере. Например, поворот сферы Блоха не меняет евклидового расстояния. Отсюда можно предположить, что следовая метрика может сохраняться при унитарных преобразованиях:

$$D(U\rho U^\dagger, U\sigma U^\dagger) = D(\rho, \sigma). \quad (9.21)$$

Это предположение может быть легко проверено. Мы будем часто возвращаться к сфере Блоха при рассмотрении следовой метрики.

Для понимания свойств следовой метрики лучше всего начать с доказательства формулы, которая является обобщением выражение (9.3) для классической следовой метрики:

$$D(\rho, \sigma) = \max_P \text{tr}(P(\rho - \sigma)). \quad (9.22)$$

Здесь максимум берется либо по всем проекторам P , либо по всем положительно определенным операторам $P \leq I$; формула верна в любом из этих двух случаев. Эта формула позволяет дать интересную интерпретацию следовой метрики. Напомним, что элементы POVM – это положительно определенные операторы $P \leq I$. Значит, следовая метрика равна максимальной разности вероятностей получения результата измерения, соответствующего элементу POVM P , для состояний ρ и σ .

Мы докажем формулу (9.22) для случая, когда максимум берется по всем проекторам. Для случая положительно определенных операторов $P \leq I$ доказательство проводится аналогичным образом. Доказательство основано на том факте, что разность $\rho - \sigma$ можно представить в виде $\rho - \sigma = Q - S$, где Q и S – положительно определенные операторы с ортогональными носителями (см. упр. 9.7). Следовательно, $|\rho - \sigma| = Q + S$, и, значит, $D(\rho, \sigma) = (\text{tr}(Q) + \text{tr}(S)) / 2$. Но $\text{tr}(Q - S) = \text{tr}(\rho - \sigma) = 0$, так что $\text{tr}(Q) = \text{tr}(S)$, и, следовательно, $D(\rho - \sigma) = \text{tr}(Q)$. Пусть P – проектор на носитель оператора Q . Тогда $\text{tr}(P(\rho - \sigma)) = \text{tr}(P(Q - S)) = \text{tr}(Q) = D(\rho, \sigma)$. Пусть теперь P – произвольный проектор. Тогда $\text{tr}(P(\rho, \sigma)) = \text{tr}(P(Q - S)) \leq \text{tr}(PQ) \leq \text{tr}(Q) = D(\rho, \sigma)$. Формула (9.22) доказана.

Упражнение 9.7. Покажите, что для любых состояний ρ и σ можно представить их разность в виде $\rho - \sigma = Q - S$, где Q и S – положительно определенные операторы с ортогональными носителями. (Указание. Используйте спектральное разложение $\rho - \sigma = UDU^\dagger$ и разбейте диагональную матрицу D на положительную и отрицательную части. Такое разложение нам еще пригодится.)

Существует способ рассмотрения квантовой следовой метрики, который еще больше связывает ее с классической:

Теорема 9.1. Пусть E_m – элементы POVM, а $p_m \equiv \text{tr}(\rho E_m)$ и $q_m \equiv \text{tr}(\sigma E_m)$ – вероятности получения результата измерений, обозначенного буквой m . Тогда

$$D(\rho, \sigma) = \max_{\{E_m\}} D(p_m, q_m), \quad (9.23)$$

где максимум берется по всем POVM $\{E_m\}$.

Доказательство.

Заметим, что

$$D(p_m, q_m) = \frac{1}{2} \sum_m |\text{tr}(E_m(\rho - \sigma))|. \quad (9.24)$$

Используя спектральное разложение, можно записать $\rho - \sigma = Q - S$, где Q и S — положительно определенные операторы с ортогональными носителями. Следовательно, $|\rho - \sigma| = Q + S$ и

$$|\mathrm{tr}(E_m(\rho - \sigma))| = |\mathrm{tr}(E_m(Q - S))| \quad (9.25)$$

$$\leq \mathrm{tr}(E_m(Q + S)) \quad (9.26)$$

$$\leq \mathrm{tr}(E_m|\rho - \sigma|). \quad (9.27)$$

Отсюда

$$D(p_m, q_m) \leq \frac{1}{2} \sum_m \mathrm{tr}(E_m|\rho - \sigma|) = \quad (9.28)$$

$$= \frac{1}{2} \mathrm{tr}(|\rho - \sigma|) = \quad (9.29)$$

$$= D(\rho, \sigma). \quad (9.30)$$

Здесь мы использовали условие полноты для элементов POVM, $\sum_m E_m = I$.

Равенство достигается для измерений, POVM которых содержит проекторы на носители операторов Q и S . Эти измерения дают такие распределения вероятностей, что $D(p_m, q_m) = D(\rho, \sigma)$. ■

Таким образом, если две матрицы плотности близки друг к другу в смысле следовой метрики, то при любом измерении над этими квантовыми состояниями распределения вероятностей результатов близки друг к другу в смысле классической следовой метрики. Это дает вторую интерпретацию следовой метрики для двух квантовых состояний, как наибольшего значения следовой метрики для распределений вероятностей, полученных при измерениях над этими квантовыми состояниями.

Мы использовали термин «следовая метрика», поэтому нужно проверить, выполняются ли для неё свойства метрики на пространстве матриц плотности. Очевидно, что в случае геометрической картины для одного кубита это верно. Верно ли это в более общем случае? Очевидно, что $D(\rho, \sigma) = 0$ тогда и только тогда, когда $\rho = \sigma$ и что $D(\cdot, \cdot)$ симметрична по своим аргументам. Осталось проверить, что выполняется неравенство треугольника

$$D(\rho, \tau) \leq D(\rho, \sigma) + D(\sigma, \tau). \quad (9.31)$$

Чтобы показать это, заметим, что по уравнению (9.22) существует такой проектор P , что

$$D(\rho, \tau) = \mathrm{tr}(P(\rho - \tau)) \quad (9.32)$$

$$= \mathrm{tr}(P(\rho - \sigma)) + \mathrm{tr}(P(\sigma - \tau)) \quad (9.33)$$

$$\leq D(\rho, \sigma) + D(\sigma, \tau). \quad (9.34)$$

Таким образом, следовая метрика, действительно, является метрикой.

Мы еще не знаем всех свойств следовой метрики, однако уже можем доказать несколько действительно необычных результатов, которые оказываются

полезными во многих случаях. Наиболее интересный результат заключается в том, что никакой физический процесс не может увеличить расстояние между двумя квантовыми состояниями, как это показано на рис. 9.4. Сформулируем это более точно в виде следующей теоремы:

Теорема 9.2 (сохраняющие след квантовые преобразования являются сжимающими). Пусть \mathcal{E} — сохраняющие след квантовые преобразования, а ρ и σ — матрицы плотности. Тогда

$$D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \leq D(\rho, \sigma). \quad (9.35)$$

Доказательство.

Используя спектральное разложение, запишем $\rho - \sigma = Q - S$, где Q и S — положительно определенные матрицы с ортогональными носителями. Пусть P — проектор, такой, что $D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) = \text{tr}[P(\mathcal{E}(\rho) - \mathcal{E}(\sigma))]$. Заметим, что $\text{tr}(Q) - \text{tr}(S) = \text{tr}(\rho) - \text{tr}(\sigma) = 0$, $\text{tr}(Q) = \text{tr}(S)$ и поэтому $\text{tr}(\mathcal{E}(Q)) = \text{tr}(\mathcal{E}(S))$. Используя это, получим

$$D(\rho, \sigma) = \frac{1}{2} \text{tr} |\rho - \sigma| \quad (9.36)$$

$$= \frac{1}{2} \text{tr} |Q - S| \quad (9.37)$$

$$= \frac{1}{2} \text{tr}(Q) + \frac{1}{2} \text{tr}(S) \quad (9.38)$$

$$= \frac{1}{2} \text{tr}(\mathcal{E}(Q)) + \frac{1}{2} \text{tr}(\mathcal{E}(S)) \quad (9.39)$$

$$= \text{tr}(\mathcal{E}(Q)) \quad (9.40)$$

$$\geq \text{tr}(P\mathcal{E}(Q)) \quad (9.41)$$

$$\geq \text{tr}(P(\mathcal{E}(Q) - \mathcal{E}(S))) \quad (9.42)$$

$$= \text{tr}(P(\mathcal{E}(\rho) - \mathcal{E}(\sigma))) \quad (9.43)$$

$$= D(\mathcal{E}(\rho) - \mathcal{E}(\sigma)). \quad (9.44)$$

Теорема доказана. ■

Существует важный частный случай этой теоремы, который можно понять с помощью следующей аналогии. Представьте, что вам показывают две различные картины. Если вы достаточно хорошо видите, вам несложно отличить их друг от друга. С другой стороны, если закрыть большие части этих картин, отличить их будет сложнее. Это проиллюстрировано на рис. 9.5. Аналогично, если мы «закроем» части двух квантовых состояний, расстояние между ними не увеличится. Чтобы это доказать, напомним, что взятие частичного следа является сохраняющим след квантовым преобразованием. Согласно теореме 9.2, для состояний ρ^{AB} и σ^{AB} составной квантовой системы AB расстояние между $\rho^A = \text{tr}_B(\rho^{AB})$ и $\sigma^A = \text{tr}_B(\sigma^{AB})$ не больше расстояния между ρ^{AB} и σ^{AB} ,

$$D(\rho^A, \sigma^A) \leq D(\rho^{AB}, \sigma^{AB}). \quad (9.45)$$

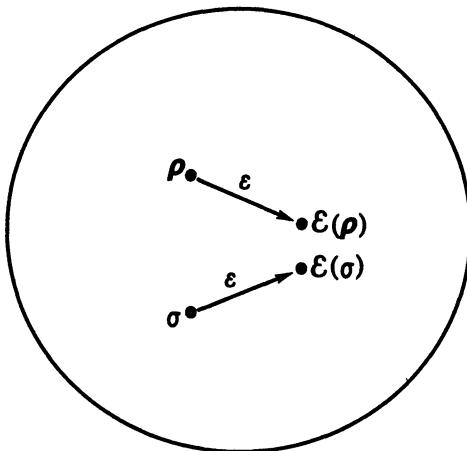


Рис. 9.4. Сохраняющие след квантовые преобразования являются сжимающими в пространстве матриц плотности

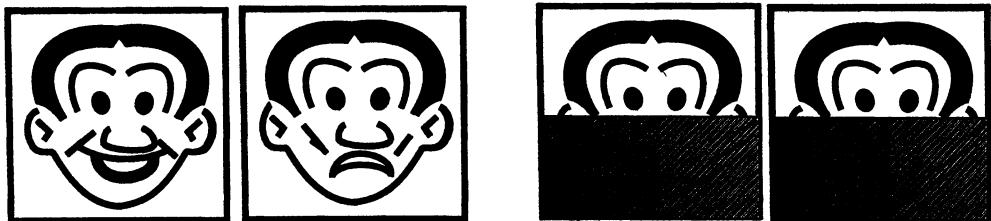


Рис. 9.5. Объекты менее различимы, если доступна только часть информации о них.

Во многих случаях нужно оценить следовую метрику для смеси состояний. В этом может помочь следующая теорема.

Теорема 9.3 (сильная выпуклость следовой метрики). Пусть $\{p_i\}$ и $\{q_i\}$ — распределения вероятностей, с одинаковым набором индексов, а ρ_i и σ_i — матрицы плотности с тем же набором индексов. Тогда

$$D \left(\sum_i p_i \rho_i, \sum_i q_i \sigma_i \right) \leq D(p_i, q_i) + \sum_i p_i D(\rho_i, \sigma_i), \quad (9.46)$$

где $D(p_i, q_i)$ — классическая следовая метрика для распределений вероятностей $\{p_i\}$ и $\{q_i\}$.

Это свойство используется при доказательстве выпуклости следовой метрики, поэтому мы называем его *сильной выпуклостью*.

Доказательство.

В соответствии с формулой 9.22 существует проектор P , такой, что

$$D\left(\sum_i p_i \rho_i, \sum_i q_i \sigma_i\right) = \sum_i p_i \operatorname{tr}(P \rho_i) - \sum_i q_i \operatorname{tr}(P \sigma_i) \quad (9.47)$$

$$= \sum_i p_i \operatorname{tr}(P(\rho_i - \sigma_i)) + \sum_i (p_i - q_i) \operatorname{tr}(P \sigma_i) \quad (9.48)$$

$$\leq \sum_i p_i D(\rho_i, \sigma_i) + D(p_i, q_i), \quad (9.49)$$

где $D(p_i, q_i)$ — классическая следовая метрика для распределений вероятностей $\{p_i\}$ и $\{q_i\}$. Формула (9.22) использована в последней строке. ■

Частным случаем этой теоремы является тот факт, что следовая метрика является *совместно выпуклой* по своим аргументам:

$$D\left(\sum_i p_i \rho_i, \sum_i p_i \sigma_i\right) \leq \sum_i p_i D(\rho_i, \sigma_i). \quad (9.50)$$

Упражнение 9.8 (выпуклость следовой метрики). Покажите, что следовая метрика выпукла по своему первому аргументу:

$$D\left(\sum_i p_i \rho_i, \sigma\right) \leq \sum_i p_i D(\rho_i, \sigma). \quad (9.51)$$

Так как следовая метрика симметрична, из выпуклости по первому аргументу следует выпуклость по второму аргументу.

Упражнение 9.9 (существование неподвижной точки). Теорема Шаудера о неподвижной точке — классический математический результат, заключающийся в том, что любое непрерывное отображение в себя выпуклого компактного множества в гильбертовом пространстве имеет неподвижную точку. Используя эту теорему, докажите, что любое сохраняющее след квантовое преобразование \mathcal{E} имеет неподвижную точку, т. е., что существует ρ , такое, что $\mathcal{E}(\rho) = \rho$.

Упражнение 9.10. Пусть сохраняющее след квантовое преобразование \mathcal{E} является строго сжимающим, т. е. для любых ρ и σ выполняется неравенство $D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) < D(\rho, \sigma)$. Докажите, что \mathcal{E} имеет единственную неподвижную точку.

Упражнение 9.11. Пусть \mathcal{E} — сохраняющее след квантовое преобразование, для которого существуют матрица плотности ρ_0 и сохраняющее след квантовое преобразование \mathcal{E}' , такие, что

$$\mathcal{E}(\rho) = p \rho_0 + (1-p) \mathcal{E}'(\rho) \quad (9.52)$$

для некоторого $0 < p \leq 1$. Это означает, что входное состояние ρ с вероятностью p заменяется на состояние ρ_0 , а с вероятностью $1-p$ изменяется с помощью

преобразования \mathcal{E}' . Используя совместную выпуклость следовой метрики, покажите, что преобразование \mathcal{E} является строго сжимающим и, следовательно, имеет единственную неподвижную точку.

Упражнение 9.12. Рассмотрим деполяризующий канал, введенный в подразд. 8.3.4, $\mathcal{E}(\rho) = pI/2 + (1-p)\rho$. Для произвольных ρ и σ найдите $D(\mathcal{E}(\rho), \mathcal{E}(\sigma))$, используя блоховское представление, и явно докажите, что отображение \mathcal{E} является строго сжимающим, т. е. что $D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) < D(\rho, \sigma)$.

Упражнение 9.13. Покажите, что канал с классической ошибкой (подразд. 8.3.3) является сжимающим, но не является строго сжимающим. Найдите множество неподвижных точек для этого канала.

9.2.2 Степень совпадения

Второй мерой различия квантовых состояний является *степень совпадения*. Степень совпадения не является метрикой для матриц плотности, но мы покажем, что из нее можно получить полезную метрику. Мы дадим здесь определение и приведем основные свойства степени совпадения. Для состояний ρ и σ степень совпадения определяется как

$$F(\rho, \sigma) = \text{tr} \sqrt{\rho^{1/2} \sigma \rho^{1/2}}. \quad (9.53)$$

С первого взгляда не очевидно, что это полезная мера различия состояний ρ и σ . Она даже не выглядит симметричной! Мы покажем, что степень совпадения симметрична по своим аргументам и имеет другие свойства, которые характерны для хорошей меры различия.

Существуют два важных случая, в которых степень совпадения можно записать в более явном виде. Во-первых, если ρ и σ коммутируют, т. е. они диагональны в некотором ортонормированном базисе $|i\rangle$:

$$\rho = \sum_i r_i |i\rangle\langle i|, \quad \sigma = \sum_i s_i |i\rangle\langle i|. \quad (9.54)$$

В этом случае

$$F(\rho, \sigma) = \text{tr} \sqrt{\sum_i r_i s_i |i\rangle\langle i|} \quad (9.55)$$

$$= \text{tr} \left(\sum_i \sqrt{r_i s_i} |i\rangle\langle i| \right) \quad (9.56)$$

$$= \sum_i \sqrt{r_i s_i} \quad (9.57)$$

$$= F(r_i, s_i), \quad (9.58)$$

т. е. если состояния ρ и σ коммутируют, квантовая степень совпадения $F(\rho, \sigma)$ равна классической степени совпадения $F(r_i, s_i)$ для распределений их собственных значений r_i и s_i .

Во-вторых, вычислим степень совпадения для чистого состояния $|\psi\rangle$ и произвольного состояния ρ . Из формулы (9.53) мы видим, что

$$F(|\psi\rangle, \sigma) = \text{tr} \sqrt{\langle\psi|\rho|\psi\rangle} |\psi\rangle\langle\psi| \quad (9.59)$$

$$= \sqrt{\langle\psi|\rho|\psi\rangle}, \quad (9.60)$$

т. е. степень совпадения равна квадратному корню из перекрытия состояний $|\psi\rangle$ и ρ . Этот важный результат мы будем часто использовать.

В случае одного кубита можно явно вычислить расстояние между его состояниями в следовой метрике и дать его геометрическую интерпретацию (половина евклидового расстояния между соответствующими точками на сфере Блоха). К сожалению, не известно подобной геометрической интерпретации для степени совпадения состояний кубита.

Тем не менее, степень совпадения обладает многими свойствами следовой метрики. Например, она инвариантна относительно унитарных преобразований:

$$F(U\rho U^\dagger, U\sigma U^\dagger) = F(\rho, \sigma). \quad (9.61)$$

Упражнение 9.14 (инвариантность степени совпадения относительно унитарных преобразований). Докажите равенство (9.61), используя тот факт, что для любого положительного оператора A выполняется равенство $\sqrt{UAU^\dagger} = U\sqrt{AU^\dagger}$.

Существует также полезное свойство степени совпадения, аналогичное свойству (9.22) для следовой метрики.

Теорема 9.4 (теорема Ульмана). Пусть ρ и σ — состояния квантовой системы Q . Введем вторую систему R , которая является копией Q . Тогда

$$F(\rho, \sigma) = \max_{|\psi\rangle, |\varphi\rangle} |\langle\psi|\varphi\rangle|, \quad (9.62)$$

где максимум берется по всем чистым состояниям $|\psi\rangle$ и $|\varphi\rangle$ системы QR , до которых можно расширить ρ и σ

Для доказательства теоремы Ульмана нам потребуется простая лемма.

Лемма 9.5. Пусть A — произвольный оператор, а U — унитарный оператор. Тогда

$$|\text{tr}(AU)| \leq \text{tr}|A|, \quad (9.63)$$

причем равенство имеет место при $U = V^\dagger$, где $A = |A|V$ — полярное разложение оператора A .

Доказательство.

Для случая равенства доказательство очевидно. Заметим, что

$$|\text{tr}(AU)| = |\text{tr}(|A|VU)| = \left| \text{tr}(|A|^{1/2}|A|^{1/2}VU) \right|. \quad (9.64)$$

Применив неравенство Коши–Шварца для скалярного произведения Гильберта–Шмидта, получим

$$|\text{tr}(AU)| \leq \sqrt{\text{tr}|A|\text{tr}(U^\dagger V^\dagger |A| VU)} = \text{tr}|A|. \quad (9.65)$$

Лемма доказана. ■

Доказательство.

(Теорема Ульмана)

Зафиксируем ортонормированные базисы $|i_R\rangle$ и $|i_Q\rangle$ в системах R и Q . Так как R и Q имеют одинаковую размерность, можно считать, что индекс i в них имеет одинаковый набор возможных значений. Введем $|m\rangle \equiv \sum_i |i_R\rangle|i_Q\rangle$. Пусть $|\psi\rangle$ — некоторое расширение состояния ρ . Тогда из разложения Шмидта легко получить

$$|\psi\rangle = (U_R \otimes \sqrt{\rho} U_Q)|m\rangle, \quad (9.66)$$

где U_R и U_Q — некоторые унитарные операторы в системах R и Q . Аналогично, если $|\varphi\rangle$ — некоторое расширение состояния σ , то существуют унитарные операторы V_R и V_Q , такие, что

$$|\varphi\rangle = (V_R \otimes \sqrt{\sigma} V_Q)|m\rangle. \quad (9.67)$$

Взяв скалярное произведение, получим

$$|\langle\psi||\varphi\rangle| = \left| \langle m | \left(U_R^\dagger V_R \otimes U_Q^\dagger \sqrt{\rho} \sqrt{\sigma} V_Q \right) | m \rangle \right|. \quad (9.68)$$

Используя результат упражнения 9.16, мы видим, что

$$|\langle\psi||\varphi\rangle| = \left| \text{tr} \left(V_R^\dagger U_R U_Q^\dagger \sqrt{\rho} \sqrt{\sigma} V_Q \right) \right|. \quad (9.69)$$

Введя обозначение $U \equiv V_Q V_R^\dagger U_R U_Q^\dagger$, запишем уравнение:

$$|\langle\psi||\varphi\rangle| = |\text{tr}(\sqrt{\rho}\sqrt{\sigma}U)|. \quad (9.70)$$

Согласно лемме 9.5,

$$|\langle\psi||\varphi\rangle| \leq \text{tr} |\sqrt{\rho}\sqrt{\sigma}| = \text{tr} \sqrt{\rho^{1/2}\sigma\rho^{1/2}}. \quad (9.71)$$

Чтобы показать, что равенство может выполняться, подставим вместо $\sqrt{\rho}\sqrt{\sigma}$ его полярное разложение $|\sqrt{\rho}\sqrt{\sigma}|V$. Положим $U_Q = U_R = V_R = I$, а $V_Q = V^\dagger$. Легко показать, что при этих условиях достигается равенство. ■

Упражнение 9.15. Покажите, что

$$F(\rho, \sigma) = \max_{|\varphi\rangle} |\langle\psi||\varphi\rangle|, \quad (9.72)$$

где $|\psi\rangle$ — некоторое *фиксированное* расширение ρ , а максимум берется по всем расширениям σ до чистого состояния.

Упражнение 9.16. Скалярное произведение Гильберта–Шмидта и запутанность. Предложим, что R и Q — две квантовые системы с одним гильбертовом пространством. Пусть $|i_R\rangle$ и $|i_Q\rangle$ — ортонормированные базисы для R и Q . Пусть A — оператор, действующий на R , а B — оператор, действующий на Q . Введем $|m\rangle \equiv \sum_i |i_R\rangle|i_Q\rangle$. Покажите, что

$$\text{tr}(A^\dagger B) = \langle m | (A \otimes B) | m \rangle, \quad (9.73)$$

где с левой стороны стоит произведение *матриц*, причем подразумевается, что матричные элементы A вычисляются в базисе $|i_R\rangle$, а матричные элементы B — в базисе $|i_Q\rangle$.

В отличие от выражение (9.53) формула Ульмана (9.62) не позволяет в явном виде вычислять степень совпадения. Однако, во многих случаях свойства степени совпадения легче получать из формулы Ульмана. Например, из нее видно, что степень совпадения симметрична по своим аргументам: $F(\rho, \sigma) = F(\sigma, \rho)$, и что она всегда заключена между 0 и 1: $0 \leq F(\rho, \sigma) \leq 1$. Если $\rho = \sigma$, из формулы Ульмана очевидно, что $F(\rho, \sigma) = 1$. Если $\rho \neq \sigma$, то для любых расширений ρ и σ до чистых состояний $|\psi\rangle$ и $|\varphi\rangle$ имеем $|\psi\rangle \neq |\varphi\rangle$ и, значит, $F(\rho, \sigma) < 1$. С другой стороны, из формулы (9.53) также можно получить некоторые полезные свойства степени совпадения. Например, что $F(\rho, \sigma) = 0$ тогда и только тогда, когда носители ρ и σ ортогональны. Интуитивно понятно, что в этом случае состояния идеально различимы и можно ожидать, что степень совпадения достигает минимума. Итак, степень совпадения симметрична по своим аргументам и $0 \leq F(\rho, \sigma) \leq 1$, причем равенство нулю достигается тогда и только тогда, когда носители ρ и σ ортогональны, а равенство единице — тогда и только тогда, когда $\rho = \sigma$.

Мы видели, что квантовую следовую метрику можно связать с классической, рассматривая распределения вероятностей исходов измерений. Подобным образом можно показать, что

$$F(\rho, \sigma) = \min_{\{E_m\}} F(p_m, q_m), \quad (9.74)$$

где минимум берется по всем POVM $\{E_m\}$, а $p_m \equiv \text{tr}(\rho E_m)$ и $q_m \equiv \text{tr}(\sigma E_m)$ — распределения вероятностей для ρ и σ , соответствующие POVM $\{E_m\}$. Чтобы доказать это, заметим, что

$$F(\rho, \sigma) = \text{tr}(\sqrt{\rho}\sqrt{\sigma}U) = \quad (9.75)$$

$$= \sum_m \text{tr}(\sqrt{\rho}\sqrt{E_m}\sqrt{E_m}\sqrt{\sigma}U). \quad (9.76)$$

Неравенство Коши–Шварца приводит к

$$F(\rho, \sigma) \leq \sum_m \sqrt{\text{tr}(\rho E_m) \text{tr}(\sigma E_m)} \quad (9.77)$$

$$= F(p_m, q_m). \quad (9.78)$$

Отсюда

$$F(\rho, \sigma) \leq \min_{\{E_m\}} F(p_m, q_m). \quad (9.79)$$

Чтобы доказать равенство, нужно найти такой POVM $\{E_m\}$, для которого неравенство Коши–Шварца обращается в равенство для каждого члена суммы, т. е. $\sqrt{E_m}\sqrt{\rho} = \alpha_m\sqrt{E_m}\sqrt{\sigma}U$ для некоторого набора комплексных чисел α_m . Но $\sqrt{\rho}\sqrt{\sigma}U = \sqrt{\rho^{1/2}\sigma\rho^{1/2}}$, поэтому для невырожденного ρ

$$\sqrt{\sigma}U = \rho^{-1/2}\sqrt{\rho^{1/2}\sigma\rho^{1/2}}. \quad (9.80)$$

После подстановки получим, что равенство имеет место при

$$\sqrt{E_m}(I - \alpha_m M) = 0, \quad (9.81)$$

где $M \equiv \rho^{-1/2} \sqrt{\rho^{1/2} \sigma \rho^{1/2}} \rho^{-1/2}$. Представим M в виде спектрального разложения $M = \sum_m \beta_m |m\rangle\langle m|$ и выберем $E_m = |m\rangle\langle m|$, а $\alpha_m = 1/\beta_m$. Равенство для вырожденных ρ следует из непрерывности.

Мы доказали три важных свойства следовой метрики, а именно что она является метрикой, не увеличивается при квантовых преобразованиях, и что она обладает свойствами сильной выпуклости. Следует заметить, что аналогичные свойства выполняются и для степени совпадения, причем их доказательства существенно отличаются от соответствующих доказательств для следовой метрики, поэтому их стоит рассмотреть детально.

Степень совпадения не является метрикой. Однако, существует простой способ превратить ее в метрику. Основная идея ясна из рис. 9.6. Угол между точками на сфере является метрикой. Для квантового случая теорема Ульмана утверждает, что степень совпадения для двух состояний равна максимальному скалярному произведению их расширений до чистого состояния. Это подсказывает нам определить угол между состояниями ρ и σ как

$$A(\rho, \sigma) \equiv \arccos F(\rho, \sigma). \quad (9.82)$$

Очевидно, что этот угол неотрицателен, симметричен по своим аргументам и равен нулю тогда и только тогда, когда $\rho = \sigma$. То, что угол является метрикой, можно увидеть, если доказать, что для него выполняется неравенство треугольника.

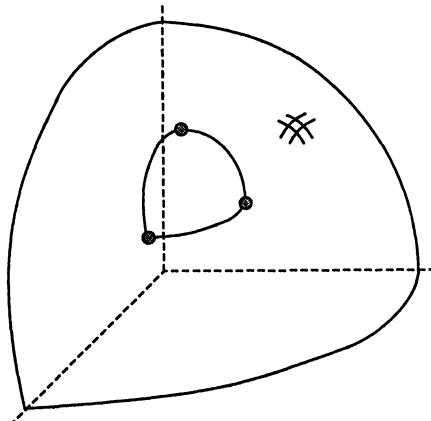


Рис. 9.6. Угол между двумя точками на поверхности единичной сферы является метрикой.

Мы докажем неравенство треугольника, используя теорему Ульмана и несколько очевидных свойств трехмерных векторов. Пусть $|\varphi\rangle$ — расширение σ .

Выберем такие расширения для $|\psi\rangle$ и $|\gamma\rangle$ для ρ и τ , что

$$F(\rho, \sigma) = \langle\psi|\varphi\rangle, \quad (9.83)$$

$$F(\sigma, \tau) = \langle\varphi|\gamma\rangle, \quad (9.84)$$

а $\langle\psi|\gamma\rangle$ положительно (это всегда можно сделать, умножив $|\psi\rangle$, $|\varphi\rangle$ и $|\gamma\rangle$ на соответствующие фазовые множители). Из рис. 9.6 очевидно, что

$$\arccos(\langle\psi|\gamma\rangle) \leq A(\rho, \sigma) + A(\sigma, \tau). \quad (9.85)$$

Согласно теореме Ульмана, $F(\rho, \tau) \geq \langle\psi|\gamma\rangle$, поэтому $A(\rho, \tau) \leq \arccos(\langle\psi|\gamma\rangle)$. Объединяя это неравенство с предыдущим, получим неравенство треугольника

$$A(\rho, \tau) \leq A(\rho, \sigma) + A(\sigma, \tau). \quad (9.86)$$

Упражнение 9.17. Покажите, что $0 \leq A(\rho, \sigma) \leq \pi/2$, причем первое неравенство превращается в равенство тогда и только тогда, когда $\rho = \sigma$.

Качественно степень совпадения ведет себя как «перевернутая» следовая метрика, она меньше, если два состояния более различимы, и больше, если они менее различимы. Следовательно, мы не должны ожидать, что степень совпадения не будет увеличиваться при квантовых преобразованиях подобно следовой метрике. Наоборот, она не будет уменьшаться. Мы назовем это свойство *монотонностью* степени совпадения под действием квантовых преобразований.

Теорема 9.6 (монотонность степени совпадения). Пусть \mathcal{E} — сохраняющее след квантовое преобразование, а ρ и σ — матрицы плотности. Тогда

$$F(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \geq F(\rho, \sigma). \quad (9.87)$$

Доказательство.

Пусть $|\psi\rangle$ и $|\varphi\rangle$ — расширения ρ и σ в совместной системе RQ , такие, что $F(\rho, \sigma) = |\langle\psi|\varphi\rangle|$. Введем модель среды E для преобразования \mathcal{E} , которая вначале находится в состоянии $|0\rangle$, а затем взаимодействует с системой Q с помощью унитарного оператора U . Заметим, что состояние $U|\psi\rangle|0\rangle$ является расширением состояния $\mathcal{E}(\rho)$, а $U|\varphi\rangle|0\rangle$ — расширением состояния $\mathcal{E}(\sigma)$. Согласно теореме Ульмана,

$$F(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \geq |\langle\psi|\langle 0|U^\dagger U|\varphi\rangle|0\rangle| \quad (9.88)$$

$$= |\langle\psi|\varphi\rangle| \quad (9.89)$$

$$= F(\rho, \sigma). \quad (9.90)$$

Теорема доказана. ■

Упражнение 9.18 (сжимаемость угла). Пусть \mathcal{E} — сохраняющее след квантовое преобразование. Покажите, что

$$A(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \leq A(\rho, \sigma). \quad (9.91)$$

Мы закончим изучение элементарных свойств степени совпадения, доказав с помощью теоремы Ульмана свойство, аналогичное свойству сильной выпуклости для следовой метрики.

Теорема 9.7 (сильная вогнутость степени совпадения). Пусть p_i и q_i — распределения вероятностей с одинаковым набором индексов, а ρ_i и σ_i — матрицы плотности с тем же набором индексов. Тогда

$$F\left(\sum_i p_i \rho_i, \sum_i q_i \sigma_i\right) \geq \sum_i \sqrt{p_i q_i} F(\rho_i, \sigma_i). \quad (9.92)$$

Неудивительно, что этот результат можно использовать для доказательства вогнутости, поэтому мы называем это свойство *сильной вогнутостью* степени совпадения. Оно не вполне аналогично сильной выпуклости следовой метрики, однако общая суть этих двух свойств позволяет нам дать им похожие названия.

Доказательство.

Пусть $|\psi_i\rangle$ и $|\varphi_i\rangle$ — расширения состояний ρ_i и σ_i , такие, что $F(\rho_i, \sigma_i) = \langle\psi_i|\varphi_i\rangle$. Введем дополнительную систему с ортонормированными базисными состояниями $|i\rangle$, соответствующими индексам i в распределениях вероятностей. Определим

$$|\psi\rangle \equiv \sum_i \sqrt{p_i} |\psi_i\rangle |i\rangle; \quad |\varphi\rangle \equiv \sum_i \sqrt{q_i} |\varphi_i\rangle |i\rangle. \quad (9.93)$$

Заметим, что $|\psi\rangle$ является расширением состояния матрицы плотности $\sum_i p_i \rho_i$, а $|\varphi\rangle$ — расширением состояния $\sum_i q_i \sigma_i$. Поэтому, согласно теореме Ульмана,

$$F\left(\sum_i p_i \rho_i, \sum_i q_i \sigma_i\right) \geq |\langle\psi|\varphi\rangle| = \sum_i \sqrt{p_i q_i} \langle\psi_i|\varphi_i\rangle = \sum_i \sqrt{p_i q_i} F(\rho_i, \sigma_i). \quad (9.94)$$

Теорема доказана. ■

Упражнение 9.19 (совместная вогнутость степени совпадения). Докажите, что степень совпадения обладает свойством *совместной вогнутости*:

$$F\left(\sum_i p_i \rho_i, \sum_i \rho_i \sigma_i\right) \geq \sum_i p_i F(\rho_i, \sigma_i). \quad (9.95)$$

Упражнение 9.20 (вогнутость степени совпадения). Докажите, что степень совпадения вогнута по первому аргументу:

$$F\left(\sum_i p_i \rho_i, \sigma\right) \geq \sum_i p_i F(\rho_i, \sigma). \quad (9.96)$$

Вогнутость по второму аргументу следует из симметрии степени совпадения.

9.2.3 Связь между мерами различия

Следовая метрика и степень совпадения тесно связаны друг с другом, несмотря на их очень разную форму. Во многих случаях они качественно могут рассматриваться как *эквивалентные* меры различия. Мы получим более точные соотношения между следовой метрикой и степенью совпадения.

В случае чистых состояний следовая метрика и степень совпадения полностью эквивалентны. Чтобы это увидеть, рассмотрим следовую метрику для двух чистых состояний $|a\rangle$ и $|b\rangle$. Используя ортогонализацию Грама–Шмидта, можно найти ортонормированные состояния $|0\rangle$ и $|1\rangle$, такие, что $|a\rangle = |0\rangle$, а $|b\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$. Заметим, что $F(|a\rangle, |b\rangle) = |\cos\theta|$. Далее,

$$D(|a\rangle, |b\rangle) = \frac{1}{2} \text{tr} \left| \begin{bmatrix} 1 - \cos^2\theta & -\cos\theta \sin\theta \\ -\cos\theta \sin\theta & -\sin^2\theta \end{bmatrix} \right| \quad (9.97)$$

$$= |\sin\theta| \quad (9.98)$$

$$= \sqrt{1 - F(|a\rangle, |b\rangle)^2}. \quad (9.99)$$

Мы видим, что следовая метрика для двух чистых состояний является функцией степени совпадения этих состояний, и, наоборот, степень совпадения можно выразить через следовую метрику. Эта взаимосвязь на уровне чистых состояний может быть использована для нахождения взаимосвязи для смешанных состояний. Пусть ρ и σ — два произвольных квантовых состояния, а $|\psi\rangle$ и $|\varphi\rangle$ — их расширения, выбранные так, что $F(\rho, \sigma) = |\langle\psi||\varphi\rangle| = F(|\psi\rangle, |\varphi\rangle)$. Вспоминая, что следовая метрика не увеличивается при взятии частичного следа, мы видим, что

$$D(\rho, \sigma) \leq D(|\psi\rangle, |\varphi\rangle) \quad (9.100)$$

$$= \sqrt{1 - F(\rho, \sigma)^2}. \quad (9.101)$$

Следовательно, если степень совпадения двух состояний близка к единице, то эти состояния близки друг к другу и в смысле следовой метрики. Справедливо и обратное утверждение. Чтобы показать это, рассмотрим POVM $\{E_m\}$, такой, что

$$F(\rho, \sigma) = \sum_m \sqrt{p_m q_m}, \quad (9.102)$$

где $p_m \equiv \text{tr}(\rho E_m)$ и $q_m \equiv \text{tr}(\sigma E_m)$ — вероятности получения результата m при измерениях над состояниями ρ и σ соответственно. Заметим, что

$$\sum_m (\sqrt{p_m} - \sqrt{q_m})^2 = \sum_m p_m + \sum_m q_m - 2F(\rho, \sigma) \quad (9.103)$$

$$= 2(1 - F(\rho, \sigma)). \quad (9.104)$$

Кроме того, $|\sqrt{p_m} - \sqrt{q_m}| \leq |\sqrt{p_m} + \sqrt{q_m}|$, поэтому

$$\sum_m (\sqrt{p_m} - \sqrt{q_m})^2 \leq \sum_m |\sqrt{p_m} - \sqrt{q_m}| |\sqrt{p_m} + \sqrt{q_m}| \quad (9.105)$$

$$= \sum_m |p_m - q_m| \quad (9.106)$$

$$= 2D(p_m, q_m) \quad (9.107)$$

$$\leq 2D(\rho, \sigma). \quad (9.108)$$

Сравнив (9.104) и (9.108), получим

$$1 - F(\rho, \sigma) \leq D(\rho, \sigma). \quad (9.109)$$

Итак, мы имеем

$$1 - F(\rho, \sigma) \leq D(\rho, \sigma) \leq \sqrt{1 - F(\rho, \sigma)^2}. \quad (9.110)$$

Мы показали, что следовая метрика и степень совпадения являются качественно эквивалентными мерами различных квантовых состояний. И действительно, во многих случаях неважно какую из этих величин использовать. Имея результат, выраженный через одну из них, можно получить эквивалентный результат выраженный через другую.

Упражнение 9.21. Для чистого и смешанного состояний можно сформулировать более сильное утверждение, чем неравенство (9.110). Докажите, что следовая метрика и степень совпадения в этом случае связаны следующим образом:

$$1 - F(|\psi\rangle, \sigma)^2 \leq D(|\psi\rangle, \sigma). \quad (9.111)$$

9.3 Насколько квантовый канал сохраняет информацию?

Друзья приходят и уходят, враги накапливаются.

Закон Джонса (приписывается Томасу Джонсу)

Насколько квантовый канал сохраняет информацию? Точнее, пусть квантовая система находится в состоянии $|\psi\rangle$, и происходит некоторый процесс, переводящий ее в состояние $\mathcal{E}(|\psi\rangle\langle\psi|)$. Такая картина довольно часто наблюдается в квантовых вычислениях. Например, $|\psi\rangle$ — это начальное состояние памяти квантового компьютера, а \mathcal{E} описывает динамические изменения состояния памяти из-за шумовых процессов, возникающих вследствие взаимодействия

с внешней средой. Другой пример — квантовый канал для передачи состояния $|\psi\rangle$ из одного места в другое. Канал всегда не идеален, его действие описывается квантовым преобразованием \mathcal{E} .

Очевидный способ количественного описания того, насколько состояние $|\psi\rangle$ сохраняется в канале — это использовать статистические меры различия, введенные в предыдущем разделе. Например, мы можем вычислить степень совпадения начального состояния $|\psi\rangle$ с конечным $\mathcal{E}(|\psi\rangle\langle\psi|)$. Для случая деполяризующего канала получаем

$$F(|\psi\rangle, \mathcal{E}(|\psi\rangle\langle\psi|)) = \sqrt{\langle\psi| \left(p \frac{I}{2} + (1-p)|\psi\rangle\langle\psi| \right) |\psi\rangle} \quad (9.112)$$

$$= \sqrt{1 - \frac{p}{2}}. \quad (9.113)$$

Этот результат интуитивно понятен: чем больше вероятность деполяризации p , тем меньше степень совпадения начального состояния с конечным. Если величина p очень мала, то степень совпадения близка к единице и состояние $\mathcal{E}(\rho)$ практически неотличимо от начального состояния $|\psi\rangle$.

Нет особых причин для использования в этом примере степени совпадения. С тем же успехом мы могли бы использовать следовую метрику. Однако, далее в этой главе мы ограничимся степенью совпадения и связанными с ней величинами. На основе свойств следовой метрики, которые мы получили в предыдущем разделе, в большинстве случаев несложно провести параллельное рассмотрение. Однако, оказывается, что вычисления удобнее проводить со степенью совпадения, поэтому мы и будем использовать ее.

Мера сохранения информации — степень совпадения $F(|\psi\rangle, \mathcal{E}(|\psi\rangle\langle\psi|))$ — имеет некоторые недостатки, которые нужно устраниć Для реальной памяти квантового компьютера или для квантового канала передачи данных нам заранее не известно начальное состояние $|\psi\rangle$. Однако, можно вычислить наихудшее поведение системы, минимизируя степень совпадения по всем возможным начальным состояниям:

$$F_{\min} \equiv \min_{|\psi\rangle} F(|\psi\rangle, \mathcal{E}(|\psi\rangle\langle\psi|)). \quad (9.114)$$

Например, для деполяризующего канала $F_{\min} = \sqrt{1 - p/2}$, так как степень совпадения в этом случае не зависит от начального состояния $|\psi\rangle$. Более интересный пример — канал с затуханием фазы,

$$\mathcal{E}(\rho) = p\rho + (1-p)Z\rho Z. \quad (9.115)$$

Для такого канала степень совпадения равна

$$F(|\psi\rangle, \mathcal{E}(|\psi\rangle\langle\psi|)) = \sqrt{\langle\psi|(|\psi\rangle\langle\psi| + (1-p)Z|\psi\rangle\langle\psi|Z)|\psi\rangle} \quad (9.116)$$

$$= \sqrt{p + (1-p)\langle\psi|Z|\psi\rangle^2}. \quad (9.117)$$

Второе слагаемое под знаком корня неотрицательно и равно нулю при $|\psi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. Следовательно, для канала с затуханием фазы минимальная степень совпадения равна

$$F_{\min}(\mathcal{E}) = \sqrt{1 - p}. \quad (9.118)$$

Вам может показаться странным, почему в определении F_{\min} минимум берется только по *чистым состояниям*. В конце концов квантовая система не может ли находиться вначале в смешанном состоянии ρ ? Например, память квантового компьютера может быть запутана с другими его частями, и, следовательно, ее начальное состояние будет смешанным. К счастью, совместная вогнутость степени совпадения позволяет нам показать, что учет смешанных состояний не влияет на F_{\min} . Чтобы это увидеть, предположим, что начальное состояние системы $\rho = \sum_i \lambda_i |i\rangle\langle i|$. Тогда мы имеем

$$F(\rho, \mathcal{E}(\rho)) = F\left(\sum_i \lambda_i |i\rangle\langle i|, \sum_i \lambda_i \mathcal{E}(|i\rangle\langle i|)\right) \quad (9.119)$$

$$\geq \sum_i \lambda_i F(|i\rangle, \mathcal{E}(|i\rangle\langle i|)). \quad (9.120)$$

Отсюда следует, что, по крайней мере, для одного из состояний $|i\rangle$

$$F(\rho, \mathcal{E}(\rho)) \geq F(|i\rangle, \mathcal{E}(|i\rangle\langle i|)), \quad (9.121)$$

и, следовательно, $F(\rho, \mathcal{E}(\rho)) \geq F_{\min}$.

Конечно, для нас представляет интерес защита квантовых состояний не только при передаче их по каналу, но и при вычислениях с ними. Пусть, например, мы пытаемся реализовать элемент, описываемый унитарным оператором U . Как отмечено в последней главе, такие реальные квантовые схемы подвержены шуму (к счастью, не слишком сильному), так что элемент описывается сохраняющим след преобразованием \mathcal{E} . Естественной мерой того, насколько хорошо действует элемент, является *степень совпадения для элемента*:

$$F(U, \mathcal{E}) = \min_{|\psi\rangle} F(U|\psi\rangle, \mathcal{E}(|\psi\rangle\langle\psi|)). \quad (9.122)$$

Пусть, например, мы пытаемся реализовать однокубитовый элемент NOT, но вместо этого получаем элемент, подверженный шуму, $\mathcal{E}(\rho) = (1 - p)X\rho X + pZ\rho Z$, где малый параметр p определяет величину шума. Степень совпадения для этого элемента равна

$$F(X, \mathcal{E}) = \min_{|\psi\rangle} \sqrt{\langle\psi|X((1-p)X|\psi\rangle\langle\psi|X + pZ|\psi\rangle\langle\psi|Z)X|\psi\rangle} \quad (9.123)$$

$$= \min_{|\psi\rangle} \sqrt{(1-p) + \langle\psi|Y|\psi\rangle^2} \quad (9.124)$$

$$= \sqrt{1 - p}. \quad (9.125)$$

В упр. 9.22 вы покажете, что последовательность из элементов с большой степенью совпадения также имеет большую степень совпадения. Таким образом, для выполнения квантового вычисления достаточно, чтобы каждый элемент вычисления имел большую степень совпадения. (Сравните это утверждение с подобным, но менее общим утверждением в гл. 4 относительно аппроксимации квантовых схем).

Упражнение 9.22 (цепное свойство степени совпадения). Предположим, что U и V — унитарные операторы, а \mathcal{E} и \mathcal{F} — сохраняющие след квантовые преобразования, аппроксимирующие U и V . Пусть $d(\cdot, \cdot)$ — произвольная метрика в пространстве матриц плотности (например, угол $\arccos(F(\rho, \sigma))$). Введем величину ошибки $E(U, \mathcal{E})$ следующим образом:

$$E(U, \mathcal{E}) = \max_{\rho} d(U\rho U^\dagger, \mathcal{E}(\rho)). \quad (9.126)$$

Покажите, что $E(VU, \mathcal{E} \circ \mathcal{F}) \leq E(U, \mathcal{E}) + E(V, \mathcal{F})$. Это значит, что для выполнения квантового вычисления с большой степенью совпадения, достаточно каждый его шаг выполнять с большой степенью совпадения.

Квантовые источники информации и точность воспроизведения запутанности

Мы обсуждаем динамические меры сохранения информации, но пока строго не определили, что подразумеваем под источником информации. Ниже мы введем два определения этого понятия и с их помощью рассмотрим несколько динамических мер сохранения информации. Не совсем ясно, как наилучшим образом определить квантовый источник информации. В классическом случае наилучшее решение этой задачи совсем не очевидно, возможны и различные неэквивалентные определения, на основе каждого из которых можно построить полную и полезную теорию информации. Так как классическая информация является частным случаем квантовой, неудивительно, что в квантовой механике существует еще больше способов определения источника информации. В завершение этой главы мы введем два квантовых определения источника информации, объясним, как из них получаются соответствующие меры сохранения информации и докажем некоторые элементарные свойства этих мер. Дальнейшее обсуждение квантовых источников информации мы отложим до гл. 12.

Первое определение квантового источника — это поток одинаковых квантовых систем (например, кубитов), которые возникают в результате некоторого физического процесса и имеют состояния $\rho_{X_1}, \rho_{X_2}, \dots$. Здесь X_j — независимые одинаково распределенные случайные величины, а ρ_j — некоторый фиксированный набор матриц плотности. Например, можно представить себе поток кубитов, которые с одинаковой вероятностью $1/2$ приготавливаются либо в состоянии $|0\rangle$, либо в состоянии $(|0\rangle + |1\rangle)/\sqrt{2}$.

Такое определение квантового источника через *ансамбль* квантовых систем естественным образом ведет к определению *средней по ансамблю степени совпадения*. Эта величина определяет, насколько хорошо сохраняется информа-

ция, полученная из источника при действии шума, описываемого сохраняющим след квантовым преобразованием \mathcal{E} ,

$$\bar{F} = \sum_j p_j F(\rho_j, \mathcal{E}(\rho_j))^2. \quad (9.127)$$

Здесь p_j — распределения вероятностей, соответствующие различным начальным состояниям системы ρ_j . Очевидно, что $0 \leq \bar{F} \leq 1$, и если $\bar{F} \approx 1$, то в среднем канал \mathcal{E} передает состояния, полученные из источника, с большой степенью точности. Может возникнуть вопрос, почему в правой части формулы степень совпадения возводится в квадрат. Есть два ответа на этот вопрос: простой и сложный. Простой ответ состоит в том, что средняя по ансамблю степень совпадения, определенная таким способом, связана с точностью воспроизведения запутанности, которую мы введем ниже. Более сложный ответ заключается в том, что теория квантовой информации находится сейчас в стадии разработки, и пока не вполне понятно, каким должно быть «правильное» определение для такого понятия как сохранение информации. Тем не менее, в гл. 12 мы увидим, что на основе средней по ансамблю степени совпадения и точности воспроизведения запутанности можно построить полную теорию квантовой информации. Это дает нам надежду, что эти меры определены правильно, хотя полная теория квантовой информации еще не разработана.

Упражнение 9.23. Покажите, что $\bar{F} = 1$ тогда и только тогда, когда $\mathcal{E}(\rho_j) = \rho_j$ для всех j , таких, что $p_j > 0$.

Второе определение квантового источника, которое мы рассмотрим, основано на предположении, что канал, хорошо сохраняющий информацию, хорошо сохраняет и запутанность состояний. Основная идея взята из обсуждения классической вероятности ошибки в разд. 9.1. Как там было отмечено, в квантовом процессе не существует аналого классической вероятности ошибки $p(X \neq Y)$, так как нет квантового аналога распределению вероятностей, определенному в два разных момента времени. Вместо этого, мы будем использовать квантовый аналог процесса, проиллюстрированного на рис. 9.7. Здесь динамическая мера различия вводится следующим образом. Случайная переменная X копируется в \bar{X} , и, подвергаясь шуму, переходит в Y . В качестве меры различия используется некоторое расстояние $D[(\bar{X}, X), (\bar{X}', Y)]$ между совместными распределениями (\bar{X}, X) и (\bar{X}', Y) .

Опишем квантовый аналог этой модели. Квантовая система Q находится вначале в состоянии ρ . Предполагается, что состояние Q некоторым образом запутано с окружающим миром. Эта запутанность играет роль корреляции между X и \bar{X} в классическом случае. Мы опишем эту запутанность, введя некоторую фиктивную систему R , такую, что совместная система RQ находится в чистом состоянии. Оказывается, что все наши результаты не зависят от того, как мы производим расширение до чистого состояния, поэтому, будем предполагать произвольную запутанность с внешним миром. Эволюция системы Q описывается преобразованием \mathcal{E} . Эта ситуация проиллюстрирована на рис. 9.8.

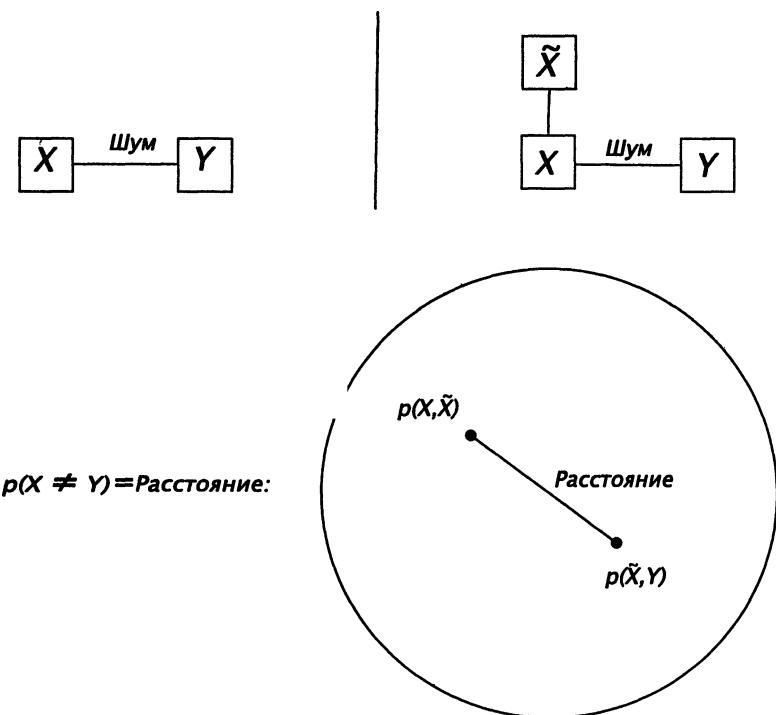


Рис. 9.7. Вероятность ошибки в канале равна расстоянию между распределениями вероятностей для (\tilde{X}, X) и (\tilde{X}', Y) в следовой метрике

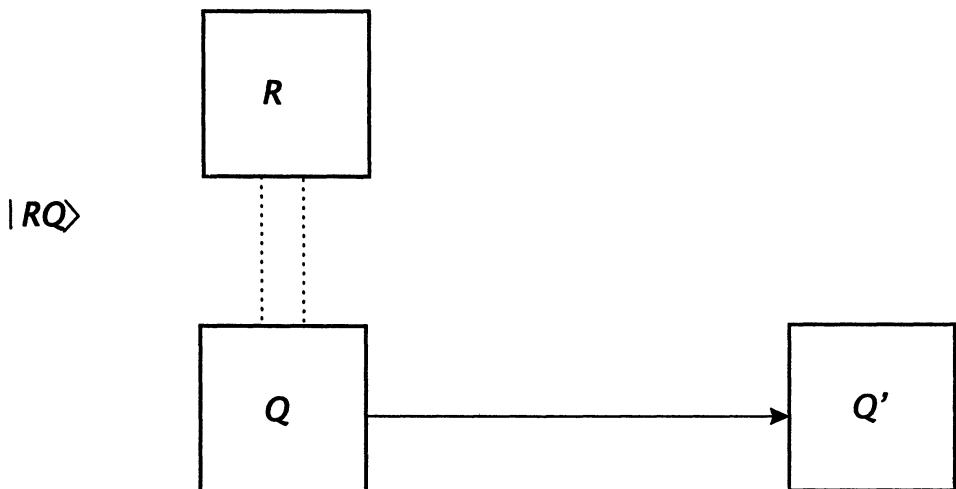


Рис. 9.8. RQ -представление квантового канала. Начальное состояние RQ является чистым.

Насколько преобразование \mathcal{E} сохраняет запутанность систем R и Q ? Количественно мы опишем это *точностью воспроизведения запутанности* $F(\rho, \mathcal{E})$, которая является функцией ρ и \mathcal{E} и определена для сохраняющих след преобразований \mathcal{E} следующим образом:

$$F(\rho, \mathcal{E}) \equiv F(RQ, R'Q')^2 \quad (9.128)$$

$$= \langle RQ | [(\mathcal{I}_R \otimes \mathcal{E})(|RQ\rangle\langle RQ|)] | RQ \rangle. \quad (9.129)$$

Здесь штрих обозначает состояние системы после действия квантового преобразования. Величина в правой части равенства — *квадрат статической степени совпадения* начального и конечного состояний системы RQ . Возведение в квадрат используется только для удобства, при этом упрощаются некоторые свойства точности воспроизведения запутанности. Обратите внимание, что точность воспроизведения запутанности зависит только от ρ и \mathcal{E} и не зависит (как может показаться) от способа расширения системы до чистого состояния $|RQ\rangle$. Чтобы показать это, используем факт, доказанный в упр. 2.81: расширения состояния ρ до двух чистых состояний $|R_1Q_1\rangle$ и $|R_2Q_2\rangle$ связаны унитарным преобразованием U , *которое действует только на систему R*, $|R_2Q_2\rangle = U|R_1Q_1\rangle$. Таким образом

$$F(|R_2Q_2\rangle, \rho^{R'_2Q'_2}) = F(|R_1Q_1\rangle, \rho^{R'_1Q'_2}), \quad (9.130)$$

что и требовалось доказать. Точность воспроизведения запутанности показывает, насколько запутанность систем R и Q сохраняется при преобразовании \mathcal{E} . Если она близка к единице, запутанность сохраняется хорошо, если же она близка к нулю, запутанность почти полностью разрушается. Не очень важно, как определять точность воспроизведения запутанности: через квадрат или через первую степень статической степени совпадения. Определение, которое дано здесь, приводит к более красивой математической записи ее свойств.

Одно из замечательных свойств точности воспроизведения запутанности состоит в том, что существует очень простая формула для ее вычисления. Пусть E_i — элементы квантового преобразования \mathcal{E} . Тогда

$$F(\rho, \mathcal{E}) = \langle RQ | \rho^{R'Q'} | RQ \rangle = \sum_i |\langle RQ | E_i | RQ \rangle|^2. \quad (9.131)$$

Запишем $|RQ\rangle = \sum_j \sqrt{p_j} |j\rangle |j\rangle$, где $\rho = \sum_j p_j |j\rangle\langle j|$. Отсюда

$$\langle RQ | E_i | RQ \rangle = \sum_{jk} \sqrt{p_j p_k} \langle j | k \rangle \langle j | E_i | k \rangle \quad (9.132)$$

$$= \sum_j p_j \langle j | E_i | j \rangle \quad (9.133)$$

$$= \text{tr}(E_i \rho). \quad (9.134)$$

Подставив это выражение в (9.131), получим полезную формулу для вычислений

$$F(\rho, \mathcal{E}) = \sum_i |\text{tr}(\rho E_i)|^2. \quad (9.135)$$

Например, точность воспроизведения запутанности для канала с затуханием фазы $\mathcal{E} = \rho + (1-p)pZ\rho Z$ равна

$$F(\rho, \mathcal{E}) = |\text{tr}(\rho)|^2 + (1-p)p|\text{tr}(\rho Z)|^2 = (1-p) + p\text{tr}(\rho Z)^2. \quad (9.136)$$

Видно, что с увеличением p точность воспроизведения запутанности уменьшается, как мы интуитивно и ожидали.

Мы ввели понятие источника квантовой информации и связанное с ним понятие меры двумя способами. Один из них основан на том, что нам нужно сохранять ансамбль квантовых состояний с большой степенью совпадения; а другой — на том, что мы хотим сохранять запутанность между источником и некоторой внешней системой. Удивительным образом эти два определения оказываются тесно связанными. Причиной этого является два полезных свойства точности воспроизведения запутанности. Во-первых, точность воспроизведения запутанности является нижней границей для квадрата статической степени совпадения входного и выходного состояний:

$$F(\rho, \mathcal{E}) \leq [F(\rho, \mathcal{E}(\rho))]^2. \quad (9.137)$$

Интуитивно этот результат означает, что сохранить состояние и его запутанность с внешним миром труднее, чем просто сохранить состояние. Доказательство следует из монотонности степени совпадения при взятии частичного следа: $F(\rho, \mathcal{E}) = F(|RQ\rangle, \rho^{R'Q'})^2 \leq F(\rho^Q, \rho^{Q'})^2$.

Второе свойство точность воспроизведения запутанности, которое позволит нам установить ее связь со средней по ансамблю степенью совпадения, это то, что она является выпуклой функцией ρ . Чтобы показать это, введем функцию $f(x) \equiv F(x\rho_1 + (1-x)\rho_2, \mathcal{E})$. Используя выражение (9.135) и проведя элементарные вычисления, получим

$$f''(x) = 2 \sum_i |\text{tr}((\rho_1 - \rho_2)E_i)|^2. \quad (9.138)$$

Видно, что $f''(x) \geq 0$, что и означает, что точность воспроизведения запутанности обладает свойством выпуклости. Объединив эти два свойства, обнаружим, что

$$F\left(\sum_j p_j \rho_j, \mathcal{E}\right) \leq \sum_j p_j F(\rho_j, \mathcal{E}) \quad (9.139)$$

$$\leq \sum_j p_j F(\rho_j, \mathcal{E}(\rho_j))^2 \quad (9.140)$$

и, следовательно,

$$F\left(\sum_j p_j \rho_j, \mathcal{E}\right) \leq \bar{F}. \quad (9.141)$$

Таким образом, любой квантовый канал \mathcal{E} , который хорошо сохраняет запутанность исходного состояния ρ с внешней системой, автоматически хорошо сохраняет и ансамбль входных состояний, заданный вероятностями p_j и состояниями ρ_j , такими что $\rho = \sum_j p_j \rho_j$. В этом смысле понятие квантового источника, основанное на точности воспроизведения запутанности, более сильное, чем понятие, основанное на ансамбле состояний. Поэтому мы преимущественно будем использовать точность воспроизведения запутанности при изучении квантовой теории информации в гл. 12.

Эту главу мы завершим коротким списком легко доказываемых свойств точности воспроизведения запутанности, которые пригодятся нам в следующих главах.

- (1) $0 \leq F(\rho, \mathcal{E}) \leq 1$. Следует из свойств статической степени совпадения.
- (2) Точность воспроизведения запутанности линейна по второму аргументу. Следует из определения точности воспроизведения запутанности.
- (3) Для чистых состояний точность воспроизведения запутанности равна квадрату статической степени совпадения входных и выходным состояниям,

$$F(|\psi\rangle, \mathcal{E}) = F(|\psi\rangle, \mathcal{E}(|\psi\rangle\langle\psi|))^2. \quad (9.142)$$

Это следует из того, что чистое состояние $|\psi\rangle$ является расширением состояния самого себя и из определения точности воспроизведения запутанности.

- (4) $F(\rho, \mathcal{E}) = 1$ тогда и только тогда, когда для всех чистых состояний $|\psi\rangle$ из носителя ρ

$$\mathcal{E}(|\psi\rangle\langle\psi|) = |\psi\rangle\langle\psi|. \quad (9.143)$$

Чтобы доказать это, предположим, что $F(\rho, \mathcal{E}) = 1$, а $|\psi\rangle$ — чистое состояние из носителя ρ . Введем величину $p = 1/\langle\psi|\rho^{-1}|\psi\rangle > 0$ (см. упр. 2.73) и такую матрицу плотности σ , что $(1-p)\sigma = \rho - p(|\psi\rangle\langle\psi|)$. Используя выпуклость, получим

$$1 = F(\rho, \mathcal{E}) \leq p\sqrt{F(|\psi\rangle, \mathcal{E})} + (1-p). \quad (9.144)$$

Отсюда следует $F(|\psi\rangle, \mathcal{E}) = 1$, что и требуется. Доказательство обратного утверждения заключается в простом применении определения точности воспроизведения запутанности.

- (5) Пусть $\langle \psi | \mathcal{E}(|\psi\rangle\langle\psi|) |\psi\rangle \geq 1 - \eta$ для всех $|\psi\rangle$ из носителя ρ и некоторого η . Тогда $F(\rho, \mathcal{E}) \geq 1 - (3\eta/2)$ (см. задачу 9.3).

Задача 9.1 (альтернативное определение степени совпадения). Покажите, что

$$F(\rho, \sigma) = \inf_P \text{tr}(\rho P) \text{tr}(\sigma P^{-1}), \quad (9.145)$$

где нижняя грань берется по всем невырожденным положительно определенным матрицам P .

Задача 9.2. Пусть \mathcal{E} — сохраняющее след квантовое преобразование. Покажите, что существует набор элементов этого преобразования $\{E_i\}$, такой, что

$$F(\rho, \mathcal{E}) = |\text{tr}(\rho E_1)|^2. \quad (9.146)$$

Задача 9.3. Докажите сформулированное выше свойство (5) точности воспроизведения запутанности.

Краткое содержание главы

- Следовая метрика: $D(\rho, \sigma) \equiv \frac{1}{2} \text{tr} |\rho - \sigma|$, дважды выпуклая метрика матриц плотности, уменьшающаяся под действием сохраняющих след квантовых преобразований.
- Степень совпадения:

$$F(\rho, \sigma) = \text{tr} \sqrt{\rho^{1/2} \sigma \rho^{1/2}} = \max_{|\psi\rangle, |\varphi\rangle} |\langle \psi | \varphi \rangle|.$$

Сильно вогнута: $F(\sum_i p_i \rho_i, \sum_i q_i \sigma_i) \geq \sum_i \sqrt{p_i q_i} F(\rho_i, \sigma_i)$.

- Точность воспроизведения запутанности: $F(\rho, \mathcal{E})$. Мера того, насколько хорошо сохраняется запутанность при квантовомеханическом процессе, в котором система Q , находящаяся в состоянии ρ и запутанная с системой R , подвергается квантовому преобразованию \mathcal{E} .

История и дополнительная литература

Читатели, желающие узнать больше о мерах реализации квантовой информации, могут начать с диссертации Фукса 1996 года [157]. Она содержит большое количество материала по мерам различия, в том числе 528 ссылок на работы, сгруппированных по темам. Кроме того, там можно найти доказательство формулы (9.74) и еще много интересного. Доказательство того, что квантовое преобразование уменьшает следовую метрику, было выполнено Рускаи [343]. Мон

нотонность степени совпадения доказана Барнумом, Кейвсом, Фуксом, Йожа и Шумахером [34]. Иногда в литературе степенью совпадения называют квадрат величины, которую мы назвали степенью совпадения. В работе Ульмана [394], где Ульман доказывает названную его именем теорему, также подробно обсуждаются основные свойства степени совпадения. Доказательство теоремы Ульмана, приведенное в этой книге, принадлежит Йожа [203]. Цепное свойство степени совпадения и его связь с квантовым вычислением при наличии шума детально описаны Аароновой, Китаевым и Нисаном [10]. Шумахер [352] ввел понятие *точности воспроизведения запутанности* и доказал множество ее основных свойств. Нилл и Лафлам [216] установили связь между степенью совпадения и точностью воспроизведения запутанности (задача 9.3). Более подробное доказательство этого факта приведено в работе Барнума, Нилла и Нильсена [60]. Задача 9.1 принадлежит Альберти [14].

Глава 10

ИСПРАВЛЕНИЕ КВАНТОВЫХ ОШИБОК

Мы узнали, что запутанность можно победить запутанностью.

Джон Прескилл

Ошибаться и исправлять ошибки — часть божьего замысла.

Уильям Блейк

В этой главе объясняется, как сделать надежной обработку квантовой информации при наличии шума. Излагаемый материал охватывает три большие темы: основы теории *квантовых кодов, исправляющих ошибки; квантовые вычисления, устойчивые к ошибкам; пороговая теорема*. Мы начнем с изложения основ теории квантовых кодов, исправляющих ошибки, которые позволяют защитить квантовую информацию от шума. С помощью этих кодов выполняется *кодирование* квантовых состояний специальным образом, делающим их устойчивыми к влиянию шума, а затем *декодирование*, когда понадобится восстановить исходное состояние. В разд. 10.1 рассмотрены основные идеи исправления классических ошибок и некоторые принципиальные условия, которые должны быть выполнены, чтобы было возможно исправление квантовых ошибок. В разд. 10.2 приведен простой пример кода, исправляющего ошибки, который мы в разд. 10.3 обобщим в теорию квантовых кодов, исправляющих ошибки. В разд. 10.4 объяснено несколько идей классической теории линейных кодов и то, как из них получаются квантовые коды *Кальдербанка–Шора–Стина* (CSS коды). Раздел 10.5 дополнит наш обзор квантовых кодов, исправляющих ошибки, обсуждением хорошо разработанного класса симплектических (стабилизирующих) кодов, тесно связанных с классическими кодами, исправляющими ошибки.

При рассмотрении теории исправления квантовых ошибок предполагаем, что кодирование и декодирование квантовых состояний могут быть выполнены безошибочно. Это справедливо, если, например, мы хотим передать квантовые состояния по каналу связи с шумом и можем использовать почти безошибочные квантовые компьютеры для кодирования и декодирования состояний на входе и выходе канала. Однако, такое предположение нельзя сделать, если квантовые элементы, используемые для кодирования и декодирования, сами подвержены шуму. К счастью, теория *квантового вычисления, устойчивого к*

ошибкам, которая излагается в разд. 10.6, позволяет обойтись без предположения об идеальности кодирования и декодирования. Более того, устойчивость к ошибкам позволяет производить логические операции над *закодированными* квантовыми состояниями так, чтобы исключить в них ошибки. Глава завершается *пороговой теоремой* квантовых вычислений (подразд. 10.6.4): если шум в *каждом квантовом элементе системы меньше некоторого постоянного порогового значения*, с помощью этой системы можно выполнить произвольно длинное квантовое вычисление. Конечно, это утверждение верно не во всех случаях, мы обсудим условия его применимости. Тем не менее, пороговая теорема является важным результатом, показывающим, что шум, судя по всему, не является фундаментальным препятствием для длинных квантовых вычислений.

10.1 Введение

Шум очень мешает работе вычислительных систем. Мы стремимся строить наши системы так, чтобы полностью избежать шума. Если же это невозможно, мы стараемся защитить их от его последствий. Например, компоненты современных компьютеров очень надежны, обычно в них происходит менее одной ошибки на 10^{17} операций. Для большинства практических задач можно считать, что в компонентах компьютера полностью отсутствует шум. С другой стороны, многие широко используемые системы существенно подвержены шуму. Модемы и CD-проигрыватели используют коды, исправляющие ошибки, чтобы защититься от него. Методы борьбы с шумом могут быть достаточно сложными, но их основные принципы понять довольно просто. Ключевая идея состоит в том, что если мы хотим защитить сообщение от шума, нужно *закодировать* его, добавив некоторую избыточную информацию. Таким образом, даже если часть информации в закодированном сообщении будет испорчена, избыточность позволит нам *декодировать* его, восстановить всю исходную информацию.

Например, предположим, что мы хотим передать из одного места в другое один бит информации по классическому каналу связи с шумом. Шум в канале изменяет бит с вероятностью $p > 0$; с вероятностью $1 - p$ бит передается без ошибки. Такой канал называют *двоичным симметричным каналом*, его схема изображена на рис. 10.1. Простое средство защиты передаваемого бита от шума в двоичном симметричном канале – заменить его на три копии:

$$0 \rightarrow 000 \tag{10.1}$$

$$1 \rightarrow 111 \tag{10.2}$$

Строки 000 и 111 иногда называют *логическим 0* и *логическим 1*, так как они играют роль нуля и единицы соответственно. Теперь мы передаем все три бита по каналу. Адресат, получив три бита, должен решить, каково было значение исходного бита. Предположим, что было получено 001. Если вероятность из-

менения бита p не слишком велика, то в канале наверняка был изменен третий бит, и исходный бит был 0.

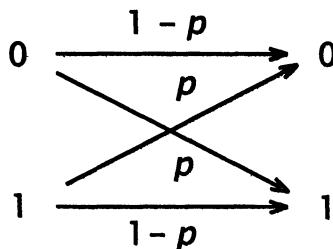


Рис. 10.1. Двоичный симметричный канал.

Этот тип декодирования называется *выбором по большинству*, так как окончательное значение 0 или 1 определяется по тому, какое из значений встретилось большее число раз. Выбор по большинству не сработает, если при передаче изменились два или три бита. Вероятность этого $3p^2(1-p) + p^3$, т. е. вероятность ошибки в нашей системе $p_e = 3p^2 - 2p^3$. Без кодирования вероятность ошибки p . При использовании этого кода передача более надежна ($p_e < p$), если $p < 1/2$.

Только что описанный тип кода называют *кодом с повторением*, так как кодирование сообщения заключается в повторении его несколько раз. Аналогичный метод используется и при разговоре: если мы не понимаем кого-то, например из-за иностранного акцента, то просим повторить сказанное. Мы можем не разобрать всех слов при каждом повторе, но, объединив их вместе, можно понять все сорбщение. В теории кодов, исправляющих классические ошибки, разработано много сложных методов, однако основная идея всегда заключается в добавлении избыточной информации при кодировании, количеством которой выбирается в зависимости от интенсивности шума в канале так, чтобы можно было восстановить исходное сообщение.

10.1.1 Трехкубитовый код, исправляющий классические ошибки

Чтобы защитить квантовые состояния от шума, нам хотелось бы разработать *квантовые коды, исправляющие ошибки*, которые основаны на подобных принципах. Существует несколько важных различий между классической и квантовой информацией, поэтому нужны новые идеи, чтобы создать такие коды. На первый взгляд, мы имеем три проблемы:

- *Невозможность копирования*. Можно было бы попытаться использовать код с повторением, копируя квантовые состояния три или более раз. Однако, это запрещено теоремой о невозможности копирования (см. Вставку 12.1). Даже если копирование возможно, нельзя измерить и сравнить три квантовых состояния, переданных по каналу.

- *Непрерывность ошибки.* Множество возможных ошибок одного кубита является непрерывным. Определение того, какая ошибка произошла, потребует бесконечной точности и, следовательно, бесконечных ресурсов.
- *Разрушение квантовой информации при измерении.* При классическом исправлении ошибок мы смотрим на полученную по каналу информацию и решаем, какое декодирование применять. В квантовой механике измерение полностью разрушает квантовое состояние, что делает восстановление исходной информации невозможным.

К счастью, как мы покажем, все эти проблемы можно обойти. Предположим, что мы передаем кубиты по каналу, который оставляет их неизменными с вероятностью $1 - p$ и меняет с вероятностью p , т. е. с вероятностью p состояние $|\psi\rangle$ переходит в состояние $X|\psi\rangle$, где X — матрица Паули σ^x , или *оператор классического изменения бита*. Такой канал называется каналом с классической ошибкой. Код, который мы сейчас опишем, может исправлять такие ошибки.

Предположим, что мы кодируем состояние одного кубита $a|0\rangle + b|1\rangle$ трёх кубитами: $a|000\rangle + b|111\rangle$. Удобно записать это преобразование следующим образом:

$$|0\rangle \rightarrow |0_L\rangle \equiv |000\rangle \quad (10.3)$$

$$|1\rangle \rightarrow |1_L\rangle \equiv |111\rangle. \quad (10.4)$$

Суперпозиция состояний $|0\rangle$ и $|1\rangle$ кодируется соответствующей суперпозицией состояний $|0_L\rangle$ и $|1_L\rangle$. Обозначения $|0_L\rangle$ и $|1_L\rangle$ показывают, что это *логические*, а не *физические* ноль и единица. Схема, осуществляющая такое кодирование, изображена на рис. 10.2.

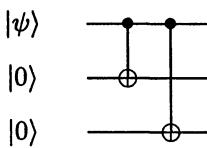


Рис. 10.2. Схема кодирования для трехкубитового кода, исправляющего классические ошибки. Кодируемые данные поступают по верхней линии

Упражнение 10.1. Проверьте, что схема на рис. 10.2 действительно осуществляет описанное выше кодирование.

Предположим, что состояние $a|0\rangle + b|1\rangle$ было без ошибок закодировано в $a|000\rangle + b|111\rangle$. Каждый из трех кубитов передается независимо по каналу с классической ошибкой. Пусть при передаче произошла ошибка не более, чем в одном кубите. Существует простая процедура исправления такой ошибки, которая позволяет восстановить исходное квантовое состояние. Она состоит из двух частей:

- (1) *Обнаружение ошибки, или нахождение ее синдрома.* Мы производим измерение, которое показывает, какая ошибка произошла. Результат измерения называется *синдромом ошибки*. Для канала с классической ошибкой существует четыре различных синдрома, соответствующих четырем проекторам:

$$P_0 \equiv |000\rangle\langle 000| + |111\rangle\langle 111| \quad \text{ошибки нет} \quad (10.5)$$

$$P_1 \equiv |100\rangle\langle 100| + |011\rangle\langle 011| \quad \text{ошибка в первом кубите} \quad (10.6)$$

$$P_2 \equiv |010\rangle\langle 010| + |101\rangle\langle 101| \quad \text{ошибка во втором кубите} \quad (10.7)$$

$$P_3 \equiv |001\rangle\langle 001| + |110\rangle\langle 110| \quad \text{ошибка в третьем кубите.} \quad (10.8)$$

Предположим, например, что ошибка произошла в первом кубите, так что полученное состояние $\psi = a|100\rangle + b|011\rangle$. Заметим, что в этом случае $\langle\psi|P_1|\psi\rangle = 1$, так что результат такого измерения (синдром ошибки) обязательно будет равен 1. Синдромы, соответствующие операторам P_0 , P_2 и P_3 , будут равны нулю. Более того, определение синдромов не меняет квантовое состояние: после измерений оно останется равным $a|100\rangle + b|011\rangle$. Обратите внимание, что синдромы содержат информацию только о том, какая ошибка произошла. По ним мы не сможем определить a и b и узнать, какое состояние было закодировано. Это является общим свойством синдромов. При получении информации о квантовом состоянии оно непременно нарушается.

- (2) *Исправление ошибки.* Мы используем синдром ошибки, чтобы понять, как восстановить исходное состояние. Например, если синдром, соответствующий оператору P_1 , равен 1, это означает, что ошибка произошла в первом кубите. Мы инвертируем первый кубит и в точности восстанавливаем исходное состояние $a|000\rangle + b|111\rangle$. В четырех возможных случаях наши действия такие: если равен единице синдром, соответствующий оператору P_0 , то никакой ошибки не произошло и мы оставляем состояние неизменным; если равен единице один из синдромов, соответствующих P_1 , P_2 или P_3 , мы инвертируем первый, второй или третий кубит соответственно. Легко показать, что в каждом случае в точности восстанавливается исходное состояние.

Такая процедура исправления ошибки сработает, если только ошибка произошла не более, чем в одном кубите. Вероятность этого равна $(1-p)^3 + 3p(1-p)^2 = 1 - 3p^2 + 2p^3$. Вероятность того, что ошибка останется неисправлена, равна $3p^2 - 2p^3$, т. е. точно такая же, как для классического кода с повторением, который мы обсуждали ранее. Точно так же при $p < 1/2$ кодирование и декодирование увеличивают надежность передачи квантового состояния.

Улучшение анализа ошибок

Приведенный выше анализ ошибок недостаточен. Проблема заключается в том, что квантовые состояния и возможные ошибки бывают различными. Пространство состояний непрерывно, так что ошибка может изменить состояние

как в небольшой степени, так и полностью. Одним из примеров является классическая ошибка X , которая никак не влияет на состояние $(|0\rangle + |1\rangle)/\sqrt{2}$, но меняет состояние $|0\rangle$ на $|1\rangle$. В первом случае не нужно заботиться об исправлении такой ошибки, во втором придется ее исправлять.

Чтобы разобраться с этой проблемой, мы используем понятие *степени совпадения*, введенное в гл. 9. Вспомним, что степень совпадения чистого и смешанного состояний есть $F(|\psi\rangle, \rho) = \sqrt{\langle\psi|\rho|\psi\rangle}$. Задача исправления квантовых ошибок — увеличить эту степень совпадения при хранении или передаче информации до максимально возможного значения. Давайте сравним *минимальную* степень совпадения, возможную при использовании трехкубитового кода, исправляющего классические ошибки, со случаем, когда никакого исправления ошибок не производится. Предположим, что рассматривается состояние $|\psi\rangle$. Без использования кода, исправляющего ошибки, состояние после передачи кубита по каналу будет

$$\rho = (1 - p)|\psi\rangle\langle\psi| + pX|\psi\rangle\langle\psi|X. \quad (10.9)$$

Степень совпадения в этом случае

$$F = \sqrt{\langle\psi|\rho|\psi\rangle} = \sqrt{(1 - p) + p\langle\psi|X|\psi\rangle\langle\psi|X|\psi\rangle}. \quad (10.10)$$

Второе слагаемое под знаком квадратного корня неотрицательно и равно нулю при $|\psi\rangle = |0\rangle$, т. е. минимальная степень совпадения равна $\sqrt{1 - p}$. Предположим, что трехкубитовый код используется для защиты состояния $|\psi\rangle = a|0_L\rangle + b|1_L\rangle$. Квантовое состояние после передачи кубита и исправления ошибки

$$\rho = [(1 - p)^3 + 3p(1 - p^2)]|\psi\rangle\langle\psi| + \dots \quad (10.11)$$

Здесь многоточием заменены слагаемые, дающие вклад от ошибок в двух или трех кубитах. Эти члены положительны, так что опустив их, мы найдем нижнюю оценку степени совпадения. Мы видим, что $F = \sqrt{\langle\psi|\rho|\psi\rangle} \geq \sqrt{(1 - p)^3 + 3p(1 - p)^2}$, т. е. степень совпадения не больше $\sqrt{1 - 3p^2 + 2p^3}$. Таким образом степень совпадения увеличивается при $p < 1/2$. Этот результат совпадает с тем, что был получен ранее более грубым способом.

Упражнение 10.2. Действие канала с классической ошибкой может быть описано квантовым преобразованием $\mathcal{E}(\rho) = (1 - p)\rho + pX\rho X$. Покажите, что его также можно представить как $\mathcal{E}(\rho) = (1 - 2p)\rho + 2pP_+\rho P_+ + 2pP_-\rho P_-$, где P_+ и P_- — проекторы на собственные состояния X , $(|0\rangle + |1\rangle)/\sqrt{2}$ и $(|0\rangle - |1\rangle)/\sqrt{2}$ соответственно. В таком представлении кубит при передаче остается неизменным с вероятностью $1 - 2p$, и измеряется в базисе $|+\rangle, |-\rangle$ с вероятностью $2p$.

Существует другой подход к рассмотрению синдромов. Он будет полезен при обобщении трехкубитового кода. Предположим, что вместо измерений четырех проекторов P_0, P_1, P_2, P_3 мы производим два измерения: наблюдаемой Z_1Z_2 (т. е. $Z \otimes Z \otimes I$) и затем наблюдаемой Z_2Z_3 . Эти наблюдаемые имеют

собственные значения ± 1 , т. е. в каждом измерении мы получаем один бит информации. Два измерения дают четыре возможных результата, как и было описано выше. Результат первого измерения, $Z_1 Z_2$, показывает, совпадают ли первый и второй кубиты. Действительно, спектральное разложение $Z_1 Z_2$ есть

$$Z_1 Z_2 = (|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes I - (|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I, \quad (10.12)$$

что соответствует измерению проекторов $(|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes I$ и $(|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I$. Мы получаем $+1$, если кубиты совпадают, и -1 в противном случае. Точно также измерение $Z_2 Z_3$ показывает, совпадают ли второй и третий кубиты. По результатам этих измерений мы можем сказать, произошла ли классическая ошибка, и если да, то в каком кубите. Если оба измерения дают $+1$, с большой вероятностью ошибки не было. Если первое измерение дает $+1$, а второе -1 , ошибка скорее всего произошла в третьем кубите, если же первое измерение дает -1 , а второе $+1$, то ошибка в первом кубите. Если оба измерения дают -1 , скорее всего ошибка произошла во втором кубите. Существенно, что ни одно из измерений не дает информации об амплитудах a и b закодированного квантового состояния и, таким образом, не разрушает суперпозиций квантовых состояний, которые мы хотим сохранить при использовании этого кода.

Упражнение 10.3. Покажите, что измерения $Z_1 Z_2$ и $Z_2 Z_3$ с точностью до переобозначения результатов эквивалентны измерениям четырех проекторов, определенных в (10.5)-(10.8), в том смысле, что обе процедуры дают одинаковую статистику измерений и оставляют кубиты в одинаковых состояниях.

10.1.2 Трехкубитовый код, исправляющий фазовые ошибки

Только что описанный код интересен, однако он не является существенно новым по сравнению с классическим кодом, исправляющим ошибки. Кроме того, он не решает многие проблемы, в частности, с его помощью можно исправлять только классические ошибки. Более интересен код, исправляющий *фазовые ошибки*. С вероятностью $1 - p$ состояние кубита не изменяется. С вероятностью p изменяется относительная фаза состояний $|0\rangle$ и $|1\rangle$. Более точно оператор фазовой ошибки, Z , действуя на кубит с вероятностью $p > 0$, переводит состояние $a|0\rangle + b|1\rangle$ в состояние $a|0\rangle - b|1\rangle$. Классического аналога такой ошибки не существует, однако канал с фазовой ошибкой можно легко превратить в канал с классической ошибкой. Предположим, что мы работаем в базисе $|+\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}$, $|-\rangle \equiv (|0\rangle - |1\rangle)/\sqrt{2}$. В этом базисе оператор Z меняет $|+\rangle$ на $|-\rangle$ и наоборот, т. е. работает как оператор классической ошибки. Это наводит на мысль использовать для исправления фазовых ошибок состояния $|0_L\rangle \equiv |+++>$ и $|1_L\rangle \equiv |--->$ в качестве логических нуля и единицы. Все операции исправления ошибок — кодирование, обнаружение ошибки и восстановление — выполняются так же, как для канала с классической ошибкой, но в базисе $|+\rangle$ и $|-\rangle$ вместо $|0\rangle$ и $|1\rangle$. Для замены базиса мы используем элемент Адамара.

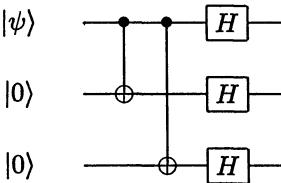


Рис. 10.3. Схема кодирования для трехкубитового кода, исправляющего фазовые ошибки.

Кодирование для канала с фазовой ошибкой осуществляется в два этапа. Сначала мы кодируем состояние одного кубита тремя кубитами, точно так же, как для канала с классической ошибкой, и затем применяем преобразование Адамара к каждому из этих трех кубитов (рис. 10.3). Поиск ошибки производится такими же проективными измерениями, как и раньше, но сопряженными преобразованиями Адамара, $P_j \rightarrow P'_j \equiv H^{\otimes 3}P_jH^{\otimes 3}$. Точно так же, синдромы ошибки могут быть найдены измерением величин $H^{\otimes 3}Z_1Z_2H^{\otimes 3} = X_1X_2$ и $H^{\otimes 3}Z_2Z_3H^{\otimes 3} = X_2X_3$. Интересно интерпретировать эти измерения аналогично измерениям Z_1Z_2 и Z_2Z_3 при исправлении классической ошибки. Здесь измерения X_1X_2 и X_2X_3 соответствуют сравнению знаков первого и второго или второго и третьего кубитов соответственно. Действительно, измерение X_1X_2 дает +1 для состояний типа $|+\rangle|+\rangle\otimes(\cdot)$ или $|-\rangle|-\rangle\otimes(\cdot)$ и -1 для состояний типа $|+\rangle|-\rangle\otimes(\cdot)$ или $|-\rangle|+\rangle\otimes(\cdot)$. Обнаруженная ошибка исправляется теми же операторами, что и в случае классической ошибки, но также сопряженными с преобразованием Адамара. Например, если мы обнаружили изменение знака первого кубита с $|+\rangle$ на $|-\rangle$, мы исправляем ошибку, действуя на первый кубит оператором $HX_1H = Z_1$. Аналогично мы поступаем и в случае других ошибок.

Очевидно, что код, исправляющий фазовые ошибки, имеет те же характеристики, что и код, исправляющий классические ошибки. В частности, он имеет такую же минимальную степень совпадения и, следовательно, тот же критерий большей надежности по сравнению с отсутствием исправления ошибок. Мы можем назвать каналы с фазовой и классической ошибками *унитарно эквивалентными*, так как существует такой унитарный оператор U (преобразование Адамара), что действие одного канала совпадает с действием другого, если на вход первого канала применяется оператор U , а на выходе U^\dagger . Эти операторы могут быть включены в схемы кодирования и исправления ошибок; для произвольных унитарных операторов эта идея отражена в задаче 10.1.

Упражнение 10.4. Рассмотрим трехкубитовый код, исправляющий классические ошибки. Предположим, что мы находим синдром ошибки, измеряя восемь ортогональных проекторов на состояния вычислительного базиса.

- (1) Укажите соответствующие проекторы и объясните, как нужно интерпретировать результаты измерений? Как определить, произошла ли ошибка, и если произошла, то в каком из трех кубитов?

- (2) Покажите, что процедура восстановления может быть выполнена только для состояний вычислительного базиса.
- (3) Какова минимальная степень совпадения для такой процедуры исправления ошибок?

10.2 Код Шора

Существует простой квантовый код для исправления произвольной ошибки в одном кубите. По имени создателя он назван *кодом Шора*. Этот код является комбинацией трехкубитовых кодов, исправляющих классические и фазовые ошибки. Кубит сначала кодируется кодом, исправляющим фазовую ошибку, $|0\rangle \rightarrow |+++ \rangle$, $|1\rangle \rightarrow |--- \rangle$, а затем каждый из полученных кубитов кодируется кодом, исправляющим классическую ошибку: $|+\rangle \rightarrow (|000\rangle + |111\rangle)/\sqrt{2}$, $|-\rangle \rightarrow (|000\rangle - |111\rangle)/\sqrt{2}$. Получается девятикубитовый код с кодовыми словами

$$\begin{aligned} |0\rangle \rightarrow |0_L\rangle &\equiv \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}, \\ |1\rangle \rightarrow |1_L\rangle &\equiv \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}. \end{aligned} \quad (10.13)$$

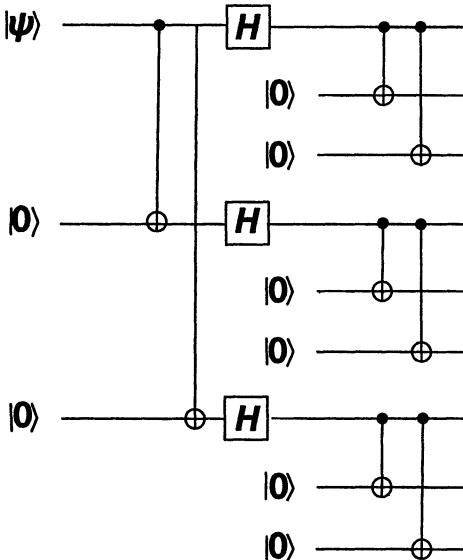


Рис. 10.4. Кодирующая схема для девятикубитового кода Шора. Часть состояний $|0\rangle$ изображена с отступом, чтобы показать, что эта схема получена объединением двух предыдущих

Кодирующая схема для кода Шора показана на рис. 10.4. Первая часть схемы такая же, как для кода, исправляющего фазовую ошибку (ср. с рис. 10.3).

Вторая часть — три копии схемы для кода, исправляющего классическую ошибку (рис. 10.2). Такое объединение кодов называют *каскадным*. Аналогичным образом можно строить новые коды из комбинации уже известных; мы будем пользоваться этим методом для получения некоторых важных результатов относительно исправления квантовых ошибок.

Код Шора исправляет как фазовую так и классическую ошибку в любом кубите. Чтобы показать это, предположим сначала, что произошла классическая ошибка в первом кубите. Как в случае кода, исправляющего классическую ошибку, мы производим измерение Z_1Z_2 и находим, что первые два кубита различаются. Это показывает, что ошибка произошла в одном из них. После этого мы сравниваем второй и третий кубиты. Производя измерение Z_2Z_3 , находим, что они совпадают. Мы делаем вывод, что ошибка произошла в первом кубите и исправляем ее, переворачивая этот кубит. Аналогично мы можем обнаружить и исправить ошибку в любом из девяти кубитов.

Подобным образом мы поступаем с фазовой ошибкой. Предположим, что она произошла в первом кубите. При этом изменится знак в первом блоке кубитов: $|000\rangle + |111\rangle$ изменится на $|000\rangle - |111\rangle$ и наоборот. Более того, к такому изменению приведет фазовая ошибка в *любом* из первых трех кубитов. Процедура, которую мы сейчас опишем, исправит любую из этих трех ошибок. Нахождение синдрома начинается со сравнения знака первого и второго блоков кубитов. Например, блоки $(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$ имеют одинаковый знак, а $(|000\rangle - |111\rangle)(|000\rangle + |111\rangle)$ — разные. Если фазовая ошибка произошла в каком-то из первых трех кубитов, мы обнаружим, что знаки первого и второго блоков различны. После этого мы сравниваем знаки второго и третьего блоков и находим, что они совпадают. Мы делаем вывод, что ошибка произошла в первом блоке из трех кубитов и исправляем ее, меняя знак первого блока. Так можно исправить ошибку в любом из девяти кубитов.

Упражнение 10.5. Покажите, что нахождение синдрома для обнаружения фазовой ошибки в коде Шора эквивалентно измерению $X_1X_2X_3X_4X_5X_6$ и $X_4X_5X_6X_7X_8X_9$.

Упражнение 10.6. Покажите, что исправление фазовой ошибки в одном из трех первых кубитов может быть выполнено с помощью оператора $Z_1Z_2Z_3$.

Предположим теперь, что в первом кубите возникли и классическая и фазовая ошибки, т. е. на него подействовал оператор Z_1X_1 . Легко видеть, что в этом случае процедура исправления классической ошибки обнаружит и исправит классическую ошибку, а процедура исправления фазовой ошибки обнаружит и исправит фазовую ошибку в первом блоке из трех кубитов. Таким образом, код Шора может исправить комбинацию из классической и фазовой ошибок в одном кубите.

Более того, сейчас мы покажем, что код Шора может исправить *произвольную* ошибку, при условии, что она произошла только в одном кубите. Ошибка может быть очень маленькой вроде поворота сферы Блоха на угол $\pi/263$ радиан вокруг оси z или, наоборот, очень большой, вроде замены кубита на произвольное неправильное состояние. Интересно, что для исправления таких ошибок нам не потребуется никакой дополнительной работы: толь-

ко что описанная процедура хорошо подходит для этого случая. Это пример той необычной ситуации, когда *непрерывное* множество ошибок одного кубита может быть исправлено с помощью процедуры, исправляющей некоторое *дискретное* подмножество ошибок. Все остальные возможные ошибки исправляются автоматически. Такая дискретизация делает исправление квантовых ошибок возможным в отличие от исправления классических ошибок в аналоговых вычислительных системах, где подобная дискретизация невозможна.

Чтобы упростить рассмотрение, предположим, что произвольная ошибка возникает только в первом кубите. Потом мы вернемся к случаю, когда шуму подвержены и другие кубиты. В соответствии с материалом, изложенным в гл. 8, мы описываем шум сохраняющим след квантовым преобразованием \mathcal{E} . Нам удобно представить преобразование \mathcal{E} в виде операторной суммы с элементами $\{E_i\}$. Предположим, что состояние закодированного кубита до возникновения ошибки $|\psi\rangle = \alpha|0_L\rangle + \beta|1_L\rangle$. Состояние после действия шума будет $\mathcal{E}(|\psi\rangle\langle\psi|) = \sum_i E_i |\psi\rangle\langle\psi| E_i^\dagger$. Рассмотрим один из членов суммы, $E_i |\psi\rangle\langle\psi| E_i^\dagger$. Так как оператор E_i действует только на первый кубит, его можно представить в виде линейной комбинации тождественного оператора I , оператора классической ошибки X_1 , оператора фазовой ошибки Z_1 и $X_1 Z_1$.

$$E_i = e_{i0}I + e_{i1}X_1 + e_{i2}Z_1 + e_{i3}X_1Z_1 \quad (10.14)$$

Квантовое состояние $E_i |\psi\rangle$ (ненормированное) может быть записано как суперпозиция состояний $|\psi\rangle$, $X_1|\psi\rangle$, $Z_1|\psi\rangle$ и $X_1Z_1|\psi\rangle$. Измерение синдрома ошибки переведет это состояние в одно из четырех состояний $|\psi\rangle$, $X_1|\psi\rangle$, $Z_1|\psi\rangle$ или $X_1Z_1|\psi\rangle$. Исходное состояние $|\psi\rangle$ может быть восстановлено из каждого из них выполнением соответствующей операции. Все это верно и для других элементов преобразования E_i . Таким образом, восстановление исходного состояния возможно независимо от вида ошибки. Это основное и очень важное свойство квантового исправления ошибок: квантовый код, исправляющий некоторое дискретное множество ошибок (фазовую, классическую или их комбинацию, как в этом примере), способен автоматически исправлять гораздо большее (непрерывное!) множество ошибок.

Что же происходит, когда шуму подвержено более одного кубита? С этим вопросом нам помогут разобраться две простые идеи. Во-первых, во многих случаях можно приближенно считать, что шум действует на кубиты независимо. Если влияние шума на кубит достаточно мало, можно представить действие шума в виде суммы с членами, соответствующими отсутствию ошибки, ошибке в одном, двух и т.д. кубитах. При этом первые два члена будут много больше остальных. Исправляя ошибку, мы избавляемся от этих двух членов и оставляем члены более высокого порядка, получая суммарное уменьшение ошибки. Более подробный анализ этой идеи будет дан ниже. Иногда, конечно, нельзя предполагать, что шум действует на кубиты независимо. В этом случае мы используем другой подход: коды, исправляющие ошибки в более чем одном кубите. Такие коды могут быть построены способом, аналогичным построению кода Шора. Основные идеи того, как это может быть сделано, мы объясним позднее в этой главе.

10.3 Теория исправления квантовых ошибок

Можем ли мы построить общую теорию кодов, исправляющих квантовые ошибки? В этом разделе приводятся основы такой теории, в том числе *условия исправления квантовых ошибок* — набор уравнений, которые должны выполняться, чтобы исправление ошибок было возможно. Конечно, это не гарантирует существование хороших кодов, исправляющих квантовые ошибки. Этот вопрос мы обсудим в разд. 10.4, но сначала мы получим базу, необходимую для построения таких кодов.

Основные идеи теории кодов, исправляющих квантовые ошибки, являются естественным обобщением идей, введенных при описании кода Шора. Квантовые состояния кодируются некоторым унитарным оператором в *код, исправляющий квантовые ошибки*, который определяется как подпространство C некоторого большего гильбертова пространства. Введем обозначение P для проектора на это подпространство. Для трехкубитового кода, исправляющего классические ошибки, $P = |000\rangle\langle 000| + |111\rangle\langle 111|$. После кодирования на полученное состояние действует шум, вызывая некоторую ошибку. Затем производятся измерения и определяется тип возникшей ошибки, ее *синдром*. После этого выполняется операция *восстановления*, которая возвращает квантовую систему в исходное состояние. Эта простая картина проиллюстрирована на рис. 10.5: различные синдромы ошибки соответствуют ортогональным подпространствам в гильбертовом пространстве. Подпространства должны быть ортогональны, иначе их будет невозможно различить при измерении синдромов. Более того, все подпространства должны быть недеформированными версиями исходного пространства кодов в том смысле, что при действии ошибки ортогональность кодов должна сохраняться, чтобы можно было восстановить исходное состояние. Эта интуитивная картина и является содержанием условий исправления квантовых ошибок, описанных ниже.

Чтобы разработать общую теорию исправления квантовых ошибок, нужно сделать как можно меньше предположений о природе шума и о процедуре, используемой для исправления ошибок. Мы не будем предполагать, что исправление ошибок происходит в два этапа (обнаружение ошибки и восстановление исходного состояния) и что шум в системе кубитов слабый. Вместо этого мы предположим только, что шум описывается квантовым преобразованием \mathcal{E} , а полная процедура исправления ошибки — сохраняющим след преобразованием \mathcal{R} , которое назовем *преобразованием исправления ошибки*. Это преобразование объединяет обнаружение ошибки и восстановление исходного состояния. Для успешного исправления ошибки мы потребуем, чтобы для любого состояния ρ , носитель которого лежит в подпространстве C ,

$$(\mathcal{R} \circ \mathcal{E})(\rho) \propto \rho. \quad (10.15)$$

Вам может показаться странным, почему мы написали \propto вместо $=$. Если \mathcal{E} — сохраняющее след квантовое преобразование, то взяв след от обеих частей формулы, мы увидим, что \propto перейдет в $=$. Однако, иногда мы будем рассматривать при исправлении ошибок не сохраняющее след квантовое преобразование \mathcal{E} .

В этих случаях больше подходит знак \propto . Конечно, преобразование \mathcal{R} должно исправлять ошибку с вероятностью 1, поэтому мы потребовали, чтобы \mathcal{R} сохраняло след.

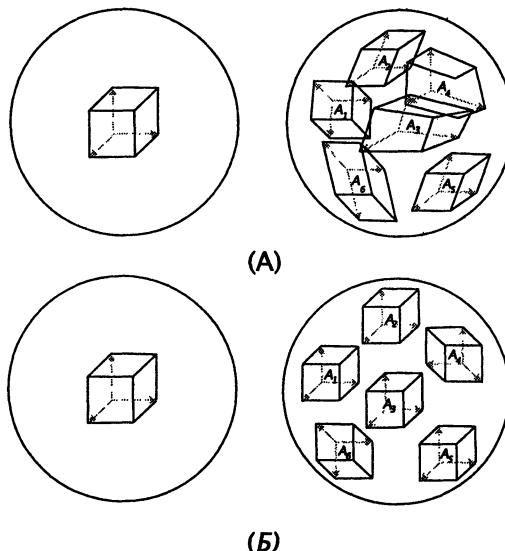


Рис. 10.5. Гильбертово пространство при квантовом кодировании А—плохой код с неортогональными деформированными подпространствами, Б—хороший код с ортогональными (различными) недеформированными подпространствами.

Условия исправления квантовых ошибок это простой набор уравнений, которые надо проверить, чтобы убедиться, что код, исправляющий квантовые ошибки, может защитить от шума \mathcal{E} . Мы используем эти условия, чтобы построить различные квантовые коды и исследовать их общие свойства.

Теорема 10.1 (условия исправления квантовых ошибок). Пусть C — квантовый код, а P — проектор на C . Предположим, что \mathcal{E} — квантовое преобразование с элементами $\{E_i\}$. Для существования квантового преобразования \mathcal{R} , исправляющего шум \mathcal{E} на множестве C , необходимо и достаточно, чтобы

$$PE_i^\dagger E_j P = \alpha_{ij} P, \quad (10.16)$$

где α — некоторая эрмитова матрица.

Мы называем элементы преобразования $\{E_i\}$ шума \mathcal{E} *ошибками*, и если такое \mathcal{R} существует, говорим, что $\{E_i\}$ является *исправляемым множеством ошибок*.

Доказательство.

Докажем сначала достаточность (10.16), явно построив преобразование \mathcal{R} , при условии, что равенство (10.16) выполняется. Мы используем конструкцию из двух частей, как и в коде Шора — обнаружение ошибки и восстановление исходного состояния и покажем таким образом что исправление ошибки всегда

может быть выполнено в виде такой двухшаговой процедуры. Пусть $\{E_i\}$ — набор элементов преобразования, удовлетворяющий условию (10.16). По определению, α — эрмитова матрица и, следовательно, она может быть приведена к диагональному виду, $d = u^\dagger \alpha u$, где u — некоторая унитарная матрица, а d диагональна. Определим операторы $F_k \equiv \sum_i u_{ik} E_i$. Согласно теореме 8.2, $\{F_i\}$ — тоже набор элементов преобразования \mathcal{E} . Прямой подстановкой получаем

$$PF_k^\dagger F_l P = \sum_{ij} u_{ki}^\dagger u_{jl} P E_i^\dagger E_j P. \quad (10.17)$$

Подстановка сюда выражения (10.16) дает $PF_k^\dagger F_l P = \sum_{ij} u_{ki}^\dagger \alpha_{ij} u_{jl} P$. Так как $d = u^\dagger \alpha u$, получаем

$$PF_k^\dagger F_l P = d_{kl} P. \quad (10.18)$$

Таким образом, мы упростили условие исправления квантовых ошибок (10.16), так как d_{kl} диагональна.

Используем упрощенное условие (10.18) и полярное разложение (подразд. 2.1.10), чтобы найти синдромы. Из полярного разложения получаем $F_k P = U_k \sqrt{P F_k^\dagger F_k P} = \sqrt{d_{kk}} U_k P$ для некоторого унитарного оператора U_k . Таким образом, F_k поворачивает подпространство кода в подпространство, определяемое проектором $P_k \equiv U_k P U_k^\dagger = F_k P U_k^\dagger / \sqrt{d_{kk}}$. Равенство (10.18) предполагает, что эти подпространства ортогональны при $k \neq l$,

$$P_l P_k = P_l^\dagger P_k = \frac{U_l P F_l^\dagger F_k P U_k^\dagger}{\sqrt{d_{ll} d_{kk}}} = 0. \quad (10.19)$$

Нахождение синдромов — это проективные измерения, определяемые проектором P_k и возможно, еще одним проектором, чтобы выполнялось условие полноты: $\sum_k P_k = I$. Восстановление исходного состояния производится операторами U_k^\dagger . Заметим, что полная процедура исправления ошибки соответствует преобразованию $\mathcal{R}(\sigma) = \sum_k U_k^\dagger P_k \sigma P_k U_k$. Для состояния ρ из этого кода простые вычисления дают

$$U_k^\dagger P_k F_l \sqrt{\rho} = U_k^\dagger P_k^\dagger F_l P \sqrt{\rho} \quad (10.20)$$

$$= \frac{U_k^\dagger U_k P F_k^\dagger F_l P \sqrt{\rho}}{\sqrt{d_{kk}}} \quad (10.21)$$

$$= \delta_{kl} \sqrt{d_{kk}} P \sqrt{\rho} \quad (10.22)$$

$$= \delta_{kl} \sqrt{d_{kk}} \sqrt{\rho}. \quad (10.23)$$

Таким образом,

$$\mathcal{R}(\mathcal{E}(\rho)) = \sum_{kl} U_k^\dagger P_k F_l \rho F_l^\dagger P_k U_k = \quad (10.24)$$

$$= \sum_{kl} \delta_{kl} d_{kk} \rho \propto \quad (10.25)$$

$$\propto \rho, \quad (10.26)$$

что и требовалось.

Чтобы доказать необходимость условия исправления квантовых ошибок (10.16), предположим, что $\{E_i\}$ — множество ошибок, которые могут быть исправлены преобразованием \mathcal{R} с элементами $\{R_j\}$. Определим квантовое преобразование как $\mathcal{E}_C(\rho) \equiv \mathcal{E}(P\rho P)$. Поскольку $P\rho P$ находится в подпространстве кода для любого ρ ,

$$\mathcal{R}(\mathcal{E}_C(\rho)) \propto P\rho P, \quad (10.27)$$

для всех ρ . Коэффициент пропорциональности c не зависит от ρ , так как обе части уравнения должны быть линейными по ρ . Если переписать это соотношение в терминах элементов преобразования, то получим

$$\sum_{ij} R_j E_i P \rho P E_i^\dagger R_j^\dagger = c P \rho P. \quad (10.28)$$

Это равенство справедливо для всех ρ . Отсюда следует, что преобразование с элементами $\{R_j E_i\}$ идентично преобразованию с единственным элементом $\sqrt{c}P$. Из теоремы 8.2 видно, что существуют такие комплексные числа c_{ki} , что

$$R_k E_i P = c_{ki} P \quad (10.29)$$

Сопряженное равенство имеет вид $P E_i^\dagger R_k^\dagger = c_{ki}^* P$ и, следовательно, $P E_i^\dagger R_k^\dagger R_k E_j P = c_{ki}^* c_{kj} P$. Но \mathcal{R} — преобразование, сохраняющее след, поэтому $\sum_k R_k^\dagger R_k = I$. Суммирование $P E_i^\dagger R_k^\dagger R_k E_j P = c_{ki}^* c_{kj} P$ по k дает

$$P E_i^\dagger E_j P = \alpha_{ij} P, \quad (10.30)$$

где $\alpha_{ij} = \sum_k c_{ki}^* c_{kj}$ — некоторая эрмитова матрица. Мы получили условие квантового исправления ошибок. ■

Непосредственная проверка условия исправления квантовых ошибок — простая, но долгая процедура. В разделах 10.4 и 10.5 мы введем теоретический формализм, в котором используется условие исправления квантовых ошибок в качестве основы для построения множества интересных классов кодов, и исключаются сложности, связанные с прямой проверкой условия исправления квантовых ошибок. Пока же предлагаем вам упражнение, показывающее условие квантового исправления ошибок в действии.

Упражнение 10.7. Рассмотрим трехкубитовый код, исправляющий классические ошибки (подразд. 10.1.1) и соответствующий проектор $P = |000\rangle\langle 000| + |111\rangle\langle 111|$. Шум, от которого защищает этот код, имеет следующие элементы преобразования: $\{\sqrt{(1-p)^3}I, \sqrt{p(1-p)^2}X_1, \sqrt{p(1-p)^2}X_2, \sqrt{p(1-p)^2}X_3\}$, где p — вероятность классической ошибки. Заметим, что это преобразование не сохраняет след, так как мы пренебрегли элементами преобразования, которые соответствуют ошибкам в двух и трех кубитах. Проверьте условие квантового исправления ошибок для данного кода и шумового процесса.

Вставка 10.1. Исправление квантовых ошибок без измерения

В основном тексте мы описываем исправление квантовых ошибок как процесс, состоящий из двух частей: обнаружение ошибки с использованием квантового измерения, и восстановление исходного состояния с помощью унитарного оператора, зависящего от результата измерения. Можно исправлять ошибки, используя только унитарные операторы и вспомогательные системы в приготовленных заранее состояниях. Такой метод полезен для некоторых реальных квантовых систем, в которых сложно провести необходимые измерения. Мы действуем практически так же, как в гл. 8, где объясняется, как расширить произвольное квантовое преобразование до унитарного. Сейчас мы повторим основные идеи применительно к исправлению квантовых ошибок.

Предположим, что измерение синдромов ошибок в основной системе описывается операторами M_i , а U_i — соответствующие им унитарные операторы. Введем вспомогательную систему с базисными состояниями $|i\rangle$, соответствующими возможным синдромам ошибок. Перед исправлением ошибок эта система переводится в состояние $|0\rangle$. Определим унитарный оператор U , действующий на основную и вспомогательную системы, как

$$U|\psi\rangle|0\rangle \equiv \sum_i (U_i M_i |\psi\rangle)|i\rangle. \quad (10.31)$$

Этот унитарный оператор может быть также определен на всем пространстве состояний, поскольку

$$\langle\varphi| \langle 0 | U^\dagger U |\psi\rangle |0\rangle = \sum_{ij} \langle\varphi| M_i^d a g M_j |\psi\rangle \delta_{ij} \quad (10.32)$$

$$= \sum_i \langle\varphi| M_i^d a g M_i |\psi\rangle \quad (10.33)$$

$$= \langle\varphi||\psi\rangle, \quad (10.34)$$

т. е. U сохраняет скалярные произведения и, следовательно, может быть обобщен на все пространство состояний. Действие оператора U на систему совпадает с действием преобразования $\mathcal{R}(\sigma) = \sum_i U_i M_i \sigma M_i^\dagger U_i^d a g$. Точно такое же преобразование было определено в основном тексте для исправления квантовых ошибок. Заметим, что для того, чтобы процедура исправления ошибок работала, нужно приводить вспомогательную систему в исходное состояние.

10.3.1 Дискретизация ошибок

Мы обсудили защиту квантовой информации от определенного шумового процесса \mathcal{E} . Однако, в общем случае не известно, какой шум действует на квантовую систему. Было бы полезно, если бы некоторый код C и преобразова-

ние исправления ошибок \mathcal{R} могли защитить систему от целого класса шумов. К счастью, условие квантового исправления ошибок легко модифицировать так, чтобы оно предоставляло именно такую защиту.

Теорема 10.2. Предположим, что C — квантовый код, а \mathcal{R} — преобразование исправления ошибок, построенное в доказательстве теоремы 10.1 для защиты от шума \mathcal{E} с элементами преобразования $\{E_i\}$. Пусть \mathcal{F} — преобразование с элементами $\{F_i\}$, которые являются линейными комбинациями $\{E_i\}$, т. е. $F_j = \sum_i m_{ji} E_i$, где m_{ji} — матрица с комплексными элементами. Тогда преобразование исправления ошибок \mathcal{R} также исправляет ошибки, вызванные шумом \mathcal{F} .

Доказательство.

Согласно теореме 10.1, элементы преобразования $\{E_i\}$ должны удовлетворять условию исправления квантовых ошибок $PE_i E_j^\dagger P = \alpha_{ij} P$. Как показано в доказательстве теоремы 10.1, элементы преобразования \mathcal{E} могут быть выбраны так, что $\alpha_{ij} = d_{ij}$ — диагональная матрица с действительными элементами. Преобразование исправления ошибок \mathcal{R} имеет элементы в соответствии с $U_k^\dagger P_k$, где равенством (10.23) U_k и P_k выбраны так, что для любого ρ из пространства кода

$$U_k^\dagger P_k E_i \sqrt{\rho} = \delta_{ki} \sqrt{d_{kk}} \sqrt{\rho}. \quad (10.35)$$

Подставив сюда $F_i = \sum_i m_{ij} E_i$, получим

$$U_k^\dagger P_k F_j \sqrt{\rho} = \sum_i m_{ji} \delta_{ki} \sqrt{d_{kk}} \sqrt{\rho} \quad (10.36)$$

$$= m_{jk} \sqrt{d_{kk}} \sqrt{\rho}, \quad (10.37)$$

и, следовательно,

$$\mathcal{R}(\mathcal{F}(\rho)) = \sum_{kj} U_k^\dagger P_k F_j \rho F_j^\dagger P_k U_k \quad (10.38)$$

$$= \sum_{kj} |m_{jk}|^2 d_{kk} \rho \propto \quad (10.39)$$

$$\propto \rho, \quad (10.40)$$

что и требовалось доказать. ■

Этот результат позволяет ввести более эффективный язык для описания квантовых кодов, исправляющих ошибки. Вместо того, чтобы говорить о том, что класс ошибок \mathcal{E} может быть исправлен кодом C и преобразованием исправления ошибок \mathcal{R} , можно сказать, что набор операторов ошибки (или просто ошибок) $\{E_i\}$ исправляем. Под этим мы подразумеваем, что для этих операторов выполняется условие исправления квантовых ошибок

$$P E_i^\dagger E_j P = \alpha_{ij} P. \quad (10.41)$$

Из теорем 10.1 и 10.2 видно, что любой шумовой процесс \mathcal{E} с элементами преобразования, являющимися линейными комбинациями операторов ошибок $\{E_i\}$, может быть исправлен с помощью преобразования исправления ошибок \mathcal{R} !

Рассмотрим пример применения этого подхода. Пусть \mathcal{E} — квантовое преобразование, действующее на один кубит. Тогда его элементы $\{E_i\}$ могут быть записаны в виде линейной комбинации матриц Паули $\sigma_0, \sigma_1, \sigma_2, \sigma_3$. Следовательно, чтобы проверить, что код Шора может исправить произвольную ошибку в первом кубите, достаточно проверить равенство

$$P\sigma_i^1\sigma_j^1P = \alpha_{ij}P, \quad (10.42)$$

где σ_i^1 — матрицы Паули (I, X, Y и Z), действующие на первый кубит. Если это равенство выполняется, можно быть уверенными, что любая ошибка в первом кубите может быть исправлена! (Проверить это равенство достаточно просто, что является частью упражнения 10.10). Этот результат объясняет одно явление, которое может показаться загадочным при первом знакомстве с литературой по исправлению квантовых ошибок: многие авторы уделяют особое внимание деполяризующему каналу $\mathcal{E}(\rho) = (1-p)\rho + p/3(X\rho X + Y\rho Y + Z\rho Z)$. Может показаться, что это сильно ограничивает применимость их моделей исправления ошибок, но это не так. Только что мы показали, что способность исправлять ошибки деполяризующего канала автоматически дает возможность исправлять произвольные однокубитовые ошибки.

Таким образом, мы выяснили, что квантовые ошибки могут быть дискретизированы, так как для исправления непрерывного множества ошибок одного кубита достаточно исправить лишь конечный набор ошибок: четыре матрицы Паули. Подобный результат справедлив и для многокомпонентных квантовых систем. Это совершенно непохоже на исправление ошибок в классических аналоговых системах. В таких системах исправление ошибок очень сложно из-за бесконечного числа синдромов ошибок. Исправление ошибок при классической цифровой обработке информации намного успешнее, благодаря конечному числу синдромов ошибки. Удивительно, что исправление квантовых ошибок гораздо больше похоже на цифровое, чем на аналоговое классическое исправление ошибок.

Упражнение 10.8. Проверьте, что трехкубитовый код, исправляющий фазовые ошибки $|0_L\rangle = |+++>, |1_L\rangle = |--->$, удовлетворяет условию исправления квантовых ошибок для набора операторов $\{I, Z_1, Z_2, Z_3\}$.

Упражнение 10.9. Опять рассмотрим трехкубитовый код, исправляющий фазовые ошибки. Пусть P_i и Q_i — проекторы на состояния $|0\rangle$ и $|1\rangle$ соответственно для кубита i . Докажите, что трехкубитовый код, исправляющий фазовые ошибки, защищает от множества ошибок $\{I, P_1, Q_1, P_2, Q_2, P_3, Q_3\}$.

Упражнение 10.10. Проверьте прямым вычислением условие исправления квантовых ошибок для кода Шора и набора операторов ошибок, состоящего из I и X_j, Y_j, Z_j для $j = 1\dots 9$.

Упражнение 10.11. Найдите элементы однокубитового квантового преобразования \mathcal{E} , которое заменяет входное состояние ρ на совершенно случайное состояние $I/2$. Удивительно, что даже такие ошибки могут быть исправлены кодами типа кода Шора!

10.3.2 Модели независимых ошибок

Как объединить исправление квантовых ошибок и критерий надежности квантовых вычислений, введенный в гл. 9? Мы объясним здесь, как это может быть сделано с использованием предположения о *независимости ошибок* в разных кубитах. Интуитивно понятно, что если шумовой процесс действует независимо на разные кубиты, то при условии, что шум достаточно слабый, исправление ошибок должно приводить к увеличению степени совпадения. Чтобы проиллюстрировать это, мы начнем с рассмотрения деполяризующего канала, который особенно просто демонстрирует основные идеи. Затем распространим эти идеи на другие важные типы каналов.

Вспомним, что деполяризующий канал может быть описан одним параметром, а именно, вероятностью p . Действие такого канала на один кубит определено формулой $\mathcal{E}(\rho) = (1 - p)\rho + p/3(X\rho X + Y\rho Y + Z\rho Z)$. Кубит остается неизменным с вероятностью $(1 - p)$ и подвергается действию операторов X , Y или Z с вероятностью $p/3$. Деполяризующий канал особенно легко рассматривать в терминах исправления квантовых ошибок, так как он просто описывается четырьмя основными операторами ошибок I , X , Y и Z , которые чаще всего используются при анализе квантовых кодов. Мы обсудим деполяризующий канал и затем вернемся к рассмотрению процессов, не имеющих такой простой интерпретации в терминах I , X , Y и Z . Простое вычисление показывает, что минимальная степень совпадения для состояний, переданных по деполяризующему каналу, $F = \sqrt{1 - 2p/3} = 1 - p/3 + O(p^2)$.

Упражнение 10.12. Покажите, что степень совпадения для состояний $|0\rangle$ и $\mathcal{E}(|0\rangle\langle 0|)$ равна $\sqrt{1 - 2p/3}$ и, используя это, докажите, что минимальная степень совпадения для деполяризующего канала равна $\sqrt{1 - 2p/3}$.

Предположим, что мы кодируем один кубит информации квантовым кодом из n кубитов, который исправляет ошибки в одном кубите. Пусть деполяризующий канал с параметром p действует независимо на каждый кубит; суммарное действие на n кубитов описывается выражением

$$\mathcal{E}^{\otimes n}(\rho) = (1 - p)^n\rho + \sum_{j=1}^n \sum_{k=1}^3 (1 - p)^{n-1} \frac{p}{3} \sigma_k^j \rho \sigma_k^j + \dots, \quad (10.43)$$

где многоточием обозначены положительные слагаемые более высокого порядка, которые мы не рассматриваем. После исправления ошибок все члены этой суммы вернутся к состоянию ρ при условии, что ρ принадлежит коду:

$$(\mathcal{R} \otimes \mathcal{E}^{\otimes n})(\rho) = [(1 - p)^n + n(1 - p)^{n-1}p]\rho + \dots \quad (10.44)$$

Степень совпадения будет удовлетворять соотношению

$$F > \sqrt{(1 - p)^{n-1}(1 - p + np)} = 1 - \frac{\binom{n}{2}}{2}p^2 + O(p^3). \quad (10.45)$$

Таким образом, если вероятность ошибки p достаточно мала, использование кода, исправляющего ошибку, увеличивает степень совпадения закодированных квантовых состояний.

Не все каналы с шумом могут быть описаны просто случайной комбинацией отсутствия ошибки, классической ошибки, и фазовой ошибки, и сочетания классической и фазовой ошибок. Многие реальные квантовые каналы не имеют такой интерпретации. Рассмотрим пример затухания амплитуды (см. подразд. 8.3.5) с элементами преобразования E_0 и E_1 :

$$E_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix}, \quad E_1 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix}. \quad (10.46)$$

Параметр γ — небольшое положительное число, характеризующее величину затухания амплитуды; при уменьшении γ до нуля затухание ослабевает и канал становится бесшумным. Естественно было бы предположить, что канал с затуханием амплитуды имеет эквивалентное описание в терминах набора элементов преобразования, причем один из элементов пропорционален тождественному оператору, $\{f(\gamma)I, E'_1, E'_2, \dots\}$, где $f(\gamma) \rightarrow 1$ при $\gamma \rightarrow 0$. Если это так, то канал с затуханием амплитуды, действующий на кубиты независимо, можно рассматривать так же, как и деполяризующий канал. Однако оказывается, что такое описание канала с затуханием амплитуды невозможно! Это следует из теоремы 8.2 просто потому, что для $\gamma > 0$ не существует линейной комбинации E_0 и E_1 , пропорциональной тождественному оператору, и, следовательно, множество элементов преобразования для канала с затуханием амплитуды не может содержать такой член.

Аналогично многие другие шумовые процессы в квантовой механике в физическом смысле близкие к тождественным, не могут быть представлены операторной суммой с большой тождественной компонентой. Интуитивно понятно, что и в этом случае исправление ошибки должно привести к увеличению степени совпадения квантовой информации, если шум достаточно слаб. Сейчас мы покажем, что это действительно так, используя в качестве примера канал с затуханием амплитуды. Простое вычисление показывает, что минимальная степень совпадения для такого канала, действующего на один кубит, равна $\sqrt{1-\gamma}$. Предположим теперь, что кубит кодируется n -кубитовым квантовым кодом, способным исправлять произвольные ошибки в одном кубите, и что канал с затуханием амплитуды с параметром γ действует независимо на каждый кубит. Мы покажем в общих чертах, что исправление квантовых ошибок позволяет достичь степени совпадения до $1-O(\gamma^2)$, так что для малых значений γ кодирование кубита дает уменьшение ошибки.

Упражнение 10.13. Покажите, что минимальная степень совпадения $F(|\psi\rangle, \mathcal{E}(|\psi\rangle\langle\psi|))$, где \mathcal{E} — преобразование для канала с затуханием амплитуды с параметром γ , равна $\sqrt{1-\gamma}$. Вводя обозначение $E_{j,k}$ для действия E_j на k -й кубит, запишем действие шума на закодированные кубиты в виде

$$\begin{aligned}\mathcal{E}^{\otimes n}(\rho) = & (E_{0,1} \otimes E_{0,2} \otimes \cdots \otimes E_{0,n})\rho(E_{0,1}^\dagger \otimes E_{0,2}^\dagger \otimes \cdots \otimes E_{0,n}^\dagger) \\ & + \sum_{j=1}^n \left[E_{1,j} \otimes \left(\bigotimes_{k \neq j} E_{0,k} \right) \right] \rho \left[E_{1,j}^\dagger \otimes \left(\bigotimes_{k \neq j} E_{0,k}^\dagger \right) \right] \\ & + O(\gamma^2).\end{aligned}\quad (10.47)$$

Подставив выражение $E_0 = (1 - \gamma/4)I + \gamma Z/4 + O(\gamma^2)$, $E_1 = \sqrt{\gamma}(X + iY)/2$ в (10.47), получим

$$\begin{aligned}\mathcal{E}^{\otimes n}(\rho) = & \left(1 - \frac{\gamma}{4}\right)^{2n} \rho + \frac{\gamma}{4} \left(1 - \frac{\gamma}{4}\right)^{2n-1} \sum_{j=1}^n (Z_j \rho + \rho Z_j) \\ & + \frac{\gamma}{4} \left(1 - \frac{\gamma}{4}\right)^{2n-2} \sum_{j=1}^n (X_j + iY_j) \rho (X_j - iY_j) + O(\gamma^2).\end{aligned}\quad (10.48)$$

Пусть ρ — состояние из пространства кодов. Очевидно, что исправление ошибки не должно менять его. Влияние слагаемых $Z_j \rho$ и ρZ_j легче всего понять, рассматривая $Z_j |\psi\rangle\langle\psi|$, где $|\psi\rangle$ — состояние из пространства кодов. По предположению, код таков, что ошибка Z_j переводит $|\psi\rangle$ в подпространство, ортогональное пространству кода, так что при определении синдрома члены $Z_j |\psi\rangle\langle\psi|$ исчезают. (Заметим, что даже если не предполагать ортогональность, подобное рассмотрение может быть проведено в терминах операторов ошибки, которые переводят состояние из пространства кода в ортогональные пространства.) Таким образом члены $Z_j \rho$, ρZ_j , $X_j \rho Y_j$ и $Y_j \rho X_j$ исчезают после исправления ошибки, а члены $X_j \rho X_j$ и $Y_j \rho Y_j$ переходят в ρ , так как код может исправлять ошибки в одном кубите. После исправление ошибок состояние системы будет иметь вид

$$\left(1 - \frac{\gamma}{4}\right)^{2n} \rho + 2n \frac{\gamma}{4} \left(1 - \frac{\gamma}{4}\right)^{2n-2} \rho + O(\gamma^2) = \rho + O(\gamma^2). \quad (10.49)$$

Таким образом, с точностью до членов порядка γ^2 исправление ошибки возвращает квантовую систему к исходному состоянию ρ , и при слабом шуме (γ мало) исключает ошибки, как и в случае деполяризующего канала. Наше рассмотрение было проведено для канала с затуханием амплитуды, однако его несложно распределить и на другие модели шума. Однако, в этой главе мы в основном будем работать с моделями шума, которые можно представить стохастическим набором операторов ошибок, соответствующих матрицам Паули, как в случае деполяризующего канала. Это позволит нам использовать методы классической теории вероятностей. Рассмотренные идеи можно распространить на более широкий класс моделей шума способом, подобным тому, который мы только что описали.

10.3.3 Вырожденные коды

Коды, исправляющие квантовые ошибки, во многом похожи на коды, исправляющие классические ошибки. Как и в классическом случае, ошибка определяется путем измерения синдрома и затем исправляется. Однако существует интересный класс кодов, исправляющих квантовые ошибки, так называемые *вырожденные коды*, которые существенно отличаются от кодов, исправляющих классические ошибки. Это можно показать на примере кода Шора. Рассмотрим действие ошибок Z_1 и Z_2 на закодированное кодом Шора состояние. Как мы уже отмечали, действие этих ошибок *одинаково* для состояний $|0_L\rangle$ и $|1_L\rangle$. В классическом случае ошибки в разных битах обязательно ведут к различным результатам. Вырожденные коды имеют как достоинства, так и недостатки. С одной стороны, к ним неприменимы классические методы доказательства, используемые для получения условий исправления ошибок. Мы увидим это в следующем подразделе, где рассматривается квантовая граница Хэмминга. С другой стороны, вырожденные коды — одни из самых интересных квантовых кодов! В некотором смысле они могут «содержать в себе больше информации», чем классические коды, так как различные ошибки не обязательно должны переводить пространство кодов в ортогональные подпространства. Возможно (хотя еще и не доказано), что это позволит создать вырожденный код, сохраняющий информацию более эффективно, чем любой невырожденный код.

10.3.4 Квантовая граница Хэмминга

Для различных приложений нужны по возможности «наилучшие» квантовые коды. Что означает слово «наилучшие» — зависит от конкретной задачи. По этой причине нам хотелось бы иметь некоторый критерий, который определяет, существует ли код с заданными характеристиками. В этом разделе мы рассмотрим квантовую границу Хэмминга — простое неравенство, дающее некоторую информацию об общих свойствах квантовых кодов. К сожалению, это неравенство применимо лишь к невырожденным кодам, но оно даст нам идеи, как должны выглядеть более общие неравенства. Пусть невырожденный код используется для кодирования k кубитов n кубитами так, что исправление ошибки возможно в любом наборе из t или меньшего числа кубитов. Допустим, произошло j ошибок, причем $j \leq t$. Возможны $\binom{n}{j}$ вариантов расположения ошибочных кубитов. Для каждого из них существует 3^j возможных ошибок (в каждом кубите может произойти одна из трех ошибок — X , Y и Z). Следовательно, полное число возможных ошибок в t или меньшем числе кубитов равно

$$\sum_{j=0}^t \binom{n}{j} 3^j. \quad (10.50)$$

(Обратите внимание, что $j = 0$ соответствует отсутствию ошибки, т. е. «ошибке I .») Чтобы закодировать k кубитов невырожденным способом, все ошиб-

ки должны соответствовать попарноортогональным 2^k -мерным подпространствам в 2^n -мерном пространстве. Из этого следует неравенство

$$\sum_{j=0}^t \binom{n}{j} 3^j 2^k \leq 2^n. \quad (10.51)$$

Это и есть квантовая граница Хэмминга. Пусть, например, мы кодируем один кубит n кубитами так, чтобы любая ошибка в одном из кубитов могла быть исправлена. В этом случае граница Хэмминга имеет вид

$$2(1 + 3n) \leq 2^n. \quad (10.52)$$

Подстановка показывает, что неравенство выполняется только при $n \geq 5$. Следовательно, не существует невырожденный код, кодирующий один кубит менее, чем пятью кубитами, и способный исправить любые ошибки в одном кубите.

Конечно, не все квантовые коды невырождены, так что граница Хэмминга не является универсальным критерием существования квантового кода. (Тем не менее на момент написания книги не известно кодов, даже вырожденных, которые нарушили бы границу Хэмминга). Позже мы приведем неравенства, которые могут быть применимы к любым квантовым кодам. Например, в подразд. 12.4.3 мы докажем квантовую границу Синглтона: любой код, кодирующий k кубитов n кубитами и исправляющий ошибки в t кубитах, должен удовлетворять неравенству $n \geq 4t + k$. Отсюда следует, что для наименьшего кода, кодирующего один кубит и исправляющего любую ошибку в одном кубите, должно выполняться неравенство $n \geq 4 + 1 = 5$, то есть он должен быть пятикубитовым.

10.4 Построение квантовых кодов

Теперь мы имеем теоретическую основу для изучения квантовых кодов, исправляющих ошибки, но у нас еще нет достаточного количества примеров таких кодов. Чтобы исправить это, мы начнем с краткого введения в теорию классических линейных кодов в подразд. 10.4.1, затем в подразд. 10.4.2 объясним, как идеи теории классических линейных кодов могут быть использованы для построения большого класса квантовых кодов, известных как коды Кальдербанка – Шора – Стина (CSS коды). Разд. 10.5 посвящен симплектическим кодам, еще более широкому классу кодов, чем CSS коды, который обеспечивает эффективные средства для построения большого числа различных квантовых кодов.

10.4.1 Классические линейные коды

Классические коды, исправляющие ошибки, имеют множество технических приложений, так что неудивительно, что хорошо разработана теория для таких кодов. Наш интерес к методам классического исправления ошибок вызван тем,

что многие из них могут быть использованы при исправлении квантовых ошибок. Особенно интересна теория *классических линейных кодов*, которая может быть применена для разработки большого числа хороших квантовых кодов, исправляющих ошибки. В этом разделе дан обзор классических линейных кодов, причем основное внимание уделено идеям, важным для исправления квантовых ошибок.

Линейный код C , кодирующий k битов информации в n -битовое пространство кода, задается *порождающей* (образующей) матрицей G размера $n \times k$ с элементами из пространства Z_2 (т. е. с нулями и единицами). Матрица G преобразует исходное сообщение в код; k -битовое сообщение x кодируется в Gx , где x рассматривается как γ -вектор столбец. Умножение и все другие арифметические операции в этом разделе производятся по модулю 2. В качестве простого примера рассмотрим образующую матрицу кода с повторением, которая преобразует один бит в три его копии:

$$G = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}. \quad (10.53)$$

Умножение матрицы G на возможные входные сообщения 0 и 1 преобразует их в закодированную форму: $G[0] = (0, 0, 0)$ и $G[1] = (1, 1, 1)$. (Напомним, что (a, b, \dots, z) — более короткое обозначение для вектора-столбца). Назовем код, кодирующий k битов информации n битами $[n, k]$ -кодом. Наш пример, таким образом, является $[3, 1]$ -кодом. Несколько более сложный пример — кодирование двух битов тройным повторением каждого из них — $[6, 2]$ -код. Образующая матрица для такого кода

$$G = \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}. \quad (10.54)$$

Действительно,

$$G(0, 0) = (0, 0, 0, 0, 0, 0), \quad G(0, 1) = (0, 0, 0, 1, 1, 1), \quad (10.55)$$

$$G(1, 0) = (1, 1, 1, 0, 0, 0), \quad G(1, 1) = (1, 1, 1, 1, 1, 1). \quad (10.56)$$

Множество возможных кодовых слов является линейной оболочкой столбцов матрицы G , поэтому, чтобы все сообщения кодировались единственным способом, мы должны потребовать, чтобы столбцы G были линейно независимы. Других ограничений на G мы не накладываем.

Упражнение 10.14. Приведите выражение для образующей матрицы, которая преобразует каждый из k битов в r его копий. Это линейный $[rk, k]$ -код, его порождающая матрица должна иметь размер $rk \times k$.

Упражнение 10.15. Покажите, что прибавление одного столбца G к другому даст порождающую матрицу для того же кода.

Большим преимуществом линейных кодов по сравнению с другими кодами является их компактная запись. Чтобы задать произвольный код, кодирующий k битов n битами, потребуется 2^k кодовых слов, каждое длиной n . Такой код полностью описывается $n2^k$ битами информации. Для линейного кода необходимо задать только kn битов образующей матрицы. Таким образом мы имеем экспоненциальную экономию объема памяти! Компактное описание обеспечивает простоту кодирования и декодирования. Это очень важное свойство классических линейных кодов, а также их квантовых аналогов — симплектических кодов. Мы видим, что кодирование линейным кодом заключается в умножении k -битового сообщения на порождающую матрицу $n \times k$. Эта процедура может быть выполнена с помощью $O(nk)$ операций.

Описание линейных кодов с помощью порождающей матрицы позволяет легко производить кодирование. Процесс исправления ошибки не так очевиден. Однако, он становится легко понятным при другом (эквивалентном) описании линейных кодов с помощью *проверочной матрицы*. По определению, $[n, k]$ -код состоит из всех n -элементных векторов x в пространстве \mathbb{Z}_2 , таких, что

$$Hx = 0, \quad (10.57)$$

где матрица H с элементами 0 или 1 имеет размер $(n - k) \times n$ и называется *проверочной матрицей*. То же самое, но более кратко: код является ядром матрицы H . Код, кодирующий k битов, имеет 2^k возможных кодовых слов, поэтому ядро H должно быть k -мерным и, следовательно, мы должны потребовать линейную независимость строк H .

Упражнение 10.16. Покажите, что прибавление одной строки проверочной матрицы H к другой не изменит код. Используя метод исключения Гаусса и перестановки битов, можно привести проверочную матрицу к *стандартному виду* $[A|I_{n-k}]$, где A — матрица $(n - k) \times k$.

Чтобы установить взаимосвязь между описаниями линейных кодов через порождающую матрицу и через проверочную матрицу, нужно разработать процедуру преобразования матрицы проверки на четность H в образующую матрицу G и обратно. Чтобы перейти от проверочной матрицы к порождающей матрице, выберем k линейно независимых векторов y_1, \dots, y_k , для которых ядро H является линейной оболочкой. Матрицу G составим из столбцов y_1, \dots, y_k . Чтобы перейти от порождающей матрицы к проверочной матрице, возьмем $n - k$ линейно независимых векторов (y_1, \dots, y_{n-k}) , ортогональных столбцам G , и составим матрицу H из строк $(y_1^T, \dots, y_{n-k}^T)$. (Под ортогональностью мы понимаем равенство нулю скалярного произведения по модулю 2.) В качестве примера рассмотрим $[3, 1]$ -код с повторением, заданный порождающей матрицей (10.53). Чтобы построить H , возьмем $3 - 1 = 2$ линейно независимых вектора, ортогональных столбцам G , например $(1, 1, 0)$ и $(0, 1, 1)$ и определим проверочную матрицу как

$$H \equiv \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}. \quad (10.58)$$

Легко проверить, что $Hx = 0$ только для кодовых слов $x = (0, 0, 0)$ и $x = 1, 1, 1$.

Упражнение 10.17. Найдите проверочную матрицу для [6, 2]-кода с повторением, заданного порождающей матрицей (10.54).

Упражнение 10.18. Покажите, что проверочная матрица и порождающая матрица для одного и того же кода удовлетворяют условию $HG = 0$.

Упражнение 10.19. Пусть линейный $[n, k]$ -код C имеет проверочную вида $H = [A|I_{n-k}]$, где A — некоторая матрица размера $(n - k) \times k$. Покажите, что соответствующая порождающая матрица

$$G = \begin{bmatrix} I_k \\ -A \end{bmatrix}. \quad (10.59)$$

(Можно заметить, что $A = -A$, так как мы работаем в пространстве \mathbb{Z}_2 . Однако, это равенство справедливо для линейных кодов не только в пространстве \mathbb{Z}_2 , но и в более общем случае.)

Проверочная матрица делает достаточно очевидным процесс обнаружения и исправления ошибки. Пусть мы кодируем сообщение x сообщением $y = Gx$, но из-за шума возникает ошибка e , преобразующая закодированное сообщение в $y' = y + e$. (Здесь $+$ обозначает побитовое сложение по модулю 2.) Так как $Hy = 0$ для любого закодированного сообщения, $Hy' = He$. Мы назовем Hy' *синдромом ошибки*. Его роль похожа на роль синдрома в исправлении квантовых ошибок; он является функцией испорченного ошибкой состояния y' подобно квантовому синдрому, который определяется результатом измерения испорченного квантового состояния. В соответствии с соотношением $Hy' = He$ синдром содержит информацию об ошибке, что позволяет восстановить исходное закодированное сообщение y . Чтобы увидеть, как это может быть сделано, предположим, что ошибка произошла не более, чем в одном бите. Синдром Hy' равен нулю в случае отсутствия ошибки и равен He_j , если ошибка произошла в j -ом бите. Здесь e_j — вектор с единственным ненулевым j -ом элементом равным 1. Если предположить, что ошибка произошла не более, чем в одном бите, то можно исправить ошибку. Вычислив синдром Hy' и сравнив его с различными возможными значениями He_j , мы определим, в каком бите произошла ошибка (это возможно при $He_j \neq He_k$ для $j \neq k$. — Ред.).

Вопрос о том, как можно исправлять ошибки с помощью линейного кода, с более общих позиций можно рассмотреть с использованием *метрики*. Пусть x и y — n -битовые сообщения. *Метрика* (Хэмминга) $d(x, y)$ для x и y вводится, как число различающихся позиций в x и y . Например, $d((1, 1, 0, 0), (0, 1, 0, 1)) = 2$. *Весом* (Хэмминга) для сообщения x называется расстояние в метрике Хэмминга от x до сообщения, состоящего из одних нулей $\text{wt}(x) \equiv d(x, 0)$, т. е. число ненулевых битов в x . Обратите внимание, что $d(x, y) = \text{wt}(x + y)$. Предположим, что мы кодируем x сообщением $y = Gx$ с помощью линейного кода.

Под действием шума в закодированном сообщении возникает ошибка, преобразующая сообщение в $y' = y + e$. Если вероятность изменения бита меньше $1/2$, то кодовое слово вероятнее всего таково, что число измененных битов в y' по сравнению с y минимально, т. е. y такое, что $\text{wt}(e) = d(y, y')$ минимально. В принципе исправление ошибки может быть произведено просто заменой y' на такой y . На практике, однако, это может быть довольно неэффективно, так как определение минимального расстояния $d(y, y')$ в общем случае требует перебора 2^k возможных кодовых слов y . Важной задачей классической теории кодирования является построение кодов специального вида, позволяющих исправлять ошибки более эффективно. Мы не рассматриваем такие построения в этой книге.

Общие свойства кодов также могут быть описаны с помощью метрики Хэмминга. Определим *кодовое расстояние* как минимальное расстояние между двумя кодовыми словами:

$$d(C) \equiv \min_{x, y \in C, x \neq y} d(x, y). \quad (10.60)$$

Но $d(x, y) = \text{wt}(x + y)$. Если x и y — кодовые слова, то из линейности кода следует, что $x + y$ — также кодовое слово. Отсюда получаем, что

$$d(C) = \min_{x \in C, x \neq 0} \text{wt}(x). \quad (10.61)$$

Вводя обозначение $d \equiv d(C)$, мы говорим, что код C является $[n, k, d]$ -кодом. Важность кодового расстояния состоит в том, что код с кодовым расстоянием, не меньшим $2t + 1$ для некоторого положительного t , может исправлять ошибки в не большее, чем t битах просто заменяя испорченное состояние y' единственным кодовым словом y , таким, что $d(y, y') \leq t$.

Упражнение 10.20. Пусть H — проверочная матрица такая, что любые ее $d - 1$ столбцы линейно независимы, но существует набор из линейно d зависимых столбцов. Покажите, что код, заданный матрицей H , имеет кодовое расстояние d .

Упражнение 10.21 (граница Синглтона). Покажите, что $[n, k, d]$ -код должен удовлетворять неравенству $n - k \geq d - 1$.

Хорошим примером класса линейных кодов, исправляющих ошибки, являются коды Хэмминга. Пусть $r \geq 2$ и H — матрица с $2^r - 1$ столбцами битов длины r , не равными тождественно нулю. Такая проверочная матрица определяет линейный $[2^r - 1, 2^r - r - 1]$ -код, который называется *кодом Хэмминга*. Особенno важен для исправления квантовых ошибок случай $r = 3$, $[7, 4]$ -код с проверочной матрицей

$$H \equiv \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}. \quad (10.62)$$

Любые два столбца H различны и, следовательно, линейно независимы. Первые три столбца линейно зависимы, поэтому из упр. 10.20 следует, что кодовое расстояние для такого кода равно 3. Таким образом, код может исправлять ошибку в одном бите. Процедура исправления ошибки очень простая. Пусть ошибка возникла в j -ом бите. Из матрицы (10.62) видно, что синдром ошибки He_j — это просто двоичное представление j , показывающее, какой бит нужно изменить, чтобы исправить ошибку.

Упражнение 10.22. Покажите, что все коды Хэмминга имеют кодовое расстояние 3 и, следовательно, могут исправлять ошибку в одном бите. Т. е. коды Хэммига — $[2^r - 1, 2^r - r - 1, 3]$ -коды.

Что можно сказать относительно общих свойств линейных кодов? В частности, нам хотелось бы получить условия существования кодов с заданными параметрами. Не удивительно, что существует много методов для получения таких условий. Один такой набор условий называется *границей Варшамова–Гильберта*: для больших n существует $[n, k]$ -код, исправляющий ошибки в t битах, для некоторого k , такого, что

$$\frac{n}{k} \geq 1 - H\left(\frac{t}{n}\right), \quad (10.63)$$

где $H(x) \equiv -x \log(x) - (1-x) \log(1-x)$ — двоичная шенноновская энтропия, которая будет подробно рассмотрена в гл. 11. Важность границы Варшамова–Гильберта заключается в том, что она гарантирует существование хороших кодов при условии, что не слишком большое количество битов (k) кодируется не слишком маленьким количеством битов (n). Доказательство границы Варшамова–Гильберта достаточно просто и оставлено в качестве упражнения.

Упражнение 10.23. Докажите границу Варшамова–Гильберта.

Мы завершим наш обзор теории классического исправления ошибок введением понятия *двойственности*. Пусть C — $[n, k]$ -код с порождающей матрицей G и проверочной матрицей H . Можно построить другой код, C^\perp , *двойственный* коду C с порождающей матрицей H^T и проверочной матрицей G^T . Другими словами, код, двойственный коду C , содержит все возможные кодовые слова сообщения y , каждое из которых ортогонально всем сообщениям кода C . Код называется слабо самодвойственным, если $C \subseteq C^\perp$ и строго самодвойственным, если $C = C^\perp$. Построение двойственного кода естественным образом возникает в теории исправления квантовых ошибок и является основой построения важного класса квантовых кодов — CSS кодов.

Упражнение 10.24. Покажите, что код с порождающей матрицей G слабо самодвойственный тогда и только тогда, когда $G^T G = 0$.

Упражнение 10.25. Пусть C — линейный код. Покажите, что если $x \in C^\perp$, то $\sum_{y \in C} (-1)^{xy} = |C|$, а если $x \notin C^\perp$, то $\sum_{y \in C} (-1)^{xy} = 0$

10.4.2 Коды Кальдербанка–Шора–Стина

Наш первый пример большого класса квантовых кодов исправляющих ошибки — коды Кальдербанка–Шора–Стина, также называемые CSS кодами. CSS коды являются важным подклассом симплектических кодов.

Пусть C_1 и C_2 — классические линейные $[n, k_1]$ и $[n, k_2]$ -коды, такие, что $C_2 \subset C_1$, а C_1 и C_2^\perp могут исправить t ошибок. Построим квантовый $[n, k_1 - k_2]$ -код $\text{CSS}(C_1, C_2)$, способный исправлять ошибки в t кубитах, CSS код C_1 по C_2 , следующим образом. Допустим, что $x \in C_1$ — любое кодовое слово из C_1 . Введем квантовое состояние $|x + C_2\rangle$:

$$|x + C_2\rangle \equiv \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y\rangle, \quad (10.64)$$

где $+$ означает побитовое сложение по модулю 2. Пусть x' — элемент C_1 такой, что $x - x' \in C_2$. Легко видеть, что $|x + C_2\rangle = |x' + C_2\rangle$, и, следовательно, состояние $|x + C_2\rangle$ зависит только от класса смежности C_1/C_2 , в котором находится x . Это объясняет обозначение, которое мы использовали для $|x + C_2\rangle$. Кроме того, если x и x' принадлежат к разным классам смежности по C_2 , то не существует таких $y, y' \in C_2$, для которых $x + y = x' + y'$ и, следовательно, $|x + C_2\rangle$ и $|x' + C_2\rangle$ — ортонормированные состояния. Определим квантовый код $\text{CSS}(C_1, C_2)$ как линейную оболочку состояний $|x + C_2\rangle$ для всех $x \in C_1$. Число классов смежности C_2 в C_1 равно $|C_1|/|C_2|$, так что размерность $\text{CSS}(C_1, C_2)$ равна $|C_1|/|C_2| = 2^{k_1 - k_2}$ и, следовательно, $\text{CSS}(C_1, C_2)$ является $[n, k_1 - k_2]$ -кодом.

Мы можем использовать классические свойства C_1 и C_2^\perp для обнаружения и исправления квантовых ошибок. Действительно, с помощью кода $\text{CSS}(C_1, C_2)$ можно исправить до t классических и фазовых ошибок, используя свойства C_1 и C_2^\perp соответственно. Предположим, что классическая ошибка описывается n -битовым вектором e_1 , в котором единицы расположены в местах, где произошла ошибка, а нули в остальных местах. Фазовая ошибка описывается n -битовым вектором e_2 . Если исходное состояние было $|x + C_2\rangle$, то испорченное ошибками состояние равно

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)\dot{e}_2} |x + y + e_1\rangle. \quad (10.65)$$

Для обнаружения классической ошибки удобно ввести вспомогательную систему из достаточного количества кубитов для хранения синдрома кода C_1 . Все вспомогательные кубиты вначале находятся в состоянии $|0\rangle$. Мы используем обратимое вычисление, чтобы применить проверочную матрицу H_1 кода C_1 , преобразовав состояние $|x + y + e_1\rangle|0\rangle$ в $|x + y + e_1\rangle|H_1(x + y + e_1)\rangle = |x + y + e_1\rangle|H_1e_1\rangle$ (так как член $x + y \in C_1$ уничтожается проверочной матрицей). В результате этой операции получим состояние

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)\dot{e}_2} |x + y + e_1\rangle|H_1e_1\rangle. \quad (10.66)$$

Упражнение 10.26. Пусть H — проверочная матрица. Объясните, как выполнить преобразование $|x\rangle|0\rangle \rightarrow |x\rangle|Hx\rangle$, используя схему, состоящую только

из элементов CNOT. Обнаружение ошибки производится измерением вспомогательного состояния. В результате измерения получаем H_1e_1 . Исключение вспомогательной системы дает

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y) \cdot e_2} |x + y + e_1\rangle. \quad (10.67)$$

Зная синдром ошибки H_1e_1 , можно определить ошибку e_1 , так как код C_1 может исправлять до t ошибок. Исправление выполняется простым применением элементов NOT к кубитам, соответствующим ненулевым позициям в e_1 . После исправления получаем состояние

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y) \cdot e_2} |x + y\rangle. \quad (10.68)$$

Чтобы обнаружить фазовую ошибку, мы применяем элемент Адамара к каждому кубиту. При этом получаем состояние

$$\frac{1}{\sqrt{|C_2|2^n}} \sum_z \sum_{y \in C_2} (-1)^{(x+y) \cdot (e_2+z)} |z\rangle, \quad (10.69)$$

где сумма берется по всем возможным n -битовым z . Введя обозначение $z' = z + e_2$, получим

$$\frac{1}{\sqrt{|C_2|2^n}} \sum_{z'} \sum_{y \in C_2} (-1)^{(x+y) \cdot z'} |z' + e_2\rangle. \quad (10.70)$$

Легко показать (см. упр. 10.25), что если $z' \in C_2^\perp$, то $\sum_{y \in C_2} (-1)^{y \cdot z'} = |C_2|$, а если $z' \notin C_2^\perp$, то $\sum_{y \in C_2} (-1)^{y \cdot z'} = 0$. Поэтому можно переписать состояние следующим образом:

$$\frac{1}{\sqrt{2^n/|C_2|}} \sum_{z' \in C_2^\perp} (-1)^{x \cdot z'} |z' + e_2\rangle. \quad (10.71)$$

Это выражение очень похоже на то, которое было получено для случая классической ошибки, заданной вектором e_2 ! Как и при исправлении классической ошибки, мы вводим вспомогательную систему и обратным образом применяем проверочную матрицу H_2 для кода C_2^\perp , чтобы определить синдром H_2e_2 . Затем, исправив «классическую ошибку» e_2 , получаем состояние

$$\frac{1}{\sqrt{2^n/|C_2|}} \sum_{z' \in C_2^\perp} (-1)^{x \cdot z'} |z'\rangle. \quad (10.72)$$

После этого применяем элемент Адамара к каждому кубиту. Мы можем получить непосредственно этот результат; тот же результат получается, если применить элементы Адамара к состоянию (10.71) с $e_2 = 0$. Так как элемент Адамара совпадает с обратным элементом Адамара, вернемся к состоянию (10.68) с $e_2 = 0$:

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y\rangle, \quad (10.73)$$

т. е. к исходному закодированному состоянию.

Важным применением CSS кодов является доказательство квантового аналога границы Варшамова–Гильберта, гарантирующей существование хороших квантовых кодов. В пределе больших n квантовый $[n, k]$ -код, способный исправлять ошибки в t и менее кубитах, существует для некоторых k , таких, что

$$\frac{n}{k} \geq 1 - 2H\left(\frac{2t}{n}\right), \quad (10.74)$$

Таким образом, существует хороший квантовый код, исправляющий ошибки, если только не пытаться кодировать n кубитами слишком большое число кубитов k . Доказательство границы Варшамова–Гильберта для CSS кодов гораздо сложнее, чем в классическом случае из-за ограничений на классические коды C_1 и C_2 . Оно оставлено в качестве задачи в конце главы.

Итак, C_1 и C_2 — классические линейные $[n, k_1]$ и $[n, k_2]$ -коды соответственно, такие, что $C_2 \subset C_1$, а C_1 и C_2^\perp способны исправлять ошибки в t или менее битах. $\text{CSS}(C_1, C_2)$ — квантовый $[n, k_1 - k_2]$ -код, способный исправлять произвольные ошибки не более, чем в t кубитах. Для обнаружения и исправления ошибок требуются только элементы Адамара и CNOT, причем их количество линейно зависит от размера кода. Число элементов, выполняющих кодирование и декодирование, также линейно зависит от размера кода. Мы не обсуждаем этот вопрос здесь, в более общем виде он будет рассмотрен в подразд. 10.5.8.

Упражнение 10.27. Покажите, что код, заданный формулой

$$|x + C_2\rangle \equiv \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{u \cdot y} |x + y + v\rangle \quad (10.75)$$

с параметрами u и v , эквивалентен коду $\text{CSS}(C_1, C_2)$ в том смысле, что оба кода имеют одинаковые свойства исправления ошибок. Такой код будем называть в дальнейшем $\text{CSS}_{u,v}(C_1, C_2)$; он будет полезен нам при изучении квантового распределения ключей в подразд. 12.6.5.

Код Стина

Важный пример CSS кода можно построить, используя $[7, 4, 3]$ -код Хэмминга с проверочной матрицей

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}. \quad (10.76)$$

Обозначим этот код через C , и введем $C_1 \equiv C$ и $C_2 \equiv C^\perp$. Чтобы использовать C_1 и C_2 для построения CSS кода, проверим сначала, что $C_2 \subset C_1$.

По определению, проверочная матрица кода $C_2 = C^\perp$ равна транспонированной порождающей матрице кода $C_1 = C$:

$$H[C_2] = G[C_1]^T = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}. \quad (10.77)$$

Упражнение 10.28. Проверьте, что транспонированная матрица (10.77) является порождающей матрицей $[7, 4, 3]$ -кода Хэмминга. Сравнивая матрицы (10.77) и (10.76), мы видим, что линейная оболочка строк $H[C_2]$ строго содержит линейную оболочку строк $H[C_2]$, и, так как соответствующие коды являются ядрами этих матриц, мы делаем вывод, что $C_2 \subset C_1$. Кроме того, поскольку $C_2^\perp = (C^\perp)^\perp = C$ и C_1 и C_2^\perp имеют кодовое расстояние 3 и способны исправлять ошибки в одном бите. Так как C_1 является $[7, 4]$ -кодом, а C_2^\perp — $[7, 3]$ -кодом, то $\text{CSS}(C_1, C_2)$ — квантовый $[7, 1]$ -код, способный исправлять ошибки в одном кубите.

Этот квантовый $[7, 1]$ -код нам будет удобно использовать в примерах этой главы. По имени создателя он называется *кодом Стина*. Кодовые слова из C_2 могут быть легко получены из (10.77) и упр. 10.28. Мы не будем выписывать их явно, а запишем их в качестве составляющих состояния $|0_L\rangle$ кода Стина, $|0 + C_2\rangle$:

$$\begin{aligned} |0_L\rangle = \frac{1}{\sqrt{8}} & \left[|0000000\rangle + |1010101\rangle + |0110011\rangle \right. \\ & + |1100110\rangle + |0001111\rangle + |1011010\rangle \\ & \left. + |0111100\rangle + |1101001\rangle \right]. \end{aligned} \quad (10.78)$$

Чтобы определить другое кодовое слово кода Стина, нужно найти элемент C_1 , не содержащийся в C_2 . Таким элементом, например, является $(1, 1, 1, 1, 1, 1, 1)$. Для $|1_L\rangle$ получаем:

$$\begin{aligned} |1_L\rangle = \frac{1}{\sqrt{8}} & \left[|1111111\rangle + |0101010\rangle + |1001100\rangle \right. \\ & + |0011001\rangle + |1110000\rangle + |0100101\rangle \\ & \left. + |1000011\rangle + |0010110\rangle \right]. \end{aligned} \quad (10.79)$$

10.5 Симплектические коды

*Мы когерентность делим, чтоб спасти
Её, когда один нарушил бит,
У нас ошибка встанет на пути
И время вычислений удлинит.*

*Так можем сдвиг по фазе мы учесть.
Когда же ошибка вновь вкрадется в код,
Её мы измеряем – и Бог весть,
По X, по Y или Z она пойдет.*

*Из зашумленных девяти, семи, пяти
Один выводим точный. Чтобы сбой
Отсечь, мы данные должны найти,
Что коммутировать способны меж собой.*

*Призвав на память группы, мы учтем
Ошибки квантовым путем.*

Сонет по исправлению квантовых ошибок
Д. Готтесмана

Симплектические (стабилизирующие) коды являются важным классом квантовых кодов. Они строятся аналогично классическим линейным кодам. Чтобы понять симплектические коды, полезно сначала разработать *формализм стабилизаторов*, эффективный метод описания широкого класса квантовомеханических преобразований. Применение формализма стабилизаторов выходит далеко за пределы квантового исправления ошибок. Однако, в этой книге мы используем его в основном для этой цели. После введения формализма стабилизаторов мы покажем, как с его помощью можно описать унитарные элементы и измерения, а также приведем важную теорему, определяющую ограничения на применение стабилизаторов. Затем опишем построение симплектических кодов, приведем конкретные примеры кодов и схемы для кодирования, декодирования и исправления.

10.5.1 Формализм стабилизаторов

Основная идея формализма стабилизаторов может быть проиллюстрирована следующим примером. Рассмотрим ЭПР состояние двух кубитов

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \quad (10.80)$$

Легко проверить, что это состояние удовлетворяет равенствам $X_1X_2|\psi\rangle = |\psi\rangle$ и $Z_1Z_2|\psi\rangle = |\psi\rangle$; мы говорим, что состояние $|\psi\rangle$ *стабилизируется* операторами X_1X_2 и Z_1Z_2 . Очевидно, что это единственное такое состояние с точностью до общего фазового множителя. Основная идея формализма стабилизаторов за-

ключается в том, что для большого числа квантовых состояний проще работать с операторами, которые стабилизируют их, чем собственно с этими состояниями. Это утверждение на первый взгляд достаточно удивительно, однако оно верно. Оказывается, что многие квантовые коды, в том числе CSS коды и код Шора, гораздо более компактно описываются стабилизаторами, чем векторами состояний. Что более важно, ошибки в кубитах, операции, подобные элементу Адамара, фазовому элементу и даже CNOT элементу, а также измерения в вычислительном базисе легко описываются формализмом стабилизаторов.

Основная причина эффективности формализма стабилизаторов заключается в использовании *теории групп*, основные элементы которой приведены в Приложении 2. Наиболее интересная для нас группа — группа Паули G_n для n кубитов. Для одного кубита группа Паули определена как множество всех матриц Паули с множителями ± 1 и $\pm i$:

$$G_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}. \quad (10.81)$$

Этот набор матриц образует группу по отношению к операции матричного умножения. Вам может показаться странным, почему мы не опустили множители ± 1 и $\pm i$. Причина этого в том, что эти множители делают множество G_1 замкнутым по отношению к умножению, а это необходимо, чтобы G_1 было группой. Группа Паули для n кубитов определяется как множество, содержащее все возможные тензорные произведения из n матриц Паули также с множителями ± 1 и $\pm i$.

Теперь мы можем более точно ввести понятие стабилизатора. Пусть S — подгруппа G_n . Обозначим через V_S множество n -кубитовых состояний, которые сохраняются под действием любого элемента из S . V_S называется *векторным пространством, стабилизированным S*, а S называется *стабилизатором* пространства V_S . Предлагаем вам убедиться в правильности утверждения следующего упражнения.

Упражнение 10.29. Покажите, что произвольная линейная комбинация элементов V_S принадлежит V_S . Следовательно, V_S является подпространством n -мерного пространства состояний кубитов. Покажите, что V_S является пересечением подпространств, стабилизируемых каждым оператором из S (т. е. пересечением собственных пространств, соответствующих собственному числу 1, всех элементов S).

Рассмотрим простой пример действия формализма стабилизаторов. Пусть $n = 3$ и $S = \{I, Z_1Z_2, Z_2Z_3, Z_1Z_3\}$. Подпространство, стабилизируемое оператором Z_1Z_2 , является линейной оболочкой векторов $|000\rangle, |001\rangle, |110\rangle$, и $|111\rangle$; подпространство, стабилизируемое оператором Z_2Z_3 , является линейной оболочкой векторов $|000\rangle, |100\rangle, |011\rangle$, и $|111\rangle$. Элементы $|000\rangle$ и $|111\rangle$ — общие для этих двух наборов. Уже из этого можно заключить, что V_S в данном случае — линейная оболочка этих двух векторов.

В этом примере мы определили V_S , рассмотрев подпространства, стабилизируемые только двумя операторами из S . Это показывает возможность описания группы с помощью ее *образующих*. Как определяется в Приложении 2,

элементы g_1, \dots, g_l из группы G называются ее образующими, если любой элемент группы может быть записан в виде произведения элементов из набора g_1, \dots, g_l . В этом случае мы записываем $G = \langle g_1, \dots, g_l \rangle$. В нашем примере $S = \langle Z_1Z_2, Z_2Z_3 \rangle$, так как $Z_1Z_3 = (Z_1Z_2)(Z_2Z_3)$ и $I = (Z_1Z_2)^2$. Большим преимуществом такого способа описания групп является его *компактность*. Действительно, в Приложении 2 показано, что группа G размера $|G|$ имеет не более $\log(|G|)$ образующих. Кроме того, чтобы проверить, что некоторый вектор стабилизируется группой S , достаточно проверить, что он стабилизируется образующими группы; если это так, то вектор стабилизируется и любыми произведениями образующих. Это делает такое представление групп наиболее удобным для нас. (Обозначение $\langle \dots \rangle$, которое мы используем для образующих группы, совпадает с обозначением для средних наблюдаемых величин, введенных в подразд. 2.2.5, однако на практике всегда ясно, как это обозначение используется.)

Не все подгруппы S группы Паули являются стабилизаторами нетривиального векторного пространства. Рассмотрим, например, подгруппу G_1 , состоящую из элементов $\{\pm I, \pm X\}$. Очевидно, что единственное решение уравнения $(-I)|\psi\rangle = |\psi\rangle$ есть $|\psi\rangle = 0$, и, следовательно, группа $\{\pm I, \pm X\}$ является стабилизатором тривиального векторного пространства. Каким же условиям должна удовлетворять S , чтобы стабилизировать нетривиальное векторное пространство V_S ? Можно легко указать два условия: необходимо, чтобы (а) элементы S коммутировали и (б) $-I$ не являлся элементом S . Эти условия являются и достаточными; мы докажем это позже.

Упражнение 10.30. Покажите, что из $-I \notin S$ следует $\pm iI \notin S$.

Чтобы увидеть, почему эти условия являются необходимыми, предположим, что V_S — нетривиальное векторное пространство, т. е. оно содержит ненулевой вектор $|\psi\rangle$. Пусть N и M — элементы S . Эти элементы являются тензорными произведениями матриц Паули, возможно с некоторым общим множителем. Поскольку матрицы Паули коммутируют или антисимметричны, то и N и M должны коммутировать или антисимметричны. Чтобы доказать условие (а), допустим, что N и M антисимметричны. При этом $-NM = MN$ и мы имеем $-|\psi\rangle = -NM|\psi\rangle = MN|\psi\rangle = |\psi\rangle$, где первое и последнее равенство следуют из того, что N и M стабилизируют $|\psi\rangle$. Итак, мы имеем $-|\psi\rangle = |\psi\rangle$; это означает, что $|\psi\rangle$ — нулевой вектор. Мы пришли к противоречию, так как $|\psi\rangle$ — ненулевой вектор. Следовательно, N и M должны коммутировать. Чтобы доказать условие (б), что $-I \notin S$, заметим, что если $-I$ является элементом S , то мы имеем $-I|\psi\rangle = |\psi\rangle$, что опять ведет к противоречию.

Упражнение 10.31. Пусть S — подгруппа G_n с образующими g_1, \dots, g_l . Покажите, что все элементы S коммутируют тогда и только тогда, когда g_i и g_j коммутируют для любой пары i, j .

Хорошим примером использования формализма стабилизаторов является семибитовый код Стина. Оказывается, что шесть образующих $g_1 \dots g_6$; по-

казанных на рис. 10.6, задают стабилизатор кодового пространства кода Стина. Оцените, насколько яснее и компактнее такое описание по сравнению с достаточно запутанным описанием через векторы состояний (10.78) и (10.79). Дополнительные преимущества проявятся, когда мы будем рассматривать исправление квантовых ошибок с этой точки зрения. Обратите также внимание на похожую структуру образующих на рис. 10.6 и проверочных матриц классических линейных кодов C_1 и C_2^\perp , использованных для построения кода Стина. (Для кода Стина код $C_1 = C_2^\perp$ является [7, 4, 3]-кодом Хэмминга с проверочной матрицей (10.76).) Первые три образующих стабилизатора содержат X в позициях, соответствующих единицам в проверочной матрице для кода C_1 . Остальные три образующих содержат Z в позициях, соответствующих единицам в проверочной матрице для кода C_2^\perp . Используя этот факт, легко выполнить следующее упражнение.

Образующая	Оператор
g_1	$III XXXX$
g_2	$I XXI XXX$
g_3	$X IXIX IX$
g_4	$III ZZZZ$
g_5	$IZZI IZZZ$
g_6	$ZIZIZIZ$

Рис. 10.6. Образующие стабилизатора для семикубитового кода Стина. Каждый элемент представляет собой тензорное произведение соответствующих кубитов. Например, $ZIZIZIZ = Z \otimes I \otimes Z \otimes I \otimes Z \otimes I \otimes Z = Z_1 Z_3 Z_5 Z_7$

Упражнение 10.32. Проверьте, что образующие, показанные на рис. 10.6, стабилизируют кодовые слова кода Стина, приведенные в подразд. 10.4.2. Подобным образом мы будем использовать формализм стабилизаторов для описания широкого класса квантовых кодов. Сейчас важно понять, что нет ничего необычного в коде Стина: это всего лишь подпространство векторного пространства, которое может быть описано с помощью стабилизаторов.

Мы хотим, чтобы образующие g_1, \dots, g_i были *независимы* в том смысле, что удаление одного из них делает задаваемую ими группу меньше:

$$\langle g_1, \dots, g_{i-1}, g_{i+1}, \dots, g_l \rangle \neq \langle g_1, \dots, g_l \rangle \quad (10.82)$$

Определить прямым вычислением, является ли набор образующих независимым, достаточно трудоемко. К счастью, это можно сделать простым способом, основанным на понятии проверочной матрицы. Матрица названа проверочной потому, что она играет ту же роль в теории симплектических кодов, что и проверочная матрица в теории классических линейных кодов.

Пусть $S = \langle g_1, \dots, g_l \rangle$. Существует очень полезный способ представления образующих g_1, \dots, g_l с использованием *проверочной матрицы*. Это матрица $l \times 2n$, строки которой соответствуют образующим от g_1 до g_l . Левая половина матрицы содержит единицы в позициях, соответствующих операторам X в образующих. Правая половина матрицы содержит единицы в позициях, соответствующих операторам Z . Единица, находящаяся в одной позиции в левой и правой половинах матрицы, соответствует оператору Y в образующей. Более строго, i -я строка строится следующим образом. Если g_i содержит I в j -ом кубите, то в j -ом и $n + j$ -ом столбцах стоят нули; если g_i содержит X в j -ом кубите, то в j -ом столбце стоит 1, а в $n + j$ -ом — ноль; если g_i содержит Y в j -ом кубите, то в j -ом и $n + j$ -ом столбцах стоят единицы; наконец, если g_i содержит Z в j -ом кубите, то в j -ом столбце стоит ноль, а в $n + j$ -ом — единица. Для семикубитового кода Стина мы можем записать проверочную матрицу, используя рис. 10.6:

$$\left[\begin{array}{ccccccc|cccccccc} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array} \right]. \quad (10.83)$$

Проверочная матрица не содержит информации о множителях перед образующими, однако она включает много другой полезной информации, причем так, что мы введем специальное обозначение $r(g)$ для строки ($2n$ -мерного вектора), соответствующей элементу g группы Паули. Определим $2n \times 2n$ матрицу Λ следующим образом:

$$\Lambda = \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix}. \quad (10.84)$$

Здесь матрицы I имеют размер $n \times n$. Элементы g и g' группы Паули коммутируют тогда и только тогда, когда $r(g)\Lambda r(g')^T = 0$. Формула $x\Lambda y^T$ определяет некоторое «косое» скалярное произведение матричных строк x и y , которое показывает, коммутируют ли соответствующие им элементы группы Паули.

Упражнение 10.33. Покажите, что g и g' коммутируют тогда и только тогда, когда $r(g)\Lambda r(g')^T = 0$. (При использовании проверочных матриц арифметические операции производятся по модулю 2.)

Упражнение 10.34. Пусть $S = \langle g_1, \dots, g_l \rangle$. Покажите, что $-I$ не является элементом S тогда и только тогда, когда $g_j^2 = I$ для всех j , и $g_j \neq -I$ для всех j .

Упражнение 10.35. Пусть S — подгруппа G_n , не содержащая $-I$. Покажите, что $g^2 = I$ для всех $g \in S$ и, следовательно, $g^\dagger = g$.

Полезная взаимосвязь между независимостью образующих и проверочной матрицей устанавливается с помощью следующего утверждения:

Утверждение 10.3. Пусть $S = \langle g_1, \dots, g_l \rangle$ не содержит $-I$. Образующие g_1, \dots, g_l независимы тогда и только тогда, когда строки соответствующей проверочной матрицы линейно независимы.

Доказательство.

Приведем доказательство от противного. Заметим сначала, что g_i^2 равно I для всех i (упр. 10.35). Кроме того, $r(g) + r(g') = r(gg')$, т. е. сложение в строковом представлении соответствует умножению элементов группы. Поэтому строки проверочной матрицы линейно зависят ($\sum_i a_i r(g_i) = 0$ и $a_j \neq 0$ для некоторого j) тогда и только тогда, когда $\prod_i g_i^{a_i}$ равно тождественному оператору с точностью до некоторого множителя. Но $-I \notin S$, поэтому множитель должен быть равен 1, и последнее условие эквивалентно условию $g_j = g_j^{-1} = \prod_{i \neq j} g_i^{a_i}$. Следовательно, g_1, \dots, g_l не независимые образующие. ■

С помощью следующего утверждения легко доказать, что V_S имеет размерность 2^n , если S задается $l = n - k$ коммутирующими независимыми образующими и $-I \notin S$. Мы еще не раз используем это утверждение. Доказательство опять проводится с использованием проверочной матрицы.

Утверждение 10.4. Пусть группа $S = \langle g_1, \dots, g_l \rangle$ задана l независимыми образующими и $-I \notin S$. Допустим, что i — некоторое число из набора $1, \dots, l$. Существует $g \in G_n$, такое, что $gg_i g^\dagger = -g_i$ и $gg_j g^\dagger = g_j$ для любого $j \neq i$.

Доказательство.

Пусть G — проверочная матрица, соответствующая операторам g_1, \dots, g_l . В соответствии с утверждением (10.3) строки G линейно независимы, поэтому существует такой $2n$ -мерный вектор x , что $G\Lambda x = e_i$, где e_i — l -мерный вектор с единицей в i -й позиции и остальными нулями в остальных позициях. Выберем g так, что $r(g) = x^T$. Тогда по определению x мы имеем $r(g_j)\Lambda r(g)^T = 0$ для $j \neq i$ и $r(g_i)\Lambda r(g)^T = 1$. Следовательно, $gg_i g^\dagger = -g_i$ и $gg_j g^\dagger = g_j$ для $j \neq i$. ■

Мы завершим рассмотрение основных элементов формализма стабилизаторов доказательством того, что V_S нетривиально, если S задается независимыми коммутирующими образующими и $-I \notin S$. Действительно, для $l = n - k$ образующих, V_S должно быть 2^k -мерным (мы докажем это). Интуитивно понятно, что добавление одной образующей уменьшает размерность V_S в два раза из-за того, что собственные пространства тензорного произведения матриц Паули, соответствующие собственным значениям $+1$ и -1 , делят гильбертово пространство на два подпространства одинаковой размерности.

Утверждение 10.5. Пусть $S = \langle g_1, \dots, g_l \rangle$ порождается $n - k$ независимыми коммутирующими элементами G_n и $-I \notin S$. Тогда V_S — 2^k -мерное векторное пространство.

Во всех наших последующих рассуждениях в формализме стабилизаторов мы считаем, что стабилизаторы описываются независимыми коммутирующими образующими, такими, что $-I \notin S$.

Доказательство.

Пусть $x = (x_1, \dots, x_{n-k})$ — 2^{n-k} -мерный вектор с элементами из \mathbf{Z}_2 . Введем

$$P_S^x \equiv \frac{\prod_{j=1}^{n-k} (I + (-1)^{x_j} g_j)}{2^{n-k}}. \quad (10.85)$$

Так как оператор $(I + g_j)/2$ является проектором на собственное пространство g_j , соответствующее собственному числу $+1$, легко видеть, что $P_S^{(0,\dots,0)}$ — проектор на V_S . В соответствии с утверждением 10.4, для каждого x существует g_x из множества G_n , такое, что $g_x P_S^{(0,\dots,0)}(g_x)^\dagger = P_S^x$ и, следовательно, размерность P_S^x совпадает с размерностью V_S . Легко видеть, что P_S^x для различных x ортогональны. В завершение доказательства заметим, что

$$I = \sum_x P_S^x. \quad (10.86)$$

В левой части равенства стоит проектор на 2^n -мерное пространство, в правой части — сумма 2^{n-k} ортогональных проекторов, имеющих такую же размерность, что и V_S . Таким образом, размерность V_S равна 2^k . ■

10.5.2 Унитарные операторы и формализм стабилизаторов

Мы уже обсудили использование формализма стабилизаторов для описания векторных пространств. С помощью формализма стабилизаторов можно также описывать *динамику* этих пространств в пространстве состояний под действием различных квантовых преобразований. Это очень важно, так как мы сможем описать квантовые коды, исправляющие ошибки, в формализме стабилизаторов и получим удобный способ описания шума и других динамических процессов в этих кодах. Предположим, что мы действуем унитарным оператором U на векторное пространство V_S , которое стабилизируется группой S . Пусть $|\psi\rangle$ — произвольный элемент V_S . Тогда для любого оператора g из S

$$U|\psi\rangle = Ug|\psi\rangle = UgU^\dagger U|\psi\rangle, \quad (10.87)$$

т. е. состояние $U|\psi\rangle$ стабилизируется оператором UgU^\dagger . Следовательно, векторное пространство UV_S стабилизируется группой $USU^\dagger = \{UgU^\dagger | g \in S\}$. Если g_1, \dots, g_l — образующие группы S , то $Ug_1U^\dagger, \dots, Ug_lU^\dagger$ — образующие группы USU^\dagger , поэтому, чтобы понять, как меняется стабилизатор под действием унитарного оператора, достаточно определить, как меняются его образующие.

Большим преимуществом такого подхода является то, что для некоторых унитарных операторов U изменение образующих записывается особенно просто. Предположим, например, что мы применяем элемент Адамара к одному кубиту. Заметим, что

$$HXH^\dagger = Z, \quad HYH^\dagger = -Y, \quad HZH^\dagger = X, \quad (10.88)$$

отсюда следует, что применив элемент Адамара к состоянию, стабилизируемому оператором Z (состоянию $|0\rangle$), мы получим состояние, стабилизируемое оператором X ($|+\rangle$).

Этот пример может показаться не слишком впечатляющим, поэтому рассмотрим состояние n кубитов, стабилизируемое группой $\langle Z_1, Z_2, \dots, Z_n \rangle$. Нетрудно понять, что это состояние $|0\rangle^{\otimes n}$. Применим элемент Адамара к каждому кубиту. Стабилизатор при этом перейдет в $\langle X_1, X_2, \dots, X_n \rangle$; мы получим знакомое нам состояние, являющееся суперпозицией всех состояний вычислительного базиса с равными весами. Заметим, что в этом примере для записи получившегося состояния обычным способом (в виде вектора) нужно задать 2^n амплитуд. В формализме стабилизаторов нам потребовалось всего n образующих $\langle X_1, X_2, \dots, X_n \rangle$. Можно подумать, что такая компактная запись не является неожиданностью, поскольку в данном случае мы не получаем запутанных состояний. Однако в формализме стабилизаторов можно эффективно описать и элемент CNOT, который вместе с элементом Адамара способен создать запутанные состояния. Чтобы показать это, рассмотрим, как действует элемент CNOT на операторы X_1, X_2, Z_1 и Z_2 . Обозначив через U элемент CNOT с управляющим кубитом 1 и управляемым кубитом 2, запишем

$$\begin{aligned} UX_1U^\dagger &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \\ &= \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \\ &= X_1X_2. \end{aligned} \quad (10.89)$$

Аналогичным образом получим $UX_2U^\dagger = X_2$, $UZ_1U^\dagger = Z_1$ и $UZ_2U^\dagger = Z_1Z_2$. Чтобы показать, как действует U на другие элементы группы Паули, можно воспользоваться только что полученными равенствами. Например, чтобы найти $UX_1X_2U^\dagger$, запишем $UX_1X_2U^\dagger = UX_1U^\dagger UX_2U^\dagger = (X_1X_2)X_2 = X_1$. Для матриц Y действуем аналогично: $UY_2U^\dagger = iUX_2Z_2U^\dagger = iUX_2U^\dagger UZ_2U^\dagger = iX_2(Z_1Z_2) = Z_1Y_2$.

Упражнение 10.36. Прямым вычислением проверьте, что $UX_1U^\dagger = X_1X_2$, $UX_2U^\dagger = X_2$, $UZ_1U^\dagger = Z_1$ и $UZ_2U^\dagger = Z_1Z_2$. Эти и другие полезные соотношения для элемента Адамара, фазового элемента и элементов Паули приведены на рис. 10.7.

Операция	Вход	Выход
CNOT	X_1	$X_1 X_2$
	X_2	X_2
	Z_1	Z_1
	Z_2	$Z_1 Z_2$
H	X	Z
	Z	X
S	X	Y
	Z	Z
X	X	X
	Z	$-Z$
Y	X	$-X$
	Z	$-Z$
Z	X	$-X$
	Z	Z

Рис. 10.7. Изменение элементов группы Паули под действием различных операторов В элементе CNOT кубит 1 — управляющий, а кубит 2 — управляемый

Упражнение 10.37. Чему равно UY_1U^\dagger ?

В качестве примера использования формализма стабилизаторов для описания унитарных динамических процессов, рассмотрим схему обмена, приведенную в подразд. 1.3.4. Для удобства она изображена на рис. 10.8. Рассмотрим, как операторы Z_1 и Z_2 преобразуются под действием этой схемы. Оператор Z_1 преобразуется следующим образом: $Z_1 \rightarrow Z_1 \rightarrow Z_1 Z_2 \rightarrow Z_2$, а оператор Z_2 преобразуется как $Z_2 \rightarrow Z_1 Z_2 \rightarrow Z_1 \rightarrow Z_1$. Аналогично $X_1 \rightarrow X_2$ и $X_2 \rightarrow X_1$. Очевидно, что если U — оператор обмена, то должны выполняться соотношения: $UZ_1U^\dagger = Z_2$ и $UZ_2U^\dagger = Z_1$, аналогичные соотношения для X_1 и X_2 . Эти равенства верны для схемы, изображенной на рис. 10.8. Доказательство того, что эта схема реализует элемент U , предлагаем вам в качестве упражнения.

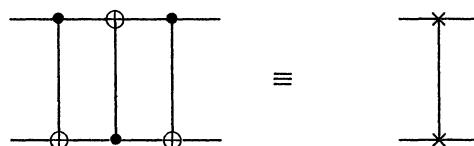


Рис. 10.8. Схема обмена для двух кубитов

Упражнение 10.38. Пусть U и V — унитарные операторы, действующие на два кубита и одинаково преобразующие X_1 , X_2 , Z_1 и Z_2 . Покажите, что $U = V$.

Пример схемы обмена интересен, однако он не демонстрирует очень полезное свойство формализма стабилизаторов — способность описывать определенный тип запутанных квантовых состояний. Мы уже показали, что с помощью формализма стабилизаторов можно описать элемент CNOT и элемент Адамара. Вместе эти два элемента могут создавать запутанные состояния (см. подразд. 1.3.6). Мы покажем, как в формализме стабилизаторов может быть описан широкий класс запутанных состояний, включая кодовые слова многих квантовых кодов.

Какие элементы, кроме элемента Адамара и CNOT, могут быть описаны в формализме стабилизаторов? Наиболее важным дополнением к этому набору является однокубитовый фазовый элемент, который определяется следующим образом:

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}. \quad (10.90)$$

Легко вычислить действие этого элемента на матрицы Паули:

$$SX S^\dagger = Y, \quad SZ S^\dagger = Z. \quad (10.91)$$

Упражнение 10.39. Проверьте (10.91).

Оказывается, что любой унитарный оператор, преобразующий элементы G_n в элементы G_n , может быть составлен из элементов Адамара, фазовых элементов и элементов CNOT. По определению, набор операторов U , такой, что $UG_n U^\dagger = G_n$, называется *нормализатором* G_n и обозначается как $N(G_n)$. Образующими нормализатора G_n являются элемент Адамара, элемент CNOT и фазовый элемент. Эти три элемента иногда называют элементами нормализатора. Доказательство этого факта простое, но полезное, оно предлагается в качестве упражнения 10.40.

Теорема 10.6. Пусть U — унитарный оператор, действующий на n кубитов, причем $UgU^\dagger \in G_n$ для любого $g \in G_n$. С точностью до общей фазы оператор U может быть составлен из $O(n^2)$ элементов Адамара, фазовых и элементов CNOT.

Упражнение 10.40. Докажите теорему 10.6 методом математической индукции в следующей последовательности:

- (1) Докажите, что из элемента Адамара и фазового элемента можно составить любой элемент нормализатора для одного кубита.
- (2) Пусть U — элемент $N(G_{n+1})$, действующий на $n + 1$ кубитов, такой, что $UZ_1U^\dagger = X_1 \otimes g$ и $UX_1U^\dagger = Z_1 \otimes g'$ для некоторых $g, g' \in G_n$. Определим элемент U' , действующий на n кубитов, следующим образом: $U'|\psi\rangle \equiv \sqrt{2}(0|U(|0\rangle \otimes |\psi\rangle))$. Используя предположение индукции, покажите, что элемент U может быть реализован с использованием $O(n^2)$ элементов Адамара, фазовых и элементов CNOT.

- (3) Покажите, что любой элемент $U \in N(G_n)$ может быть сконструирован с использованием $O(n^2)$ Адамара, фазовых и элементов CNOT.

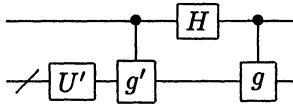


Рис. 10.9. Конструкция, используемая для доказательства того, что элементы Адамара, фазовые элементы и CNOT являются образующими нормализатора $N(G_n)$

Мы увидели, что много интересных квантовых элементов входит в нормализатор $N(G_n)$. Существуют ли элементы, не входящие в него? Оказывается, большинство квантовых элементов не входит в нормализатор. Особенно интересными являются два из них: $(\pi/8)$ -элемент и элемент Тоффоли. Пусть U — элемент Тоффоли с управляющими кубитами 1 и 2 и управляемым кубитом 3, а T — $(\pi/8)$ -элемент. Можно легко вычислить действие этих элементов на матрицы Паули:

$$TZT^\dagger = Z, \quad TXT^\dagger = \frac{X+Y}{\sqrt{2}}, \quad (10.92)$$

и

$$UZ_1U^\dagger = Z_1 \quad UX_1U^\dagger = X_1 \otimes \frac{I + Z_2 + X_3 - Z_2X_3}{2}, \quad (10.93)$$

$$UZ_2U^\dagger = Z_2 \quad UX_2U^\dagger = X_2 \otimes \frac{I + Z_1 + X_3 - Z_1X_3}{2}, \quad (10.94)$$

$$UX_3U^\dagger = X_3 \quad UZ_3U^\dagger = Z_3 \otimes \frac{I + Z_1 + Z_2 - Z_1Z_2}{2}. \quad (10.95)$$

К сожалению, рассмотрение в формализме стабилизаторов схем, содержащих $(\pi/8)$ - и Тоффоли элементы, менее удобно, чем рассмотрение схем, состоящих только из элементов Адамара, фазовых и элементов CNOT. Однако кодирование, декодирование, обнаружение и исправление ошибок для симплектических кодов может быть выполнено с использованием этих элементов, так что формализм стабилизаторов можно применять для изучения таких кодов.

Упражнение 10.41. Проверьте формулы (10.92-10.95).

10.5.3 Измерения в формализме стабилизаторов

Мы показали, как некоторый ограниченный класс унитарных элементов может быть удобно описан в формализме стабилизаторов. Измерения в вычислительном базисе также могут быть описаны в формализме стабилизаторов. Чтобы показать это, предположим, что мы производим измерение оператором $g \in G_n$

(оператор g эрмитов и, следовательно, может рассматриваться как наблюдаемая величина, см. подразд. 2.2.5). Без потери общности можно считать g произведением матриц Паули без множителя -1 или $\pm i$. Пусть система находится в состоянии $|\psi\rangle$, которое стабилизируется группой $\langle g_1, \dots, g_l \rangle$. Как этот стабилизатор меняется при измерении? Существует два возможных варианта.

- g коммутирует со всеми образующими стабилизатора.
- g антисимметрическое с одной или несколькими образующими. Пусть стабилизатор имеет образующие $\langle g_1, \dots, g_n \rangle$ и g антисимметрическое с g_1 . Без потери общности можно считать, что g коммутирует со всеми остальными образующими $\langle g_2, \dots, g_n \rangle$. Действительно, если g не коммутирует, например с g_2 , можно заменить g_2 на оператор $g_1 g_2$, с которым g коммутирует.

В первом случае g или $-g$ является элементом стабилизатора. Действительно, поскольку $g_j g |\psi\rangle = g g_j |\psi\rangle = g |\psi\rangle$ для любой образующей, состояние $g |\psi\rangle$ является элементом V_S и, следовательно, пропорционально $|\psi\rangle$. Так как $g^2 = I$, то $g |\psi\rangle = \pm |\psi\rangle$ и значит g или $-g$ является элементом стабилизатора. Предположим, что g является элементом стабилизатора. (Случай $-g$ рассматривается аналогично.) При этом $g |\psi\rangle = |\psi\rangle$ и измерение g дает $+1$ с вероятностью 1, не нарушая состояния системы и, следовательно, не изменяя стабилизатора.

Что же происходит во втором случае, когда g антисимметрическое с g_1 и коммутирует со всеми остальными образующими? Заметим, что g имеет собственные значения ± 1 и, следовательно, проекторы для результатов измерения ± 1 равны $(I \pm g)/2$ соответственно. Вероятности различных результатов измерений равны

$$p(+1) = \text{tr} \left(\frac{I + g}{2} |\psi\rangle\langle\psi| \right), \quad (10.96)$$

$$p(-1) = \text{tr} \left(\frac{I - g}{2} |\psi\rangle\langle\psi| \right). \quad (10.97)$$

Используя тот факт, что $g_1 |\psi\rangle = |\psi\rangle$ и $g g_1 = -g_1 g$, получаем

$$p(+1) = \text{tr} \left(\frac{I + g}{2} g_1 |\psi\rangle\langle\psi| \right) \quad (10.98)$$

$$= \text{tr} \left(g_1 \frac{I - g}{2} |\psi\rangle\langle\psi| \right). \quad (10.99)$$

Переставим циклически операторы под знаком следа так, чтобы g_1 оказался справа, и, применив равенство $g_1 = g_1^\dagger$, уничтожим его с помощью $|\psi\rangle$ (см. упр. 10.35). В результате получим

$$p(+1) = \text{tr} \left(\frac{I - g}{2} |\psi\rangle\langle\psi| \right) = p(-1). \quad (10.100)$$

Так как $p(+1) + p(-1) = 1$, получаем $p(+1) = p(-1) = 1/2$. Пусть результат измерения $+1$. В этом случае новое состояние системы $|\psi^+\rangle = (I + g)|\psi\rangle/\sqrt{2}$. Это состояние имеет стабилизатор $\langle g, g_2, \dots, g_n \rangle$. Точно так же, если результат измерения -1 , стабилизатор полученного состояния $\langle -g, g_2, \dots, g_n \rangle$.

10.5.4 Теорема Готтесмана–Нилла

Использование стабилизаторов для описания унитарных преобразований и измерений обобщается замечательной теоремой Готтесмана – Нилла.

Теорема 10.7 (теорема Готтесмана–Нилла). Пусть квантовое вычисление выполняется с использованием приготовления состояний в вычислительном базисе, элементов Адамара, Паули, фазовых и элементов CNOT, измерений наблюдаемых из группы Паули (которые как частный случай включают измерения в вычислительном базисе), классического управления в зависимости от результатов измерений. Такое квантовое вычисление может быть эффективно продемонстрировано на классическом компьютере.

Мы уже неявно доказали теорему Готтесмана – Нилла. На классическом компьютере можно моделировать квантовые вычисления, оперируя с образующими стабилизатора. Например, чтобы промоделировать элемент Адамара, нужно соответствующим образом изменить n образующих, описывающих квантовое состояние. Аналогичным образом можно промоделировать приготовление состояний, фазовый элемент и элементы CNOT, элементы Паули и измерения наблюдаемых величин из группы Паули с использованием $O(n^2)$ операций на классическом компьютере; следовательно, квантовое вычисление из t операций может быть промоделировано $O(n^2m)$ операциями на классическом компьютере.

Теорема Готтесмана – Нилла показывает, насколько тонким вопросом является эффективность квантового компьютера. Некоторые квантовые вычисления даже с сильно запутанными состояниями могут быть эффективно моделированы на классическом компьютере. Конечно, не все типы квантовых вычислений (и не все типы запутанных состояний) могут быть эффективно описаны в формализме стабилизаторов. Такие интересные задачи обработки квантовой информации, как квантовая телепортация (подразд. 1.3.7) и сверхплотное кодирование (подразд. 2.3) выполняются только с использованием элементов Адамара, CNOT и измерений в вычислительном базисе. Согласно теореме Готтесмана – Нилла, они могут эффективно моделироваться на классическом компьютере. Мы увидим, что большое количество квантовых кодов, исправляющих ошибки, может быть описано в формализме стабилизаторов.

Упражнение 10.42. Используйте формализм стабилизаторов, чтобы проверить, что схема, изображенная на рис. 1.13, производит телепортацию кубитов. Обратите внимание, что формализм стабилизаторов ограничивает класс состояний, которые можно телепортировать, так что в некотором смысле он не обеспечивает полного описания квантовой телепортации. Тем не менее, такой подход позволяет понять механизм телепортации.

10.5.5 Построение симплектических кодов

Формализм стабилизаторов идеально подходит для описания квантовых кодов. В данном разделе мы проиллюстрируем это на нескольких важных кодах, таких как девятикубитовый код Шора, CSS коды, и пятикубитовый квантовый код, самый маленький код, исправляющий произвольные ошибки в одном кубите. Основная идея очень проста: симплектическим $[n, k]$ -кодом называется векторное пространство V_S , стабилизируемое подгруппой S группы G_n , такой, что $-I \notin S$ и S имеет $n - k$ независимых коммутирующих образующих, $\langle g_1, \dots, g_{n-k} \rangle$. Обозначим такой код как $C(S)$.

Какие состояния образуют базис для кода $C(S)$? Так как стабилизатор S имеет $n - k$ образующих, можно выбрать любой набор из 2^k ортонормированных векторов в коде $C(S)$ в качестве оригинала базисных состояний. На практике, однако, удобнее выбрать некоторый определенный набор состояний следующим образом. Сначала выберем операторы $\bar{Z}_1, \dots, \bar{Z}_k \in G_n$, такие, что $g_1, \dots, g_{n-k}, \bar{Z}_1, \dots, \bar{Z}_k$ независимы и коммутируют (мы объясним, как это может быть сделано несколько позже). Оператор \bar{Z}_j играет роль логического оператора Паули σ_z для логического кубита с номером j , так что логическое состояние вычислительного базиса $|x_1, \dots, x_k\rangle_L$ определяется как состояние, стабилизируемое оператором

$$\langle g_1, \dots, g_{n-k}, (-1)^{x_1} \bar{Z}_1, \dots, (-1)^{x_k} \bar{Z}_k \rangle. \quad (10.101)$$

Мы определяем \bar{X}_j как такое произведение матриц Паули, которое меняет \bar{Z}_j на $-\bar{Z}_j$ ($\bar{X}_j \bar{Z}_j \bar{X}_j^\dagger = -\bar{Z}_j$) и оставляет неизменными остальные \bar{Z}_i и g_i . Очевидно, что \bar{X}_j действует как квантовый элемент NOT на j -й закодированный кубит. Оператор \bar{X}_j удовлетворяет равенству $\bar{X}_j g_k \bar{X}_j^\dagger = g_k$ для любого k и, следовательно, коммутирует со всеми образующими стабилизатора. Также легко проверить, что \bar{X}_j коммутирует со всеми \bar{Z}_i для $i \neq j$ и антикоммутирует с \bar{Z}_j .

Как связаны свойства исправления ошибок симплектического кода с образующими его стабилизатора? Допустим, что мы кодируем квантовое состояние, используя симплектический $[n, k]$ -код $C(S)$ со стабилизатором $S = \langle g_1, \dots, g_{n-k} \rangle$. Пусть в закодированном состоянии возникает ошибка E . Рассмотрение того, какие типы ошибок могут быть обнаружены и исправлены с использованием кода $C(S)$, мы проведем в три приема. Сначала мы рассмотрим, как действуют в пространстве кода различные типы ошибок, и, не приводя никаких доказательств, сформулируем интуитивные соображения, какие типы ошибок могут быть обнаружены и исправлены. Затем сформулируем и докажем общую теорему, основанную на условиях исправления ошибок и дающую ответ на вопрос, какие типы ошибок могут быть обнаружены и исправлены с помощью симплектических кодов. Наконец, мы опишем практический метод обнаружения и исправления ошибок с использованием понятия синдрома ошибки.

Пусть $C(S)$ — симплектический код, в котором возникает ошибка $E \in G_n$. Как изменится пространство кода, если E антикоммутирует с некоторым эле-

ментом стабилизатора? В этом случае E переведет $C(S)$ в ортогональное подпространство и ошибка в принципе может быть обнаружена (и, возможно, после обнаружения исправлена) с помощью подходящего проективного измерения. Если $E \in S$, не нужно ничего делать, потому что «ошибка» E не меняет квантовое состояние. Неприятность возникает, когда E коммутирует со всеми элементами группы S (т. е. $Eg = gE$ для всех $g \in S$), но не является его элементом. Множество $E \in G_n$, такое, что $Eg = gE$ для всех $g \in S$, называется *централизатором* S в G_n и обозначается как $Z(S)$. В нашем случае для стабилизирующей группы S централизатор совпадает с более знакомой группой, нормализатором S , который обозначается через $N(S)$ и определяется как группа, содержащая все элементы $E \in G_n$, такие, что $EgE^\dagger \in S$ для всех $g \in S$.

Упражнение 10.43. Покажите, что $S \subseteq N(S)$ для любой подгруппы S группы G_n .

Упражнение 10.44. Покажите, что $N(S) = Z(S)$ для любой подгруппы S группы G_n , не содержащей $-I$. Эти рассуждения о различных типах ошибок E приводят нас к следующей теореме, которая является квантовым условием исправления ошибок (теорема 10.1), сформулированным в терминах симплектических кодов.

Теорема 10.8 (условие исправления ошибок для симплектических кодов). Пусть S — стабилизатор симплектического кода $C(S)$, а $\{E_j\}$ — набор операторов из G_n , такой, что $E_j^\dagger E_k \notin N(S) \setminus S$ для всех j и k . В этом случае $\{E_j\}$ является исправляемым набором ошибок для кода $C(S)$.

Без потери общности можно ограничиться рассмотрением только таких ошибок E_j , для которых $E_j^\dagger = E_j$. В этом случае условие исправления ошибок упростится до $E_j E_k \notin N(S) \setminus S$ для всех j и k .

Доказательство.

Пусть P — проектор на пространство кода $C(S)$. Для фиксированных j и k существует две возможности: $E_j^\dagger E_k \in S$ или $E_j^\dagger E_k \in G_n \setminus N(S)$. В первом случае $PE_j^\dagger E_k P = P$, так как P не меняется при умножении на любой элемент S . Во втором случае ($E_j^\dagger E_k \in G_n \setminus N(S)$) оператор $E_j^\dagger E_k$ должен антисимметризировать с некоторым элементом g_1 группы S . Пусть g_1, \dots, g_l — образующие S , тогда

$$P = \frac{\prod_{l=1}^{n-k} (I + g_l)}{2^{n-k}}. \quad (10.102)$$

Используя антисимметричность, получим

$$E_j^\dagger E_k P = (I - g_1) E_j^\dagger E_k \frac{\prod_{l=2}^{n-k} (I + g_l)}{2^{n-k}}. \quad (10.103)$$

Но $P(I - g_1) = 0$, так как $(I + g_1)(I - g_1) = 0$. Следовательно, $PE_j^\dagger E_k P = 0$ для $E_j^\dagger E_k \in G_n \setminus N(S)$. Отсюда следует, что ошибки $\{E_j\}$ удовлетворяют квантовому условию исправления ошибок и, таким образом могут быть исправлены.

Формулировка и доказательство теоремы 10.8 являются замечательным теоретическим результатом, однако они не указывают, как производить исправление ошибок, если оно возможно! Чтобы понять, как это делать, предположим, что g_1, \dots, g_{n-k} — образующие стабилизатора симплектического $[n, k]$ -кода, а $\{E_j\}$ — множество исправляемых ошибок для этого кода. Обнаружение ошибки выполняется последовательным измерением образующих g_1, \dots, g_{n-k} , что дает синдром ошибки, состоящий из результатов измерений $\beta_1, \dots, \beta_{n-k}$. Если произошла ошибка E_j , синдром состоит из таких β_i , что $E_j g_i E_j^\dagger = \beta_i g_i$. Если E_j — единственная ошибка, имеющая такой синдром, то исправление выполняется оператором E_j^\dagger . В случае двух различных ошибок E_j и $E_{j'}$ с одинаковым синдромом $E_j P E_j^\dagger = E_{j'} P E_{j'}^\dagger$, где P — проектор на пространство кодов. Следовательно $E_j^\dagger E_{j'} P E_{j'}^\dagger E_j = P$ и, значит $E_j^\dagger E_{j'} \in S$. Таким образом, исправление ошибки E_j можно выполнить, применив оператор E_j^\dagger . Итак, для каждого возможного синдрома ошибки следует найти какую-нибудь E_j , дающую такой синдром, и использовать для ее исправления оператор E_j^\dagger .

Теорема 10.8 обосновывает определение понятия кодового расстояния для квантового кода, аналогичного для классического кода. Весом оператора $E \in G_n$ мы назовем число членов в тензорном произведении, не равных тождественному оператору. Например, вес оператора $X_1 Z_4 Y_8$ равен трем. Кодовым расстоянием симплектического кода $C(S)$ называется минимальный вес элементов $N(S) \setminus S$. Если $C(S) — [n, k]$ -код с расстоянием d , мы называем его симплектическим $[n, k, d]$ -кодом. Согласно теореме 10.8 код с расстоянием не менее $2t + 1$ способен исправлять ошибки в любых t кубитах, как и в классическом случае.

Упражнение 10.45 (исправление локализованных ошибок). Пусть $C(S)$ — симплектический $[n, k, d]$ -код. Допустим, что k кубитов кодируются n кубитами с помощью этого кода и затем подвергаются действию шума. Однако, к счастью, нам известно, что шуму подверглись только $d - 1$ кубитов, и более того, нам точно известно, какие именно $d - 1$ кубитов подверглись шуму. Покажите, что такие локализованные ошибки можно исправить.

10.5.6 Примеры

Сейчас мы приведем несколько простых примеров симплектических кодов, в том числе уже знакомые нам коды, такие как девятикубитовый код Шора и CSS коды. Мы рассмотрим эти коды с новой точки зрения — в формализме стабилизаторов. В каждом случае свойства кода легко определить, применив теорему 10.8 к образующим его стабилизаторам. Эти примеры помогут нам в построении схем для кодирования и декодирования.

Трехкубитовый код, исправляющий классические ошибки

Рассмотрим знакомый нам трехкубитовый код, исправляющий классические ошибки, который является линейной оболочкой состояний $|000\rangle$ и $|111\rangle$. Его стабилизатор имеет образующие $Z_1 Z_2$ и $Z_2 Z_3$. Путем перебора найдем, что любое

произведение двух элементов $(I, X_1, X_2, X_3, X_1X_2, X_1X_3, X_2X_3)$ из множества $\{I, X_1, X_2, X_3\}$ антисимметрическо, по крайней мере, с одной из образующих стабилизатора (кроме оператора I , который входит в S). Следовательно, согласно теореме 10.8, $\{I, X_1, X_2, X_3\}$ является множеством исправляемых ошибок для классического трехкубитового кода со стабилизатором $\langle Z_1Z_2, Z_2Z_3 \rangle$.

Обнаружение ошибки для этого кода производится с помощью измерений образующих стабилизатора Z_1Z_2 и Z_2Z_3 . Если, например, происходит ошибка X_1 , то стабилизатор преобразуется в $\langle -Z_1Z_2, Z_2Z_3 \rangle$ и измерения дают -1 и $+1$; в случае ошибки X_2 будут получены -1 и -1 ; в случае ошибки X_3 измерения дают $+1$ и -1 ; в случае тривиальной ошибки I будут получены $+1$ и $+1$. В каждом случае исправление производится очевидным образом с помощью обратного оператора ошибки, найденной с помощью измерений синдрома. Операции исправления ошибок для трехкубитового кода, исправляющего классические ошибки, представлены на рис. 10.10.

Z_1Z_2	Z_2Z_3	Тип ошибки	Действие
$+1$	$+1$	Нет ошибки	Нет
$+1$	-1	Ошибка в бите 3	Перевернуть бит 3
-1	$+1$	Ошибка в бите 1	Перевернуть бит 1
-1	-1	Ошибка в бите 2	Перевернуть бит 2

Рис. 10.10. Исправление ошибок на языке формализма стабилизаторов для трехкубитового кода, исправляющего классические ошибки.

Конечно, только что изложенная процедура повторяет то, что мы уже описали раньше для случая трехкубитового кода, исправляющего классические ошибки! Использование теории групп было бы ненужным, если бы мы хотели ограничиться таким простым примером. Реальная польза формализма стабилизаторов будет видна на более сложных примерах.

Упражнение 10.46. Покажите, что стабилизатор для трехкубитового кода, исправляющего фазовые ошибки, задается образующими X_1X_2 и X_2X_3 .

Девятикубитовый код Шора

Стабилизатор девятикубитового кода Шора имеет восемь образующих, показанных на рис. 10.11. Легко проверить условие теоремы 10.8 для множества ошибок, содержащего I и все однокубитовые ошибки. Рассмотрим, например, однокубитовые ошибки X_1 и Y_4 . Произведение X_1Y_4 антисимметрическо с Z_1Z_2 и, следовательно, не входит в $N(S)$. Аналогично все остальные произведения двух ошибок из этого множества либо входят в S , либо антисимметрическо, по крайней мере, с одним элементом S и, значит, не входят в $N(S)$. Следовательно, код Шора может исправлять произвольную однокубитовую ошибку.

Упражнение 10.47. Проверьте, что образующие на рис. 10.11 задают два кодовых слова из формулы (10.13).

Упражнение 10.48. Покажите, что операторы $\bar{Z} = X_1X_2X_3X_4X_5X_6X_7X_8X_9$ и $\bar{X} = Z_1Z_2Z_3Z_4Z_5Z_6Z_7Z_8Z_9$ являются логическими операторами Z и X для кубита, закодированного кодом Шора, т. е. что оператор \bar{Z} независим и коммутирует с образующими кода Шора, а оператор \bar{X} независим и коммутирует с образующими кода Шора и антисимметрическим относительно \bar{Z} .

Образующая	Оператор
g_1	$ZZIIIIIII$
g_2	$IIZZIIIII$
g_3	$IIZZZIIII$
g_4	$IIIIZZIII$
g_5	$IIIIIZZI$
g_6	$IIIIIIIIZZ$
g_7	$XXXXXXIII$
g_8	$XIIIIXXXX$
\bar{Z}	$XXXXXXXX$
\bar{X}	$ZZZZZZZZ$

Рис. 10.11. Восемь образующих для девятикубитового кода Шора и логические операторы Z и X . (В последних двух строчках, как это ни странно, ошибки нет!)

Пятикубитовый код

Каков минимальный размер квантового кода, способного закодировать один кубит так, чтобы можно было исправить произвольную ошибку в любом кубите закодированного состояния? Ответ на этот вопрос: пять кубитов (см. подразд. 12.4.3). Стабилизатор пятикубитового кода задается образующими, показанными на рис. 10.12. Так как пятикубитовый код является минимальным возможным кодом, способным защитить закодированное состояние от произвольной ошибки в одном кубите, может показаться, что это наиболее полезный код. Однако, во многих случаях удобнее использовать семикубитовый код Стина.

Образующая	Оператор
g_1	$XZZXI$
g_2	$IXZZX$
g_3	$XIXZZ$
g_4	$ZXIXZ$
\bar{Z}	$ZZZZZ$
\bar{X}	$XXXXX$

Рис. 10.12. Четыре образующих для пятикубитового кода и логические операторы X и Z . Обратите внимание, что последние три образующие могут быть получены из первой сдвигом вправо.

Упражнение 10.49. Используя теорему 10.8, проверьте, что пятикубитовый код защищает закодированное состояние от произвольной ошибки в одном кубите.

Кодовые слова для пятикубитового кода:

$$\begin{aligned} |0_L\rangle = \frac{1}{4} & \left[|00000\rangle + |10010\rangle + |01001\rangle + |10100\rangle \right. \\ & + |01010\rangle - |11011\rangle - |00110\rangle - |11000\rangle \\ & - |11101\rangle - |00011\rangle - |11110\rangle - |01111\rangle \\ & \left. - |10001\rangle - |01100\rangle - |10111\rangle + |00101\rangle \right] \end{aligned} \quad (10.104)$$

$$\begin{aligned} |1_L\rangle = \frac{1}{4} & \left[|11111\rangle + |01101\rangle + |10110\rangle + |01011\rangle \right. \\ & + |10101\rangle - |00100\rangle - |11001\rangle - |00111\rangle \\ & - |00010\rangle - |11100\rangle - |00001\rangle - |10000\rangle \\ & \left. - |01110\rangle - |10011\rangle - |01000\rangle + |11010\rangle \right] \end{aligned} \quad (10.105)$$

Упражнение 10.50. Покажите, что пятикубитовый код превращает квантовую границу Хэмминга [неравенство (10.51)] в равенство.

CSS коды и семикубитовый код

CSS коды являются отличным примером симплектических кодов, демонстрирующим, насколько формализм стабилизаторов упрощает построение квантовых кодов. Пусть C_1 и C_2 — классические линейные $[n, k_1]$ - и $[n, k_2]$ -коды такие, что $C_2 \subset C_1$, а коды C_1 и C_2^\perp могут исправлять t ошибок. Определим проверочную матрицу следующим образом:

$$\left[\begin{array}{c|c} H(C_2^\perp) & 0 \\ 0 & H(C_1) \end{array} \right]. \quad (10.106)$$

Чтобы показать, что эта матрица определяет симплектический код, нужно проверить, что она удовлетворяет условию коммутативности $H(C_2^\perp)H(C_1)^T = 0$. Так как $C_2 \subset C_1$, мы имеем $H(C_2^\perp)H(C_1)^T = [H(C_1)G(C_2)]^T = 0$. Легко доказать, что этот код совпадает с $\text{CSS}(C_1, C_2)$ и может исправлять ошибки в t кубитах.

Семикубитовый код Стина является примером CSS кода. Мы уже встречались с его проверочной матрицей (см. формулу (10.83)). Закодированные операторы Z и X для кода Стина определяются как

$$\bar{Z} \equiv Z_1 Z_2 Z_3 Z_4 Z_5 Z_6 Z_7, \quad \bar{X} \equiv X_1 X_2 X_3 X_4 X_5 X_6 X_7. \quad (10.107)$$

Упражнение 10.51. Докажите, что проверочная матрица, заданная выражением (10.106), соответствует стабилизатору кода $\text{CSS}(C_1, C_2)$ и, используя теорему 10.8, покажите, что этот код может исправлять произвольные ошибки в t кубитах.

Упражнение 10.52. Прямым вычислением закодированных состояний проверьте, что операторы (10.107) являются логическими операторами X и Z .

10.5.7 Стандартная форма симплектического кода

Вид логических операторов Z и X для симплектического кода станет существенно проще, если привести код к *стандартной форме*. Чтобы понять, что такое стандартная форма, рассмотрим проверочную матрицу для симплектического $[n, k]$ -кода C :

$$G = [G_1 | G_2]. \quad (10.108)$$

Матрица имеет $n - k$ строк. Перестановка строк матрицы соответствует переобозначению образующих, перестановка соответствующих столбцов в левой и правой частях — переобозначению кубитов, сложение строк — умножению образующих. Легко видеть, что можно заменить образующую g_i на $g_i g_j$, если $i \neq j$. Следовательно, существует эквивалентный код с проверочной матрицей, полученной из G приведением матрицы G_1 к стандартному гауссову виду, возможно с перестановкой кубитов:

$$\begin{matrix} r \\ n-k-r \\ n-k-r-s \end{matrix} \left[\begin{array}{ccc|ccc} \overset{r}{I} & \overset{n-r}{A} & & \overset{r}{B} & \overset{n-r}{C} & & \\ 0 & 0 & & D & E & & \end{array} \right], \quad (10.109)$$

где r — ранг матрицы G_1 . Затем, переставляя кубиты, приведем матрицу E к стандартному гауссову виду:

$$\begin{matrix} r \\ n-k-r-s \\ s \end{matrix} \left[\begin{array}{ccc|ccc} \overset{r}{I} & \overset{n-k-r-s}{A_1} & \overset{k+s}{A_2} & \overset{r}{B} & \overset{n-k-r-s}{C_1} & \overset{k+s}{C_2} & \\ 0 & 0 & 0 & D_1 & I & E_2 & \\ 0 & 0 & 0 & D_2 & 0 & 0 & \end{array} \right]. \quad (10.110)$$

Последние s образующих могут коммутировать с первыми r образующими, если только $D_2 = 0$. Поэтому можно положить $s = 0$. Если также сделать $C_1 = 0$, взяв подходящие линейные комбинации столбцов, то проверочная матрица при этом примет вид

$$\begin{matrix} r \\ n-k-r \end{matrix} \left[\begin{array}{ccc|ccc} \overset{r}{I} & \overset{n-k-r}{A_1} & \overset{k}{A_2} & \overset{r}{B} & \overset{n-k-r}{0} & \overset{k}{C} & \\ 0 & 0 & 0 & D & I & E & \end{array} \right], \quad (10.111)$$

где мы переобозначили E_2 на E и D_1 на D . Легко видеть, что такая процедура не единственна, однако мы говорим, что код с проверочной матрицей (10.111) находится в стандартной форме.

Если код находится в стандартной форме, для него легко определить закодированные операторы Z . Для этого нужно найти k операторов, независимых друг от друга и от образующих стабилизатора, а также коммутирующих друг с другом и с образующими стабилизатора. Запишем проверочную матрицу для этих k закодированных операторов Z в виде $G_z = [F_1 F_2 F_3 | F_4 F_5 F_6]$, где все матрицы F_1, \dots, F_6 имеют k строк и $r, n - k - r, k, r, n - k - r$ и k столбцов соответственно. Выберем эти матрицы так, что $G_z = [000|A_2^T 0I]$. Коммутативность таких закодированных операторов Z с элементами стабилизатора следует из уравнения $I \times (A_2^T)^T + A_2 = 0$. Эти операторы также коммутативны друг с другом, поскольку состоят только из произведений операторов Z . Независимость закодированных операторов Z от первых r образующих следует из того, что в их определении нет членов X , а независимость от следующих $n - k - r$ образующих обусловлена наличием $(n - k - r) \times (n - k - r)$ единичной матрицы в проверочной матрице для образующих и отсутствием соответствующих членов в проверочной матрице для закодированных операторов Z . Похожим образом мы можем построить закодированные операторы X с $k \times 2n$ проверочной матрицей $[0E^T I | C^T 00]$.

Упражнение 10.53. Докажите, что закодированные операторы Z независимы друг от друга.

Упражнение 10.54. Докажите, что закодированные операторы X , заданные введенной выше проверочной матрицей, независимы друг от друга и от образующих, коммутируют друг с другом и с образующими, а также X_j коммутирует с Z_k для всех $j \neq k$ и антакоммутирует с Z_j .

В качестве примера приведем к стандартной форме проверочную матрицу кода Стина (10.83). Для этого кода $n = 7$, $k = 1$. Изучение проверочной матрицы показывает, что для ее левой части σ_x ранг $r = 3$. Матрица может быть приведена к стандартной форме перестановкой кубитов 1 и 4, 3 и 4, 6 и 7 и прибавлением строки 6 к строке 4, строки 6 к строке 5, строк 4 и 5 к строке 6. Полученная матрица имеет стандартную форму

$$\left[\begin{array}{ccccccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array} \middle| \begin{array}{ccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 \end{array} \right]. \quad (10.112)$$

Матрица $A_2 = (1, 1, 0)$, следовательно, закодированный оператор Z имеет проверочную матрицу $[0000000|1100001]$, т. е. $\bar{Z} = Z_1 Z_2 Z_7$. Вспомнив, что кубиты 1 и 4, 3 и 4, 6 и 7 были переставлены, для исходного кода получим $\bar{Z} = Z_2 Z_4 Z_6$. Может показаться странным, что этот оператор не соответствует формуле (10.107), где $\bar{Z} = Z_1 Z_2 Z_3 Z_4 Z_5 Z_6 Z_7$. Однако, дело в том, что эти

два оператора отличаются множителем $Z_1 Z_3 Z_5 Z_7$, который является элементом стабилизатора кода Стина. Следовательно, оба эти оператора одинаково действуют на закодированные состояния.

Упражнение 10.55. Найдите оператор \bar{X} для стандартной формы кода Стина.

Упражнение 10.56. Покажите, что умножение закодированного оператора X или Z на некоторый элемент стабилизатора g слева не меняет его действие на код.

Упражнение 10.57. Запишите проверочные матрицы для пятикубитового и девятикубитового кодов в стандартной форме.

10.5.8 Квантовые схемы для кодирования, декодирования и исправления ошибок

Структура симплектических кодов позволяет систематически строить схемы кодирования, декодирования и исправления ошибок. Мы сначала опишем общий метод, а затем построим в качестве примеров несколько конкретных цепей. Начнем с общего случая симплектического $[n, k]$ -кода с образующими g_1, \dots, g_{n-k} и логическими операторами $\bar{Z}_1, \dots, \bar{Z}_k$.

Приготовление закодированного состояния $|0\rangle^{\otimes k}$, обычного начального состояния для квантовых вычислений, является простой процедурой. Мы начинаем с легко приготавливаемого состояния $|0\rangle^{\otimes k}$ и последовательно измеряем наблюдаемые $g_1, \dots, g_{n-k}, \bar{Z}_1, \dots, \bar{Z}_k$. Полученное состояние имеет стабилизатор $\langle \pm g_1, \dots, \pm g_{n-k}, \pm \bar{Z}_1, \dots, \pm \bar{Z}_k \rangle$, где различные знаки зависят от результатов измерений и, следовательно, известны. Эти знаки могут быть изменены на $+$, путем применения соответствующих произведений операторов Паули, как описано в доказательстве утверждения 10.4. В результате получим состояние со стабилизатором $\langle g_1, \dots, g_{n-k}, \bar{Z}_1, \dots, \bar{Z}_k \rangle$, т. е. закодированное состояние $|0\rangle^{\otimes k}$. Это состояние можно превратить в произвольное состояние вычислительного базиса $|x_1, \dots, x_k\rangle$, применив к нему соответствующие операторы из набора $\bar{X}_1, \dots, \bar{X}_k$. Недостаток такого кодирования в том, что оно не унитарно. Для унитарного кодирования может быть использован другой подход, основанный на стандартной форме проверочной матрицы. Этот подход описан в задаче 10.3. Если мы хотим закодировать *неизвестное* состояние, это можно сделать с помощью закодированного $|0\rangle^{\otimes k}$ состояния, как описано в задаче 10.4. Пока нам будет достаточно умения приготовить закодированное $|0\rangle^{\otimes k}$ состояние.

Декодирование также является достаточно простой процедурой, однако для многих целей полное декодирование не обязательно. Оказывается, что методы устойчивых к ошибкам квантовых вычислений позволяют выполнять логические операции над закодированными данными. Выходные данные такого вычисления могут быть непосредственно определены измерением логических операторов Z без необходимости декодирования и измерения в вычислительном базисе. Таким образом, унитарное квантовое декодирование, сохраняющее квантовую информацию, не очень важно для наших целей. Если такое декодирование все же необходимо, например при использовании кодов, исправляющих

ошибки для передачи информации по каналу с шумом, оно может быть выполнено с помощью унитарной кодирующей схемы из задачи 10.3, работающей в обратную сторону.

Процедура исправления ошибок для симплектического кода уже была описана в подразд. 10.5.5. Она очень похожа на процедуру кодирования: необходимо последовательно измерить образующие g_1, \dots, g_{n-k} и получить синдромы ошибок $\beta_1, \dots, \beta_{n-k}$. Далее с помощью классических вычислений можно определить необходимые для исправления ошибок операторы E_j^\dagger .

Ключом к построению схем для только что описанных процедур кодирования, декодирования и исправления ошибок, является умение измерять операторы. Напомним, что такие измерения являются обобщением проективных измерений, которые мы широко используем. При таких измерениях состояние проектируется на собственное состояние оператора, что дает в результате проекцию состояния и собственное значение. Это может напомнить вам алгоритм оценки собственного значения, описанный в гл. 5. Напомним из этой главы и упражнения 4.34, что схема, показанная на рис. 10.13, может быть использована для измерения однокубитового оператора M (с собственными значениями ± 1), с помощью управляемого элемента M . Варианты этой схемы для измерения операторов X и Z приведены на рис. 10.14 и рис. 10.15.

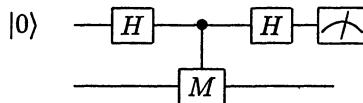


Рис. 10.13. Квантовая схема для измерения однокубитового оператора M с собственными значениями ± 1 . Измеряется нижний кубит, верхний кубит является вспомогательным

Конечно, то, что M — однокубитовый оператор, не является обязательным условием. На схеме рис. 10.13 можно заменить второй кубит на набор кубитов, а M — на произвольный эрмитов оператор с собственными значениями ± 1 . Такими операторами, например, являются произведения операторов Паули, которые нужно измерять при кодировании, декодировании и исправлении ошибок при использовании симплектических кодов.

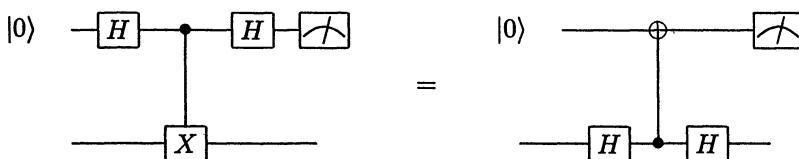


Рис. 10.14. Квантовые схемы для измерения оператора X . Слева — обычная конструкция, как на рис. 10.13, справа — эквивалентная схема

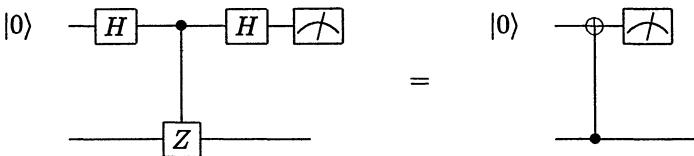


Рис. 10.15. Квантовые схемы для измерения оператора Z . Слева — обычная конструкция, как на рис. 10.13, справа — упрощенная схема.

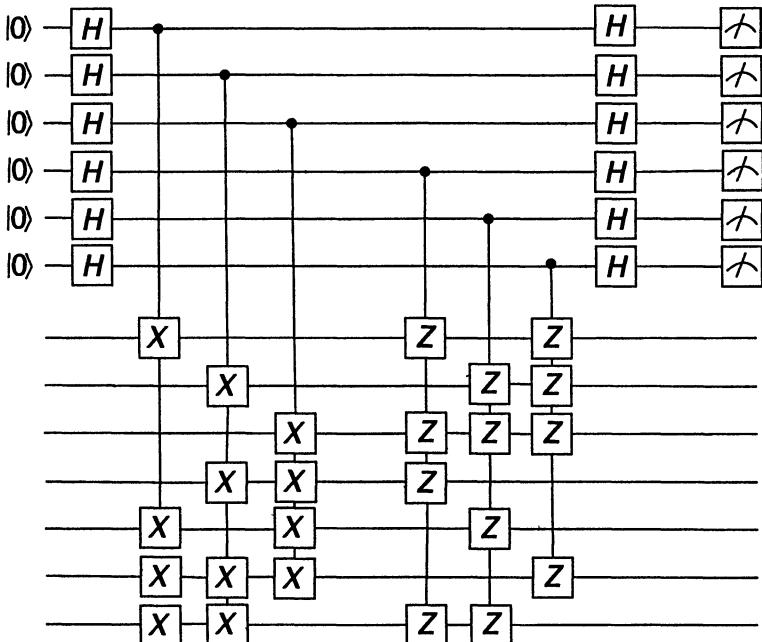


Рис. 10.16. Квантовые схемы для измерения образующих кода Стина, которые определяют синдром ошибок. Верхние шесть вспомогательных кубитов используются для измерения, а нижние семь — кубиты кода

В качестве конкретного примера рассмотрим измерение синдрома и процедуру кодирования для семикубитового кода Стина. Удобно начать со стандартной формы проверочной матрицы (10.112), так как из нее можно просто найти образующие, которые необходимо измерять. Вспомнив, что единицы в левой части матрицы соответствуют операторам X , а в правой — операторам Z , сразу получим схему, изображенную на рис. 10.16. Обратите внимание на соответствие в расположении нулей и единиц в проверочной матрице и, управляемых элементов Z и X на схеме. С помощью этой схемы можно исправлять ошибки, если после измерений применить к кубитам произведение операторов Паули, соответствующее результатам измерений. Кроме того эту схему можно использовать для приготовления закодированного логического состояния $|0\rangle$,

если дополнить ее измерением оператора \bar{Z} и исправлять знаки образующих стабилизатора, как было описано выше.

Упражнение 10.58. Проверьте, что схемы на рис. 10.13–10.15 работают правильно и докажите эквивалентность соответствующих схем.

Упражнение 10.59. Покажите, что используя эквивалентность схем на рис. 10.14 и 10.15, можно заменить схему измерения синдрома, изображенную на рис. 10.16, схемой, представленной на рис. 10.17.

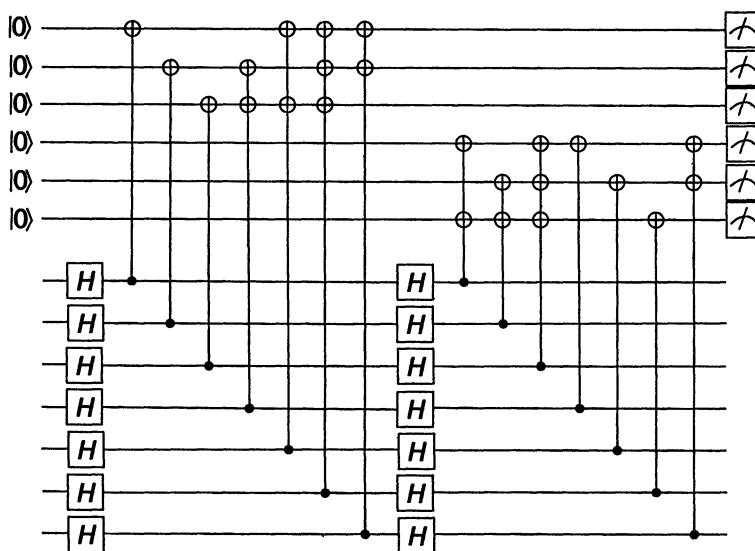


Рис. 10.17. Квантовая схема, эквивалентная схеме на рис. 10.16

Упражнение 10.60. Постройте схему измерения синдрома, аналогичную изображенной на рис. 10.16, но для девятикубитового и пятикубитового кода.

Упражнение 10.61. Найдите в явном виде операторы E_j^\dagger , соответствующие различным результатам измерения синдрома, с помощью схемы, изображенной на рис. 10.16.

10.6 Квантовые вычисления, устойчивые к ошибкам

Одним из основных применений исправления квантовых ошибок является защита квантовой информации не только при хранении и передаче, но и при выполнении вычислений над ней. Оказывается, что надежное квантовое вычисление возможно даже в том случае, если сбои могут происходить в логических элементах (при условии, что вероятность ошибки в каждом элементе меньше

определенного порогового уровня). В следующих нескольких разделах мы объясним принципы квантового вычисления, устойчивого к ошибкам, которые приводят к этому замечательному результату. В подразд. 10.6.1 мы обрисуем общую картину, затем в подразд. 10.6.2 и 10.6.3 детально рассмотрим элементы квантового вычисления, устойчивого к ошибкам, и наконец в подразд. 10.6.4 обсудим некоторые ограничения на конструкции, устойчивые к ошибкам, а также возможности их расширения. Отметим, что строгое описание многих тонкостей квантового вычисления, устойчивого к ошибкам, выходит за пределы этой книги. Для интересующихся в конце главы приведен раздел «История и дополнительная литература».

10.6.1 Устойчивость к ошибкам, общая картина

Теория квантового вычисления, устойчивого к ошибкам, объединяет множество различных идей, ведущих к формулировке порогового условия. Ниже мы последовательно опишем их. Сначала рассмотрим вычисления над закодированными данными, объясним, при каких условиях вычислительная схема устойчива к накоплению и распространению ошибок. Затем введем фундаментальную модель шума для квантовых схем, что позволит дать более точное определение устойчивости к ошибкам. На конкретном примере элемента CNOT, устойчивого к ошибкам, объясним, как он предотвращает накопление и распространение ошибок. Наконец, опишем, как можно *каскадно* объединять устойчивые к ошибкам элементы, получим пороговую теорему для квантовых вычислений и дадим простую оценку пороговой величины.

Основные принципы

Основной идеей устойчивого к ошибкам квантового вычисления является выполнение всех операций над *закодированными квантовыми состояниями* таким образом, что декодирование вообще не требуется. Рассмотрим простую квантовую схему, такую, например, как на рис. 10.18. К сожалению, шуму подвержены все компоненты этой схемы: приготовление квантовых состояний, логические элементы, измерения и даже просто передача квантовых состояний. Чтобы защититься от шума, мы заменяем каждый кубит в исходной схеме на *закодированный блок* кубитов, используя для этого код, исправляющий ошибки, например семикубитовый код Стина. Каждый логический элемент заменяется на *схему (закодированный элемент)*, выполняющую действие этого элемента над закодированным состоянием, как показано на рис. 10.19.

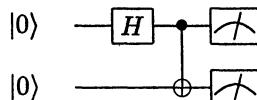


Рис. 10.18. Простая квантовая схема. Если вероятность сбоя в каждом из элементов равна p , то вероятность ошибки в выходных данных равна $O(p)$



Рис. 10.19. Схема, подобная изображенной на рис. 10.18, с использованием закодированных кубитов и закодированных логических элементов. Если все элементы схемы устойчивы к ошибкам, то вероятность ошибки в выходных данных равна $O(p^2)$, где p — вероятность сбоя в каждом элементе схемы. Обратите внимание на вторую процедуру исправления ошибок во втором кубите. Кажется, что эта процедура не должна выполняться, после предыдущего исправления ошибок с кубитом не происходит никаких изменений. Однако это не так. Хранение кубита может быть источником ошибок, поэтому такие ошибки следует периодически исправлять.

Последовательно выполняя процедуру исправления ошибок в закодированном состоянии, мы предотвращаем накопление ошибок. Конечно, чтобы предотвратить возникновение ошибок, недостаточно выполнять исправление ошибок даже после каждого закодированного элемента. Существуют две проблемы. Во-первых, и это самое важное, закодированные элементы могут приводить к распространению ошибок. Например, в элементе CNOT на рис. 10.20 ошибка в управляемом кубите распространяется и на управляемый кубит. Поэтому закодированный элемент должен быть реализован таким образом, чтобы любая ошибка могла распространяться только на небольшое число кубитов в каждом блоке закодированных данных. Это позволит эффективно исправлять такие ошибки. Такая реализация закодированных элементов называется *устойчивой к ошибкам*. Мы покажем, что возможно создать универсальный набор элементов — элемент Адамара, фазовый элемент, CNOT и $\pi/8$ -элементы, устойчивым к ошибкам. Вторая проблема заключается в том, что само исправление ошибок может вводить ошибки в закодированные кубиты. Здесь нужно тщательно следить за тем, чтобы сбой в процедуре исправления ошибок не вызвал слишком много ошибок в закодированных данных.

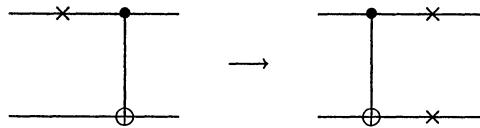


Рис. 10.20. Элемент CNOT вызывает распространение ошибки. Ошибка только в управляемом кубите передается на оба выходных кубита. Это верно и для закодированной версии элемента CNOT, работающей с закодированными кубитами.

Устойчивые к ошибкам операции: определения

Давайте определим более точно, что означает «процедура, устойчивая к ошибкам». Если сбой, происходящий только в одной компоненте процедуры, приводит к не более, чем одной ошибке в каждом выходном блоке кубитов, то такая процедура называется *устойчивой к ошибкам*. Например, рассмотрим

устойчивую к ошибкам процедуру исправления ошибок. Если сбой происходит в одной из ее компонент, то на выходе получаем блок кубитов с ошибкой не более, чем в одном кубите. Под «компонентой» процедуры мы понимаем любые элементарные операции, в том числе логические элементы, измерения, передачу и приготовление квантовых состояний. Определение устойчивости к ошибкам в литературе иногда имеет более общий вид, учитывающий некоторые дополнительные тонкости. Для наших целей достаточно приведенного выше определения.

Конечно, мы хотим применять в наших квантовых вычислениях не только закодированные элементы. Нам также будут нужны устойчивые к ошибкам процедуры измерения и приготовления квантовых состояний. Измерение наблюданной величины для набора закодированных кубитов назовем устойчивым к ошибкам, если в случае сбоя в одной компоненте этой процедуры ошибка возникнет не более, чем в одном кубите каждого блока выходных данных; кроме того, вероятность ошибки в измеренном результате должна быть $O(p^2)$, где p — максимальная вероятность сбоя в каждой компоненте процедуры измерения. Приготовление закодированного квантового состояния назовем устойчивым к ошибкам, если сбой в одном элементе этой процедуры приводит к ошибке не более, чем в одном кубите каждого блока выходных данных.

Чтобы сделать определение устойчивости к ошибкам более точным, необходимо определенная модель ошибок. Одно из основных упрощений, которое мы делаем, заключается в том, что мы рассматриваем только четыре типа ошибок — I , X , Y и Z , которые могут происходить стохастически с соответствующими вероятностями. Мы допускаем возможность скоррелированных ошибок в двух кубитах для элементов типа CNOT, однако полагаем, что они имеют вид тензорного произведения матриц Паули и имеют определенную вероятность. Такой подход позволит нам использовать знакомые методы классической теории вероятностей для определения вероятности того, что схема дает правильные результаты. При более сложном анализе устойчивости к ошибкам (см. раздел «История и дополнительная литература» в конце главы) рассматриваются гораздо более общие модели ошибок, допускающие, например, произвольно скоррелированные ошибки в нескольких кубитах. Однако, более сложные способы исследования устойчивости к ошибкам являются обобщением рассмотренного нами в сочетании с более глубоким анализом того факта (который мы уже рассматривали в этой главе), что для исправления непрерывного множества возможных ошибок достаточно исправить только некоторое дискретное множество ошибок.

Используя нашу модель ошибок, мы можем более точно определить что означает «распространение» ошибок по схеме. Рассмотрим, например, элемент CNOT, изображенный на рис. 10.20. Предположим, что перед применением CNOT в первом кубите возникла ошибка X . Если обозначить унитарный оператор, соответствующий элементу CNOT, через U , то действие схемы будет следующим: $UX_1 = UX_1U^\dagger U = X_1X_2U$, т. е. как если бы элемент был идеален, а затем ошибки X возникли в обоих кубитах. Дальше в этой главе мы будем часто применять подобное преобразование, чтобы посмотреть, как ошиб-

ки распространяются по нашей схеме. Более интересен пример распространения ошибки, когда сбой происходит в самом элементе CNOT. Пусть элементу CNOT с шумом соответствует квантовое преобразование \mathcal{E} . Это преобразование может быть записано в следующем виде: $\mathcal{E} = \mathcal{E} \circ \mathcal{U}^{-1} \circ \mathcal{U}$, где \mathcal{U} — преобразование, соответствующее идеальному элементу CNOT. Таким образом, действие элемента CNOT с шумом эквивалентно по действию идеального элемента CNOT, с последующим преобразованием $\mathcal{E} \circ \mathcal{U}^{-1}$. В случае, если наш элемент достаточно хороший, это преобразование близко к тождественному и может быть представлено в рамках нашей модели ошибок с помощью тензорных произведений операторов Паули, таких как $Z \otimes X$, действующих на два кубита с некоторой малой вероятностью p .

В приведенных ниже разделах будут подробно рассмотрены устойчивые к ошибкам реализации всех перечисленных операций: квантовая логика с универсальным набором элементов, измерение и приготовление квантовых состояний. Мы опишем конкретные схемы реализации кода Стина, которые легко обобщаются на другие симплектические коды. Сейчас, однако, представим, что у нас уже имеются все эти процедуры. Как использовать их, чтобы проводить безошибочное квантовое вычисление?

Пример: устойчивый к ошибкам элемент СНОУ

Рассмотрим реализацию устойчивого к ошибкам элемента CNOT с последующим исправлением ошибок, как показано на рис. 10.21. Кубиты будем рассматривать в четырех точках: на входе в схему (1), после элемента CNOT (2), после измерения синдрома (3) и после исправления ошибки (4). Мы хотим показать, что вероятность двух или более ошибок в первом закодированном блоке кубитов равна $O(p^2)$, где p — вероятность сбоя в каждом из компонент схемы. Так как идеальное декодирование (гипотетическое) первого блока кубитов не возможно только в случае двух или более ошибок в этом блоке, то, следовательно, схема увеличивает вероятность ошибки (в идеально декодированном кубите) на $O(p^2)$.



Рис. 10.21. Диаграмма устойчивого к ошибкам элемента, включающая исправление ошибок

Чтобы показать это, рассмотрим все возможные варианты, когда схема дает две или более ошибки в первом закодированном блоке кубитов.

- (1) По одной ошибке в каждом блоке входных данных. Это может стать причиной двух ошибок в первом выходном блоке, например, из-за распространения ошибки из второго блока в первый в закодированном элементе CNOT. Если входные данные до этого обрабатывались устойчивым к ошибкам способом, то можно утверждать, что вероятность ошибки в первом входном блоке кубитов равна $c_0 p$, так как эта ошибка должна произойти во время измерения синдрома или исправления ошибки на предыдущем шаге. Постоянная c_0 определяется числом мест, в которых могла произойти ошибка при выполнении этих операций. Если предположить, что вероятность ошибки во втором блоке кубитов также равна $c_0 p$ и что эти две ошибки (по одной в каждом блоке) происходят независимо, то мы получим для данного случая вероятность ошибки $c_0^2 p^2$. В конструкции кода Стина, которая будет описана ниже, вклад в c_0 дают шесть отдельных измерений синдромов, каждое из которых имеет примерно 10 позиций, в которых может произойти ошибка, и исправление ошибки, которое дает еще семь позиций, т. е. $c_0 \approx 70$.
- (2) Ошибка в одном из входных блоков и сбой в элементе CNOT. Вероятность этого равна $c_1 p^2$, где постоянная c_1 определяется количеством пар точек, где могут произойти такие ошибки. При использовании кода Стина ошибка во входном блоке может произойти примерно в 70 местах (мы это показали в предыдущем пункте). Это число надо умножить на 2 (так как ошибка может быть в любом из двух блоков) и на число мест в элементе CNOT, где может произойти сбой (в нашем случае это 7). В результате получаем $c_1 \approx 7 \times 2 \times 70 \approx 10^3$ пар позиций, в которых могут произойти две такие ошибки.
- (3) Обе ошибки происходят в элементе CNOT. Вероятность этого равна $c_2 p^2$, где c_2 — число пар точек в элементе CNOT, где могут произойти ошибки. Для кода Стина $c_2 \approx 10^2$.
- (4) Одна ошибка происходит в элементе CNOT, вторая — при измерении синдрома. Нас интересует только случай, когда измерение синдрома дает неправильный результат. Это происходит с вероятностью $c_3 p^2$ (для кода Стина $c_3 \approx 10^2$). Другой интересный (но несущественный для нас) случай — когда измерение синдрома дает правильный результат. В этом случае ошибка от элемента CNOT будет исправлена и на выходе останется только одна ошибка, возникшая при измерении синдрома.
- (5) Две или большее число ошибок возникают при измерении синдрома. Это происходит с вероятностью не более $c_4 p^2$, где c_4 — число пар точек, в которых могут возникнуть ошибки. (Для кода Стина $c_4 \approx 70^2 \approx 5 \times 10^3$.)
- (6) Одна ошибка возникает при измерении синдрома и одна — при исправлении ошибки. Это происходит с вероятностью не более $c_5 p^2$, где c_5 —

число пар точек, в которых могут возникнуть ошибки. (Для кода Стина $c_5 \approx 70 \times 7 \approx 500$.)

- (7) Две или большее число ошибок возникают при исправлении ошибок. Это происходит с вероятностью не более $c_6 p^2$, где c_6 — число пар точек, в которых могут возникнуть ошибки. (Для кода Стина $c_6 \approx 7^2 \approx 50$.)

Мы получили, что вероятность возникновения двух или большего числа ошибок в первом блоке кубитов в этой схеме не больше, чем cp^2 , где постоянная $c = c_0^2 + c_1 + c_2 + c_3 + c_4 + c_5 + c_6$. Для кода Стина $c \approx 10^4$. Если выполнить идеальное декодирование первого блока кубитов, то ошибки с вероятностью будут не больше cp^2 . Это действительно замечательный результат: нам удалось построить элемент CNOT, работающий без ошибок с вероятностью $1 - cp^2$, из элементов с вероятностью ошибки p . Это означает, что для достаточно малых p (например $p < 10^{-4}$) можно повысить надежность нашей схемы. Аналогичным образом можно рассмотреть другие компоненты, которые необходимы в квантовых вычислениях. Делая наши элементы устойчивыми к ошибкам, можно понизить вероятность ошибки в них с p до cp^2 для некоторой постоянной c . Мы оценили величину c только для CNOT элемента, однако, и для других устойчивых к ошибкам операций оценки дают близкие величины. Мы будем далее использовать $c \approx 10^4$ для количественных оценок.

Каскадные коды и пороговая теорема

Каскадные коды позволяют еще больше уменьшить вероятность ошибки. Идея заключается в рекурсивном применении метода, описанного выше, которое приводит к иерархии квантовых схем: C_0 (исходная схема), C_1 , C_2 и т.д. Сначала каждый кубит кодируется некоторым квантовым кодом, каждый кубит которого также кодируется, и так далее до бесконечности (см. рис. 10.22). Затем каждый элемент схемы C_0 , например элемент Адамара, заменяется на устойчивую к ошибкам процедуру в схеме C_1 , реализующую закодированный элемент Адамара и исправление ошибок. Затем каждый элемент цепи C_1 заменяется в цепи C_2 на процедуру, реализующую закодированную версию этого элемента и исправление ошибок, и т.д. Рассмотрим только что описанный двухуровневый каскадный код. Если вероятность ошибки на нижнем уровне (уровне физических кубитов) равна p , то на среднем уровне (один уровень кодирования) она равна cp^2 . На самом верхнем уровне (два уровня кодирования) вероятность того, что наша схема даст правильный результат, равна $c(cp^2)^2$. Следовательно, для каскадного кода с k уровнями вероятность ошибки равна $(cp)^{2^k}/c$, тогда как размер схемы для такого кода в d^k раз больше размера исходной схемы (d определяется максимальным числом операций, необходимых для построения устойчивой к ошибкам процедуры, реализующей закодированный элемент и исправление ошибок).

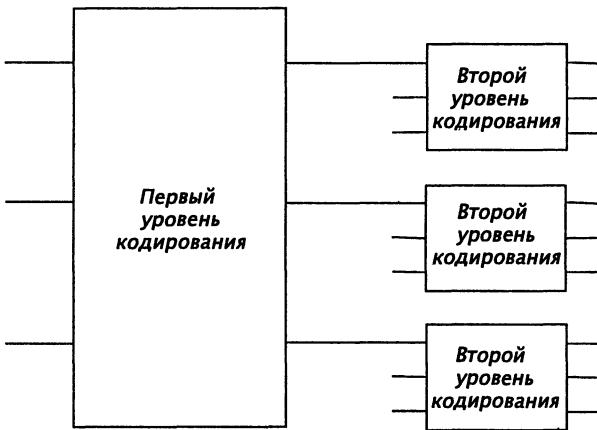


Рис. 10.22. Двухуровневый каскадный код, кодирующий один кубит девятью кубитами. Мы используем только трехкубитовые коды, чтобы сделать рисунок проще. В реальных схемах должен использоваться, например код Стина, позволяющий исправлять произвольные ошибки хотя бы в одном кубите.

Предположим, что мы хотим построить схему, содержащую $p(n)$ логических элементов, где n определяется размером задачи, а $p(n)$ — некоторый полином от n . Это может быть, например, схема для квантового алгоритма разложения на множители. Допустим, что мы хотим, чтобы окончательная точность нашей схемы была равна ε . Для этого необходимо, чтобы в каждом элементе верхнего уровня вероятность ошибки была равна $\varepsilon/p(n)$. Следовательно, число уровней k каскадного кода, который надо использовать, должен удовлетворять неравенству

$$\frac{(cp)^{2^k}}{c} \leq \frac{\varepsilon}{p(n)}. \quad (10.113)$$

Если $p < p_{\text{пор}} \equiv 1/c$, то такое k можно найти. Это условие, $p < p_{\text{пор}}$ называют *пороговым условием* для квантовых вычислений. Если оно выполняется, можно достичь произвольной точности вычислений. Насколько большим должен быть размер схемы, чтобы получить заданную точность? Заметим, что

$$d^k = \left(\frac{\log(p(n)/c\varepsilon)}{\log(1/p)} \right)^{\log d} = O(\text{poly}(\log p(n)/\varepsilon)), \quad (10.114)$$

где poly — полином некоторой фиксированной степени. Следовательно, наша схема содержит

$$O(\text{poly}(\log p(n)/\varepsilon)p(n)) \quad (10.115)$$

элементов, т. е. ее размер всего в $\text{poly}(\log p(n)/\varepsilon)$ раз больше размера исходной схемы. Обобщив наши рассуждения, получаем *пороговую теорему для квантовых вычислений*:

Теорема 10.9 (пороговая теорема для квантовых вычислений). Квантовая схема, состоящая из $p(n)$ логических элементов, может быть смоделирована с вероятностью ошибки не более ε с использованием

$$O(\text{poly}(\log p(n)/\varepsilon)p(n)) \quad (10.116)$$

физических элементов с вероятностью ошибки не более p , если p меньше некоторого *порогового значения* $p < p_{\text{пор}}$ и при заданных разумных предположениях о характере шума в физических элементах. Каково пороговое значение $p_{\text{пор}}$? Для кода Стина мы оценили, что $c \approx 10^4$; исходя из этого значения очень грубая оценка дает $p_{\text{пор}} \approx 10^{-4}$. Следует подчеркнуть, что наши рассуждения были (очень) нестрогими, гораздо более сложные вычисления дают величину порогового значения $10^{-5} - 10^{-6}$. Кроме того, эта величина очень сильно зависит от свойств вычислительной системы. Например, если в системе невозможны параллельные вычисления, то пороговое условие невозможно удовлетворить, поскольку ошибки в схеме будут накапливаться слишком быстро и их невозможно будет исправлять. Кроме квантовых операций требуются и классические вычисления, с помощью которых обрабатываются синдромы и определяется, какие элементы использовать для исправления ошибок. Обсуждение возможных ограничений при оценке порогового значения дано в подразд. 10.6.4.

Упражнение 10.62. Прямым вычислением покажите, что каскадный код, полученный объединением симплектических $[n_1, 1]$ - и $[n_2, 1]$ -кодов, является симплектическим $[n_1 n_2, 1]$ -кодом.

10.6.2 Устойчивые к ошибкам квантовые логические элементы

Основой построения устойчивых к ошибкам квантовых схем является создание устойчивых к ошибкам логических операций над закодированными состояниями. В гл. 4 (подрад. 4.5.3) мы показали, что элемент Адамара, фазовый элемент, CNOT и $\pi/8$ -элемент образуют универсальный набор логических элементов, на основе которого может быть реализовано любое квантовое вычисление. Ниже мы опишем устойчивые к ошибкам реализации.

Образующие нормализатора

Начнем с устойчивых к ошибкам реализаций образующих нормализатора — элемента Адамара, фазового элемента и CNOT для случая кода Стина. Поняв основные принципы такой нормализации, их легко обобщить на любой симплектический код. Из формулы (10.107) операторы Паули \bar{Z} и \bar{X} , действующие на закодированные состояния, могут быть выражены через операторы Паули для незакодированных состояний следующим образом:

$$\bar{Z} = Z_1 Z_2 Z_3 Z_4 Z_5 Z_6 Z_7; \quad \bar{X} = X_1 X_2 X_3 X_4 X_5 X_6 X_7. \quad (10.117)$$

Закодированный элемент Адамара \bar{H} должен при сопряжении менять \bar{X} на \bar{Z} и наоборот (то есть $\bar{H}\bar{X}\bar{H}^\dagger = \bar{Z}$ и $\bar{H}\bar{Z}\bar{H}^\dagger = \bar{X}$), также как элемент Адамара меняет \bar{Z} на \bar{X} и наоборот. Таким свойством обладает оператор $\bar{H} =$

$H_1H_2H_3H_4H_5H_6H_7$, следовательно, элемент Адамара для закодированного кубита может быть реализован, как показано на рис. 10.23.

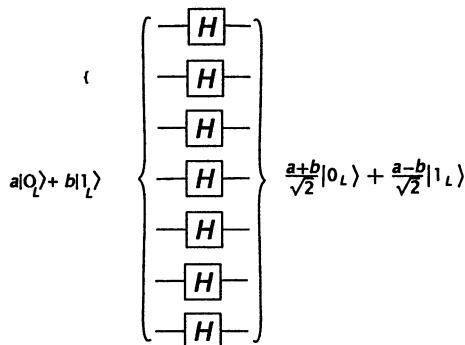


Рис. 10.23. Побитовая реализация элемента Адамара для кубита, закодированного кодом Стина.

Упражнение 10.63. Пусть U — унитарный оператор на подпространстве кода Стина и $U\bar{Z}U^\dagger = \bar{X}$ и $U\bar{X}U^\dagger = \bar{Z}$. Докажите, что с точностью до общего фазового множителя оператор U следующим образом действует на закодированные состояния: $|0_L\rangle \rightarrow (|0_L\rangle + |1_L\rangle)/\sqrt{2}$ и $|1_L\rangle \rightarrow (|0_L\rangle - |1_L\rangle)/\sqrt{2}$.

То, что мы нашли такой оператор — очень хорошее начало, однако теперь нужно доказать, что он устойчив к ошибкам. Для этого рассмотрим, как распространяются ошибки. Так как в нашей реализации элемента Адамара $\bar{H} = H^{\otimes 7}$ никакие два кубита не взаимодействуют, разумно предположить, что сбой в одной компоненте схемы приведет к не более чем одной ошибке в выходном блоке кубитов. Пусть ошибка произошла в первом кубите на входе элемента Адамара. Для определенности докажем, что это ошибка Z . Тогда полное действие на первый кубит описывается оператором HZ . Как и при рассмотрении элемента CNOT, применяя тождественный оператор $I = H^\dagger H$, получим $HZ = HZH^\dagger H = XH$, т. е. результат такой, как если бы после элемента Адамара в кубите возникла ошибка X . Аналогично, если ошибка произошла в самом элементе Адамара, его действие эквивалентно действию идеального элемента и небольшому шуму в кубите после него. Этот шум в рамках нашей модели описан операторами X , Y и Z , каждый из которых действует с некоторой небольшой вероятностью. Таким образом, схема на рис. 10.23 действительно устойчива к ошибкам, так как сбой не распространяется на соседние кубиты и, следовательно, не создает более одной ошибки в выходном блоке кубитов.

Из рассмотрения схемы, приведенной на рис. 10.23, можно получить представление об общих принципах. Во-первых, любой реализованный побитово элемент автоматически получается устойчивым к ошибкам. Сбой в таком элементе не создаст более одной ошибки в выходном блоке кубитов и, следовательно, вероятность ошибки не увеличивается, оставаясь под контролем кода, исправляющего ошибки. Говорят, что такие элементы обладают *свойством переноса*. Свойство переноса полезно тем, что оно дает общий принцип построения

ния квантовых схем, устойчивых к ошибкам. Мы увидим, что многие элементы имеют свойства переноса. Однако, устойчивый к ошибкам элемент не обязательно должен обладать свойством переноса; мы увидим это ниже на примере $\pi/8$ -элемента.

Используя код Стина, многие элементы помимо элемента Адамара можно реализовать побитово (следовательно, они будут устойчивы к ошибкам). Наиболее интересными из них являются—фазовый элемент и элементы Паули Z и X . Если побитово применить элемент X к каждому из семи кубитов кода Стина, оператор Z преобразуется в $-Z$ и, следовательно, $\tilde{Z} \rightarrow (-1)^7 \tilde{Z} = -\tilde{Z}$, а $\tilde{X} \rightarrow \tilde{X}$. Поэтому такая схема реализует закодированный элемент X для кода Стина. Она также обладает свойством переноса и, следовательно, устойчива к ошибкам. Точно так же, побитово применяя оператор Z , получим устойчивую к ошибкам реализацию закодированного элемента Z . Реализация фазового элемента, обладающего свойством переноса, немного интереснее. Элемент \tilde{S} должен преобразовывать \tilde{Z} в \tilde{Z} , а \tilde{X} в $\tilde{Y} = i\tilde{X}\tilde{Z}$. Однако, если мы применим элемент $\tilde{S} = S_1S_2S_3S_4S_5S_6S_7$, то получим преобразование \tilde{Z} в \tilde{Z} и \tilde{X} в $-\tilde{Y}$. Минус перед $-\tilde{Y}$ можно убрать с помощью оператора \tilde{Z} . Следовательно, применив операцию ZS к каждому кубиту, получим закодированный фазовый элемент, обладающий свойством переноса и, следовательно, устойчивый к ошибкам.

Реализация устойчивого к ошибкам элемента CNOT по сравнению с реализацией элементов Адамара и Паули, а также фазового элемента—на первый взгляд более сложная задача, так как мы должны работать с двумя блоками из семи кубитов. Как реализовать элемент CNOT, который не вносит больше одной ошибки в кодовый блок? К счастью, при использовании кода Стина это оказывается совсем не сложно. Соответствующая схема показана на рис. 10.24; легко увидеть, что это просто семь элементов CNOT, применяемых к соответствующим парам кубитов в двух блоках. Вас может смутить, что эта конструкция нарушает наши правила; ведь ошибка в элементе CNOT может распространиться на оба кубита! Это верно, но в данном случае несущественно, так как распространение ошибки может испортить кубит в другом блоке. В случае одной ошибки в каждом блоке выполняется условие устойчивости к ошибкам.

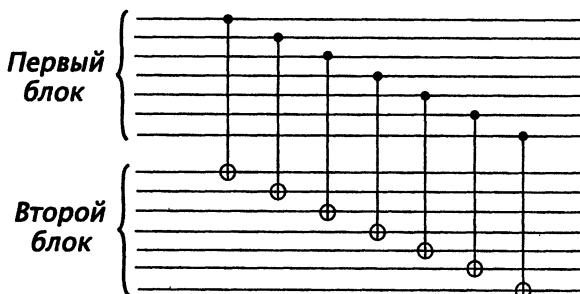


Рис. 10.24. Элемент CNOT, обладающий свойством переноса, для двух блоков кубитов, закодированных кодом Стина

Более подробно, предположим, что, например, ошибка X возникает в первом кубите перед элементом CNOT, который действует на первые кубиты каждого блока (будем называть их кубитами 1 и 8). Обозначив действие элемента CNOT через U , для действия схемы с учетом ошибки получим $UX_1 = UX_1U^\dagger U = X_1X_8U$, т. е. как если бы элемент CNOT сработал правильно, но после него возникли ошибки X в первых кубитах каждого блока. Несколько сложнее случай сбоя в самом элементе CNOT. Пусть действие ошибочного элемента описывается квантовым преобразованием \mathcal{E} . Это преобразование может быть переписано в виде $\mathcal{E} = \mathcal{E} \circ \mathcal{U}^{-1} \circ \mathcal{U}$, где преобразование \mathcal{U} описывает действие идеального элемента CNOT. Следовательно, действие ошибочного элемента эквивалентно идеальному действию элемента CNOT и последующей ошибке $\mathcal{E} \circ \mathcal{U}^{-1}$, которая близка к тождественному преобразованию, если элемент CNOT достаточно хороший. В этом случае ошибка может быть представлена в рамках нашей модели ошибок через тензорные произведения операторов Паули, такие как $X \otimes Z$, которые действуют на два кубита с некоторой малой вероятностью. К счастью, хотя ошибки и возникают в двух кубитах, эти кубиты принадлежат разным блокам. Аналогичные рассуждения можно провести и для ошибки, возникающей в других местах. Итак, ошибка в одной компоненте нашей схемы распространяется не более, чем на один кубит каждого кодового блока, так что эта реализация закодированного элемента CNOT является устойчивой к ошибкам.

Мы только что построили устойчивые к ошибкам элемент Адамара, фазовый элемент и CNOT. Согласно теореме 10.6, из них можно сконструировать любой устойчивый к ошибкам элемент нормализатора. Конечно, такие элементы не исчерпывают всех возможных унитарных операций, необходимых для квантовых вычислений, однако это многообещающее начало!

Упражнение 10.64 (обратное распространение ошибок). Очевидно, что ошибка X в управляющем кубите элемента CNOT распространяется на управляемый кубит. Оказывается, что ошибка Z в управляемом кубите распространяется обратно на управляющий кубит! Покажите это, используя формализм стабилизаторов, а также тождественность квантовых схем. Вам может пригодиться упражнение 4.20.

Устойчивый к ошибкам $\pi/8$ -элемент

Нам осталось построить всего один устойчивый к ошибкам элемент, чтобы получить стандартный набор элементов для универсального квантового вычисления. Это $\pi/8$ -элемент. Мы можем также получить универсальный набор элементов, добавив к уже имеющимся у нас элементу Адамара, фазовому элементу и элементу CNOT устойчивый к ошибкам элемент Тоффоли (см. подразд. 4.5.3). Это позволит проводить произвольное квантовое вычисление устойчивым к ошибкам способом. Оказывается, устойчивый к ошибкам $\pi/8$ -элемент очень легко построить; используя более сложные конструкции, можно реализовать и элемент Тоффоли.

Построим схему, реализующую $\pi/8$ -элемент с помощью уже известных, устойчивых к ошибкам элементов, таких как CNOT, фазовый и X элементы.

В этой схеме, однако, есть две компоненты, про которые мы пока не знаем, как сделать их устойчивыми к ошибкам. Одна из них — это приготовление *вспомогательного состояния*. Нужно, чтобы сбой в любом элементе приводил к не более чем одной ошибке в блоке кубитов, кодирующем вспомогательное состояние. Как это может быть сделано, мы объясним позже в этом разделе. Вторая компонента этой схемы — измерение. Нужно, чтобы ошибка в любом элементе процедуры измерения не влияла на его результат. Если это произойдет, ошибка распространится на несколько кубитов первого блока, так как выполнение закодированной операции SX зависит от результата измерения. Как построить такую процедуру измерения, описано в следующем разделе. (Строго говоря, для этой устойчивой к ошибкам процедуры измерения вероятность ошибки равна $O(p^2)$, где p — вероятность ошибки в одном элементе процедуры. Мы пренебрежем этим в нашем рассмотрении. Более точный анализ немного сложнее и может быть проведен аналогичным образом.)

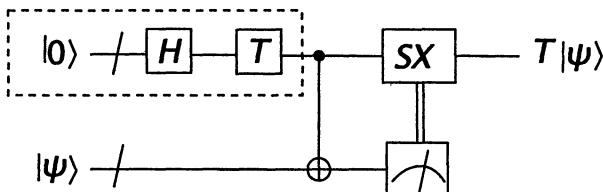


Рис. 10.25. Квантовая схема, реализующая устойчивый к ошибкам $\pi/8$ -элемент. Пунктиром обведена часть схемы для процедуры приготовления вспомогательного состояния $(|0\rangle + \exp(i\pi/4)|1\rangle)/\sqrt{2}$. Эта процедура не является устойчивой к ошибкам, как реализовать ее устойчивым к ошибкам способом, описано в тексте. Перечеркнутые линии обозначают семикубитовые блоки, двойная линия — классический бит, являющийся результатом измерения. Элемент SX управляет результатом измерения

На рис. 10.25 показана схема, реализующая $\pi/8$ -элемент. Все части схемы могут быть сделаны устойчивыми к ошибкам, за исключением может быть части, обведенной пунктирной рамкой, и измерения. В начале работы схемы мы имеем два закодированных кубита. Это кубит $|\psi\rangle = a|0\rangle + b|1\rangle$, который мы хотим преобразовать ($|0\rangle$ и $|1\rangle$ обозначают здесь логические состояния) и приготовленный кубит в состоянии

$$|\Theta\rangle = \frac{|0\rangle + \exp(i\pi/4)|1\rangle}{\sqrt{2}}. \quad (10.118)$$

Приготовление такого состояния осуществляет часть схемы, обведенная пунктирной рамкой. Как сделать эту процедуру устойчивой к ошибкам, мы вскоре объясним. Применение элемента CNOT к этим двум состояниям дает

$$\begin{aligned} & \frac{1}{\sqrt{2}} [|0\rangle (a|1\rangle + b|0\rangle) + \exp(i\pi/4)|1\rangle (a|0\rangle + b|1\rangle)] \\ &= \frac{1}{\sqrt{2}} [(a|0\rangle + b \exp(i\pi/4)|1\rangle)|0\rangle + (b|0\rangle + a \exp(i\pi/4)|1\rangle)|1\rangle]. \end{aligned} \quad (10.119)$$

После этого мы измеряем второй кубит. Если в результате получается 0, то операция завершена. В противном случае на первый кубит действуем оператором

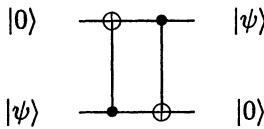
$$SX = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \quad (10.120)$$

В результате получаем состояние $a|0\rangle + b \exp(i\pi/4)|1\rangle$ (с точностью до общего фазового множителя), что и требовалось. Подробно получение этого результата описано ниже в упражнениях. Такая же конструкция используется и для реализации устойчивого к ошибкам элемента Тоффоли (см. упражнение 10.68).

Для построения устойчивого к ошибкам $\pi/8$ -элемента требуется устойчивый к ошибкам метод приготовления вспомогательного состояния Θ . Такое приготовление можно осуществить с использованием устойчивого к ошибкам измерения, которое детально описано в следующем разделе. Как показано на рис. 10.25, Θ можно приготовить, применяя элемент Адамара и затем $\pi/8$ -элемент к состоянию $|0\rangle$. Состояние $|0\rangle$ является собственным состоянием оператора Z и соответствует собственному значению +1. Поэтому Θ является собственным состоянием оператора $THZHT^\dagger = TXT^\dagger = e^{-i\pi/4}SX$, также соответствующим собственному значению +1. Следовательно, состояние Θ может быть приготовлено с помощью устойчивого к ошибкам измерения состояния $|0\rangle$ оператором $e^{-i\pi/4}SX$. Если получен результат +1, значит состояние Θ приготовлено правильно. Если же мы получили -1, можно либо повторять эту процедуру сначала, пока не получим +1, либо применить к полученному состоянию устойчивый к ошибкам элемент Z . В последнем случае, поскольку $ZSXZ = -SX$, из собственного состояния оператора $e^{-i\pi/4}SX$, соответствующего собственному значению -1, мы получим собственное состояние, соответствующее собственному значению +1. Какой бы из этих способов мы не применили, любой сбой в нашей процедуре приведет не более, чем к одной ошибке в одном кубите закодированного состояния Θ .

Нетрудно видеть, что процедура для $\pi/8$ -элемента, которую мы описали, устойчива к ошибкам как единое целое. Однако, может быть полезно это рассмотреть на конкретном примере. Предположим, что сбой происходит при построении вспомогательного состояния и в одном из его кубитов возникает ошибка. Ошибка распространяется через закодированный элемент CNOT на соответствующие кубиты в каждом из двух блоков. Одна ошибка во втором блоке не влияет на результат измерения (так как измерение устойчиво к ошибкам), поэтому мы правильно определим, применять или нет элемент SX . Ошибка в первом блоке распространится через этот элемент, что приведет к одной ошибке в выходном блоке кубитов. Также можно показать, что любая одиночная ошибка в нашей реализации $\pi/8$ -элемента не приведет к более, чем одной ошибке в выходном кодовом блоке.

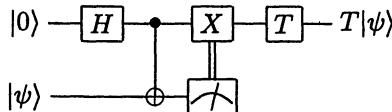
Упражнение 10.65. Можно произвести обмен кубита в неизвестном состоянии $|\psi\rangle$ с кубитом, приготовленным в состоянии $|0\rangle$ с помощью двух элементов CNOT, используя схему рисунка



Покажите, что приведенные ниже две схемы с одним элементом СNOT, измерением и классически управляемым однокубитовым элементом выполняют ту же задачу.

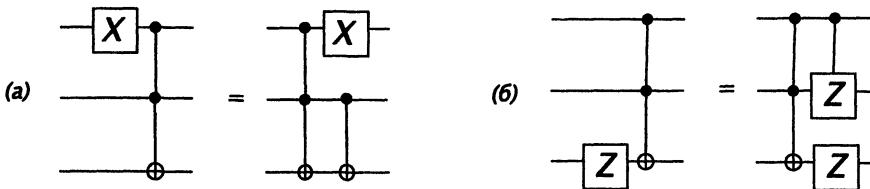


Упражнение 10.66 (устойчивый к ошибкам $\pi/8$ -элемент). Один из способов сделать устойчивый к ошибкам $\pi/8$ -элемент состоит в следующем: обменять кубит в состоянии $|\psi\rangle$ с кубитом в известном состоянии $|0\rangle$ и затем применить $\pi/8$ -элемент к результату. Это можно сделать с помощью приведенной ниже схемы.



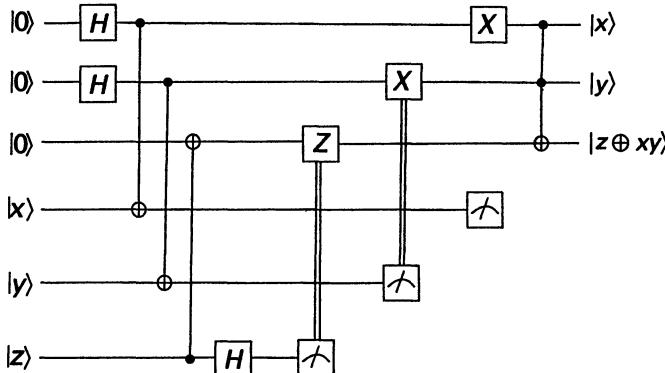
На первый взгляд кажется, что эти действия бесполезны, однако это не так. Покажите, используя соотношения $TX = \exp(-i\pi/4)SX$ и $TU = UT$ (U — элемент СNOT, T действует на управляющий кубит), что эта схема эквивалентна схеме на рис. 10.25.

Упражнение 10.67. Покажите, что приведенные ниже схемы эквивалентны.

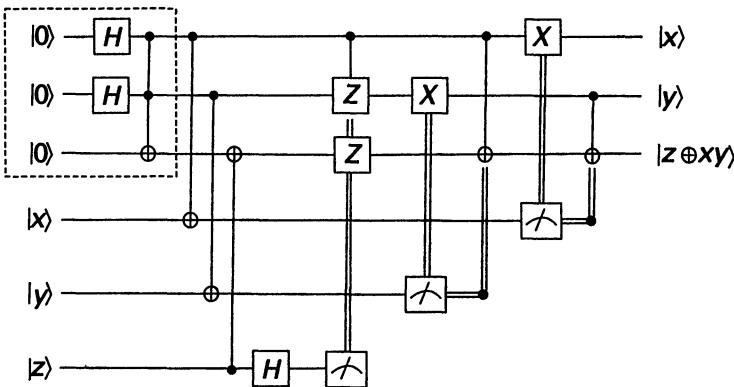


Упражнение 10.68 (устойчивый к ошибкам элемент Тоффоли). С помощью процедуры, использованной в предыдущих упражнениях для $\pi/8$ -элемента, можно построить устойчивый к ошибкам элемент Тоффоли.

- (1) Произведем обмен трехкубитового состояния $|xyz\rangle$, которое мы хотим преобразовать, с известным состоянием $|000\rangle$. После этого применим элемент Тоффоли к полученным кубитам. Покажите, что приведенная ниже схема выполняет именно такие действия.



- (2) Используя правила коммутации из упр. 10.67, покажите, что если перенести элемент Тoffoli в левую часть, то получится следующая схема:



- (3) Предположив, что схема приготовления вспомогательного состояния, обведенная пунктирной рамкой, может быть сделана устойчивым к ошибкам способом, покажите, что вся схема дает устойчивую к ошибкам реализацию элемента Тoffoli для кода Стина.

10.6.3 Устойчивое к ошибкам измерение

Очень полезным и важным средством при конструировании устойчивых к ошибкам схем является возможность *измерять оператор* M . Измерения нужны для кодирования данных, считывания результатов вычисления, определения синдрома при исправлении ошибок, а также для приготовления вспомогательных состояний, используемых в реализациях устойчивых к ошибкам элементов Тoffoli и $\pi/8$. Измерения абсолютно необходимы для проведения устойчивых к ошибкам квантовых вычислений. Чтобы измерение было устойчивым к ошибкам, должны выполняться два условия. Во-первых, сбой в любом

месте процедуры измерения должен приводить не более, чем к одной ошибке в получном блоке кубитов. Во-вторых, результат измерения должен быть правильным с вероятностью $1 - O(p^2)$, где p — вероятность сбоя. Последнее условие очень важно, так как результат измерения может быть использован для управления другими элементами квантового компьютера, и если он неправильный, ошибка может распространиться на многие кубиты в других кодовых блоках.

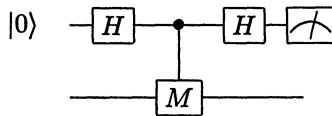


Рис. 10.26. Квантовая схема для измерения однокубитового оператора M с собственными значениями ± 1 . Вспомогательный кубит — верхний, измеряемый — нижний

Измерение однокубитовой наблюдаемой величины M можно выполнить с помощью схемы, изображенной на рис. 10.26. Пусть реализация оператора M над закодированным кубитом обладает свойством переноса, т. е. к каждому кубиту кода применяется оператор M' . Например, для кода Стина оператор $M = H$ можно реализовать путем побитового применения операторов $M' = H$, а оператор $M = S$ — путем побитового применения $M' = ZS$. Можно построить схему для измерения закодированного оператора M , как показано на рис. 10.27. (Реальный квантовый код, например Стина, требует большего числа кубитов). К сожалению, такая схема не устойчива к ошибкам. Если сбой происходит во вспомогательном состоянии на входе схемы, ошибка распространится на все закодированные кубиты.

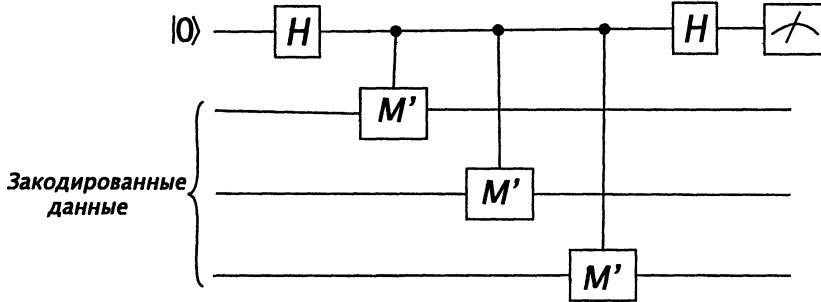


Рис. 10.27. Схема процедуры измерения закодированной наблюдаемой величины M с помощью побитового применения операторов M' . Схема не устойчива к ошибкам. Реальный код требует больше трех кубитов

Замечательный способ построения устойчивой к ошибкам измерительной схемы схематически иллюстрируется на рис. 10.28. В целях упрощения данные на рисунке кодируются только тремя кубитами. На практике нужно использовать больше кубитов, например кодировать данные семикубитовым кодом Стина. Кроме закодированных данных, в схеме используются вспомогательные

кубиты в состоянии $|0\rangle$, по одному на каждый кубит данных. Прежде всего, переведем вспомогательные кубиты в состояние Шрёдингера $|00\dots0\rangle + |11\dots1\rangle$ (обратите внимание, что это состояние не закодировано). Используемая для этого схема не устойчива к ошибкам, потому что ошибка в одном из кубитов может распространиться на несколько кубитов состояния Шрёдингера. Тем не менее, это не влияет на устойчивость к ошибкам всей схемы, так как после приготовления состояния Шрёдингера мы проводим несколько шагов *проверки* (на рисунке показан только один).

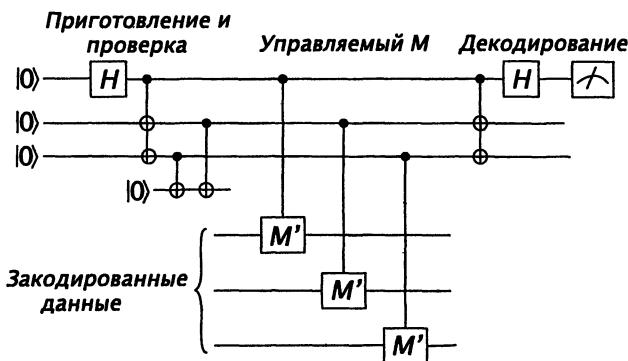


Рис. 10.28. Схема устойчивой к ошибкам процедуры измерения наблюдаемой величины M для закодированных данных. Эта процедура повторяется три раза, результат измерения определяется путем выбора по большинству. Вероятность ошибочного результата измерения равна $O(p^2)$, где p — вероятность сбоя в одной компоненте схемы. При одном сбое в схеме в закодированных данных возникает не более одной ошибки.

Процедура проверки работает следующим образом. Чтобы проверить, что состояние является состоянием Шрёдингера, достаточно проверить, что измерения всех величин $Z_i Z_j$ дают 1, т. е., что сумма любых двух кубитов четна. Чтобы проверить конкретную пару кубитов $Z_i Z_j$ ($Z_2 Z_3$ на рисунке) используем дополнительный кубит в состоянии $|0\rangle$. Мы определяем четность суммы двух кубитов, применяя к ним два элемента CNOT с вспомогательным кубитом в качестве управляемого, и затем измеряем дополнительный кубит. Если измеренная четность равна 1, это означает, что вспомогательное состояние — не состояние Шрёдингера, выбрасываем его и начинаем готовить заново. Пусть в одной из проверок четности произошел сбой. Проверка четности неустойчива к ошибкам; легко показать, что возможен сбой, приводящий к более чем одной ошибке в кубитах вспомогательного состояния. Например, если в дополнительном кубите возникла ошибка Z перед применением элементов CNOT, это вызовет ошибки Z в двух кубитах вспомогательного состояния. К счастью, можно показать, что несколько ошибок Z в кубитах вспомогательного состояния не распространяются на закодированные данные, хотя и могут привести к неправильному результату измерения. Чтобы справиться с этой проблемой, мы (как подробно описано ниже), производим измерение трижды и затем выбираем результат по большинству. Таким образом, вероятность неправильного результата (т. е. ошибки в двух или трех измерениях) равна $O(p^2)$, где p —

вероятность одного сбоя. Ошибки X и Y могут распространяться на закодированные данные, однако, к счастью, один сбой при подготовлении и проверке вспомогательного состояния может стать причиной только одной ошибки X или Y во вспомогательном состоянии, а, следовательно, и в закодированных данных. Это означает, что описанная нами процедура устойчива к ошибкам.

Упражнение 10.69. Покажите, что один сбой при подготовлении и проверке вспомогательного состояния приводит не более, чем к одной ошибке X или Y в этом состоянии.

Упражнение 10.70. Покажите, что ошибки Z во вспомогательном состоянии не распространяются на закодированные данные, но могут стать причиной неправильного результата измерения.

После того как состояние Шрёдингера проверено, мы применяем управляемый элемент M' между парами кубитов вспомогательного состояния и закодированными данными, используя каждый кубит вспомогательного состояния не более одного раза. Если вспомогательное состояние есть $|00\dots0\rangle$, закодированные данные остаются без изменения, если же вспомогательная система находится в состоянии $|11\dots1\rangle$, к закодированным данным применяется закодированный элемент M . Структура состояния Шрёдингера такова, что ошибки не могут распространяться от одного управляемого элемента M' к другому. Следовательно, один сбой при проверке вспомогательного состояния не приведет к более, чем одной ошибке в закодированных данных. Результат измерения получается декодированием состояния Шрёдингера с помощью набора элементов CNOT и элемента Адамара. Полученный кубит находится в состоянии 0 или 1 в зависимости от собственного значения M , соответствующего состоянию данных. Последние элементы никак не влияют на данные и, следовательно, ошибка в них не может распространиться на кубиты данных. Однако она может повлиять на правильность результата измерения. Если повторить процедуру измерения три раза и выбрать результат по большинству, то вероятность ошибки в результате измерения будет равна $O(p^2)$, где p — вероятность сбоя в одной компоненте схемы.

Мы описали метод проведения устойчивых к ошибкам измерений, такой, что результат измерения ошибочен с вероятностью $O(p^2)$, а один сбой приводит не более, чем к одной ошибке в закодированных данных. Эта конструкция может быть применена для любой однокубитовой наблюдаемой величины M , закодированный вариант которой может быть реализован побитово. Для кода Стина такими величинами могут быть элемент оператор Адамара, фазовый оператор и операторы Паули и с некоторой модификацией наблюдаемая $M = e^{-i\pi/4}SX$. Чтобы построить управляемый элемент для такого оператора M , мы побитово применяем управляемый элемент ZXS к каждой паре кубитов во вспомогательном состоянии и закодированных данных, а затем к каждому кубиту вспомогательного состояния применяем элемент T . Как показано в подразд. 10.6.2, устойчивое к ошибкам измерение этой наблюдаемой величины может быть использовано для приготовления вспомогательного со-

стояния, используемого в устойчивой к ошибкам реализации $\pi/8$ -элемента.

Упражнение 10.71. Проверьте, что для $M = e^{-i\pi/4}SX$ только что описанная процедура измерения M устойчива к ошибкам.

Упражнение 10.72 (построение вспомогательного состояния для устойчивого к ошибкам элемента Тоффоли). В упр. 10.68 обведенный пунктирной рамкой участок схемы приготовляет вспомогательное состояние

$$\frac{|000\rangle + |010\rangle + |100\rangle + |111\rangle}{\sqrt{2}}. \quad (10.121)$$

Покажите, как можно построить такое состояние устойчивым к ошибкам способом. Для этого может быть полезно найти образующие стабилизатора этого состояния.

Измерение образующих стабилизатора

Мы описали устойчивую к ошибкам процедуру измерения, когда M — однокубитовая наблюдаемая величина. Этот метод можно обобщить и на более общий случай. Для наших целей достаточно научиться измерять образующие стабилизатора, которые имеют вид тензорного произведения матриц Паули. Такие измерения позволят выполнить устойчивую к ошибкам процедуру исправления ошибок, начальное кодирование данных и измерение закодированных операторов Z для получения результатов вычисления.

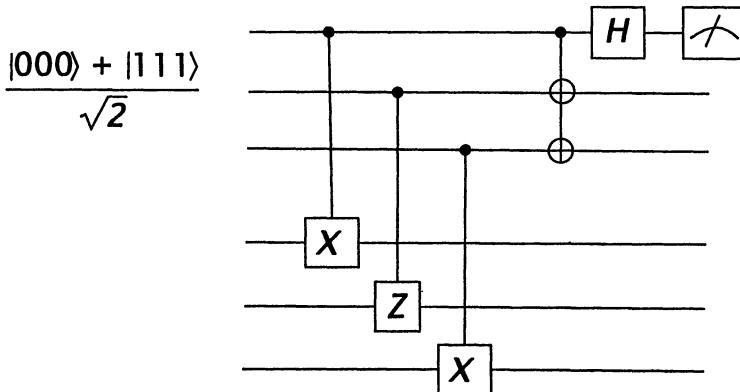


Рис. 10.29. Схема устойчивого к ошибкам измерения оператора XZX на трех кубитах.

В качестве простого примера предположим, что мы хотим измерить оператор $X_1Z_2X_3$, действующий на три первых кубита семикубитового блока, закодированного кодом Стина. Очевидное обобщение процедуры, проиллюстрированной на рис. 10.28, для такого измерения показано на рис. 10.29. Мы, как и раньше, приготавливаем и проверяем состояние Шредингера, а затем побитово применяем к закодированным данным управляемые операторы, чтобы получить устойчивую к ошибкам процедуру измерения оператора $X_1Z_2X_3$. Имея

возможность устойчиво к ошибкам измерять такие наблюдаемые величины, мы можем выполнять кодирование данных, измерение синдрома, измерение в (логическом) вычислительном базисе, т. е. все, что необходимо для квантового вычисления. Для кодирования достаточно приготавливать закодированное состояние $|0\rangle$. В случае симплектического кода (например, кода Стина) это можно сделать устойчивым способом измерив образующие стабилизатора и закодированный оператор \tilde{Z} , а затем исправив знаки образующих стабилизатора и закодированного \tilde{Z} , как было описано в доказательстве утверждения 10.4 в подразд. 10.5.1. В упр. 10.73 приведен пример устойчивого к ошибкам приготовления состояния $|0\rangle$, закодированного кодом Стина. Устойчивые к ошибкам измерения синдрома и измерения в закодированном вычислительном базисе реализуются аналогичным образом.

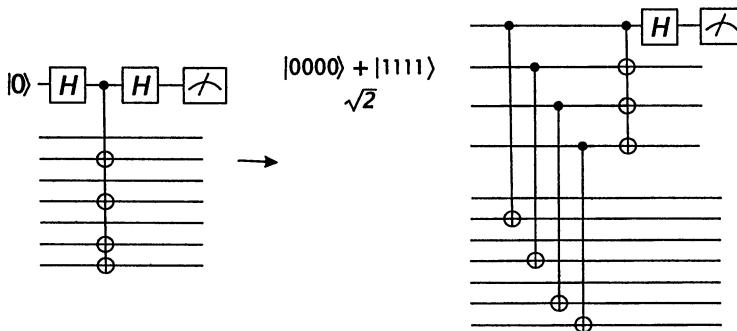


Рис. 10.30. Один этап устойчивой к ошибкам процедуры приготовления состояния $|0\rangle$, закодированного кодом Стина

Упражнение 10.73 (устойчивое к ошибкам построение закодированного состояния). Закодированное кодом Стина состояние $|0\rangle$ может быть построено следующим, устойчивым к ошибкам способом:

- (1) Начните со схемы, изображенной на рис. 10.16, и замените измерения образующих, как показано на рис. 10.30. Здесь вспомогательные кубиты находятся в состоянии Шрёдингера $|00\dots 0\rangle + |11\dots 1\rangle$, а операции переставлены так, чтобы использовать разные вспомогательные кубиты в качестве управляющих. При этом ошибки не распространяются внутри кодового блока.
- (2) Добавьте устойчивое к ошибкам измерение \tilde{Z} .
- (3) Вычислите вероятность ошибки этой схемы, а также схемы, в которой измерения образующих выполняются три раза и результат выбирается по большинству.
- (4) Перечислите все операции, которые должны управляться результатами измерения, и покажите, что они могут быть сделаны устойчивыми к ошибкам.

Упражнение 10.74. Постройте устойчивую к ошибкам квантовую схему для приготовления состояния $|0\rangle$, закодированного пятикубитовым кодом (см. подразд. 10.5.6).

10.6.4 Элементы надежного квантового вычисления

Наиболее важным результатом теории квантовых кодов, исправляющих ошибки, является *пороговая теорема для квантовых вычислений*. Она утверждает, что, если шум в отдельных квантовых элементах меньше некоторого порогового значения, можно эффективно выполнить произвольно длинное квантовое вычисление. Другими словами, шум не является серьезной проблемой для квантовых вычислений. Основная идея доказательства этого утверждения была намечена в подразд. 10.6.1. Выполнение устойчивых к ошибкам операций над закодированными состояниями попаременно с исправлением ошибок приведет к уменьшению вероятности ошибки с p до $O(p^2)$. Строя каскадные коды и иерархические устойчивые к ошибкам процедуры для них, можно уменьшить вероятность ошибки до $O(p^4)$, затем до $O(p^8)$ и далее до уровня, который нам необходим. Это можно сделать, если только вероятность ошибки $p < p_{\text{пор}}$. Для описанных выше процедур мы оценили пороговое значение $p_{\text{пор}} \sim 10^{-5} - 10^{-6}$.

Такое сильное утверждение, как пороговая теорема нуждается в уточнениях. Из нее не следует, что квантовое вычисление можно защитить от совершенно произвольного шума. Пороговая теорема основывается на небольшом количестве физически разумных предположений о виде шума, действующего на квантовый компьютер, и об имеющейся архитектуре квантового компьютера. Модель ошибки, которую мы рассмотрели, достаточно проста, и, конечно, в случае реального квантового компьютера нам придется иметь дело и с другими типами шума. Тем не менее, по-видимому введенные здесь методы в сочетании с более сложными квантовыми кодами, исправляющими ошибки, и более сложным анализом позволяют сформулировать пороговую теорему с более широкой областью применимости, чем мы рассматривали.

У нас нет возможности выполнить здесь более сложный анализ; приведем только несколько наблюдений. Во-первых, полезно заметить, что пороговая теорема требует наличия большой степени параллельности в нашей схеме. Даже если мы хотим всего лишь хранить квантовую информацию, нам периодически придется исправлять ошибки и для этого нужна схема с большой степенью параллельности. Поэтому важной задачей будущих создателей квантовых компьютеров является разработка архитектур, обеспечивающих параллельное вычисление, с тем, чтобы были применимы методы устойчивого к ошибкам квантового вычисления. Во-вторых, при рассмотрении пороговой величины мы совершенно пренебрегали сложностью *классических* вычислений и передачи данных, которые необходимы при приготовлении состояний, измерении синдрома и восстановлении состояний. Эта сложность может быть велика. Например, для восстановления состояний на высших уровнях каскадных кодов необходима передача классической информации между всеми частями квантовой системы. Эта передача должна выполняться гораздо быстрее, чем возни-

кают ошибки, иначе ошибки будут появляться снова, сводя на нет действие процедур исправления ошибок. Можно провести более сложный анализ этой проблемы, однако как и при других усложнениях это приведет к худшему пороговому значению для квантовых вычислений. В третьих, наши устойчивые к ошибкам процедуры измерения и $\pi/8$ -элементы используют вспомогательные кубиты в состоянии $|0\rangle$ (в которых возможен небольшой шум). Можно показать, что для выполнения пороговой теоремы требуется некоторый постоянный расход таких свежих кубитов. Следовательно, разработчики квантового компьютера должны сделать его архитектуру не только способной к параллельным вычислениям, но и обеспечивающей возможность переводить вспомогательные кубиты в базисные состояния.

Мы рассматривали только основные принципы и не ставили перед собой цели оптимизировать используемые методы. На практике скорее всего будут применяться улучшенные версии наших конструкций. Простое, но важное правило состоит в том, что нужно *правильно выбрать код*. Мы использовали код Стина, так как с ним легко работать и демонстрировать на нем основные принципы. Однако, на практике другие коды могут работать гораздо лучше. Например, в первом уровне каскадного кода может оказаться полезным использовать код, оптимизированный для исправления именно тех типов ошибок, которые встречаются в конкретной физической системе.

Идеи, на которых основана пороговая теорема, могут быть применены множеством различных способов в зависимости от типа шума в конкретной реализации квантового вычисления. Скептики могут сказать, что все такие модели шума, для которых можно доказать пороговую теорему, достаточно ограничены и не реализуются в реальных физических системах. Ответить на это можно только, продемонстрировав в лаборатории длительное устойчивое к ошибкам квантовое вычисление. Основной результат нашего рассмотрения заключается в доказательстве того, что не существует принципиального физического ограничения для изготовления квантового компьютера.

Подведем итоги. В этой главе мы описали основные принципы, в соответствии с которыми может быть надежно обработана квантовая информация на конкретном примере квантового вычисления. Эти принципы применимы и для других систем обработки квантовой информации, таких как квантовые каналы передачи данных, которые могут, например, использоваться для квантовой криптографии. Непрочность квантовой информации во всех известных системах делает неизбежным использование квантового исправления ошибок, однако оно оказывается настолько эффективным, что позволяет проводить надежные квантовые вычисления с помощью подверженных шуму элементов при условии, что вероятность ошибки в них меньше определенного порогового уровня.

Задача 10.1. Каналы \mathcal{E}_1 и \mathcal{E}_2 называются *эквивалентными*, если существуют унитарные каналы \mathcal{U} и \mathcal{V} , такие, что $\mathcal{E}_2 = \mathcal{U} \circ \mathcal{E}_1 \circ \mathcal{V}$.

- (1) Покажите, что отношение эквивалентности для каналов является отношением эквивалентности.

- (2) Покажите, как преобразовать код, исправляющий ошибки в канале \mathcal{E}_1 , в код, исправляющий ошибки в канале \mathcal{E}_2 . Считайте, что процедура исправления ошибок для канала \mathcal{E}_1 состоит из проективного измерения и условного унитарного преобразования. Покажите, как таким же образом выполнить процедуру исправления ошибок для \mathcal{E}_2 .

Задача 10.2 (граница Варшамова–Гильберта). Докажите границу Варшамова–Гильберта для CSS кодов, т. е. покажите, что существует CSS $[n, k]$ -код, способный исправить t ошибок, для которого

$$\frac{k}{n} \geq 1 - 2H\left(\frac{2t}{n}\right). \quad (10.122)$$

Можете также попробовать доказать границу Варшамова–Гильберта для произвольного симплектического кода, т. е. доказать, что существует симплектический $[n, k]$ -код, способный исправить t ошибок, для которого

$$\frac{k}{n} \geq 1 - \frac{2 \log(3)t}{n} - 2H\left(\frac{2t}{n}\right). \quad (10.123)$$

Задача 10.3 (кодирование симплектического кода). Пусть образующие кода имеют стандартную форму и закодированные операторы Z и X также построены в стандартной форме. Постройте цепь, преобразующую проверочную матрицу $n \times 2n$, соответствующую списку всех образующих кода с закодированными операторами Z , вида

$$G = \left[\begin{array}{ccc|ccc} 0 & 0 & 0 & I & 0 & 0 \\ 0 & 0 & 0 & 0 & I & 0 \\ 0 & 0 & 0 & 0 & 0 & I \end{array} \right] \quad (10.124)$$

в стандартную форму

$$G = \left[\begin{array}{ccc|ccc} I & A_1 & A_2 & B & 0 & C_2 \\ 0 & 0 & 0 & D & I & E \\ 0 & 0 & 0 & A_2^T & 0 & I \end{array} \right]. \quad (10.125)$$

Задача 10.4 (кодирование с помощью телепортации). Пусть нужно закодировать симплектическим кодом кубит в неизвестном состоянии $|\psi\rangle$. Постройте схему для этого следующим образом.

- (1) Объясните, как построить устойчивым к ошибкам способом частично закодированное состояние

$$\frac{|0\rangle|0_L\rangle + |1\rangle|1_L\rangle}{\sqrt{2}}, \quad (10.126)$$

записав его как стабилизированное состояние, с тем, чтобы его можно было приготовить путем измерения образующих стабилизатора.

- (2) Покажите, как можно выполнить устойчивое к ошибкам измерение в базисе Белла над состоянием $|\psi\rangle$ и незакодированным кубитом из состояния (10.126).
- (3) С помощью операторов Паули исправьте полученный после измерения закодированный кубит, так чтобы его состояние стало $|\psi\rangle$, как в обычной квантовой схеме для телепортации.

Вычислите вероятность ошибки в такой схеме. Покажите, как нужно изменить схему, чтобы она выполняла устойчивое к ошибкам декодирование.

Задача 10.5. Пусть $C(S)$ — симплектический $[n, 1]$ -код, способный исправить ошибку в одном кубите. Объясните, как может быть реализован устойчивый к ошибкам элемент CNOT, действующий на два логических кубита, закодированных этим кодом, с использованием только устойчивых к ошибкам процедур приготовления стабилизированных состояний, измерения элементов стабилизатора, а также образующих нормали заторы, применяемых побитово.

Краткое содержание главы

- **Квантовый код, исправляющий ошибки.** Квантовый $[n, k, d]$ -код кодирует k кубитов n кубитами с расстоянием d .
- **Условие квантового исправления ошибок.** Пусть C — квантовый код, исправляющий ошибки, а P — проектор на пространство кода C . Код может исправлять множество ошибок $\{E_i\}$ тогда и только тогда, когда

$$PE_i^\dagger E_j P = \alpha_{ij} P, \quad (10.127)$$

для некоторой эрмитовой матрицы α .

- **Симплектические коды.** Пусть S — стабилизатор симплектического кода $C(S)$, а $\{E_j\}$ — набор ошибок из группы Паули, такой, что $E_j^\dagger E_k \notin N(S) - S$ для всех j и k . Тогда $\{E_j\}$ — исправляемый набор ошибок для кода $C(S)$.
- **Устойчивое к ошибкам квантовое вычисление.** Универсальный набор логических операций над *закодированными* состояниями может быть выполнен так, что эффективная вероятность ошибки в закодированном состоянии равна $O(p^2)$, где p — вероятность ошибки в каждом элементе.

- **Пороговая теорема.** Если шум в каждом квантовом элементе меньше некоторого порогового значения и удовлетворяет физически разумным предположениям, то можно надежно выполнять произвольно длинное квантовое вычисление. Для достижения надежности вычисления требуется только небольшое увеличение размера схемы.

История и дополнительная литература

Существует множество замечательных работ по классической теории информации, в которых рассматриваются коды, исправляющие ошибки. Особенно мы рекомендуем работу Маквилья姆с и Слоуна [296]. Авторы этой работы начинают с элементарных основ, а затем переходят к сложным вопросам, охватывая огромный объем материала. Более современное введение, также очень хорошее, дано в работе Уэлша [414].

Квантовое исправление ошибок было независимо открыто Шором [355], который построил девятикубитовый код, описанный в разд. 10.2, и Стином [371], использовавшим другой подход — изучение интерференционных свойств многочастичных запутанных состояний. Условия квантового исправления ошибок были независимо доказаны Беннетом, Дивинченцо, Смолиным и Вутерсом [42], а также Ниллом и Лафламом [216]. Основой послужила более ранняя работа Экерта и Макчиавелло [142]. Пятикубитовый код был предложен Беннетом, Дивинченцо, Смолиным и Вутерсом [42] и независимо Лафламом, Микелем, Пазом и Зуреком [257].

Кальдербанк и Шор [104], а также Стин [372], используя идеи классического исправления ошибок, построили CSS коды (коды Кальдербанка–Шора–Стина). Кальдербанк и Шор также сформулировали и доказали границу Варшамова–Гильберта для CSS кодов. Готтесман [165] ввел формализм стабилизаторов, использовал его для построения симплектических кодов и изучил некоторые их свойства. Независимо Кальдербанка, Раинса, Шора и Слоун [102] предложили эквивалентный подход к квантовому исправлению ошибок, основанный на классической теории кодов. Им удалось классифицировать почти все квантовые коды [103], а также доказать границу Варшамова–Гильберта для произвольного симплектического кода, которая была введена Экертом и Макчиавелло [142]. Теорема Готтесмана–Нилла впервые по-видимому была сформулирована Готтесманом в работе [166], где он приписывает этот результат Ниллу, вместе с доказательством, на основе формализма стабилизаторов, который ввел Готтесман. Готтесман очень успешно применял формализм стабилизаторов для решения большого числа задач. В работе [166] приводится пример и даются ссылки на литературу. Наше рассмотрение формализма стабилизаторов основано главным образом на работе [166], где можно найти большинство описанных здесь результатов, включая утверждение о том, что элемент Адамара, фазовый элемент и CNOT являются образующими нормализатора $N(G_n)$.

Известно много построений конкретных классов квантовых кодов; мы отметим здесь только некоторые из них. Райнс, Хардин, Шор и Слоун [339] построили интересный класс кодов, не являющихся симплектическими. Многие рассматривали квантовые коды для систем, отличных от кубитов. Следует особо отметить работы Готтесмана [167] и Райнса [335], которые построили недвоичные коды и рассмотрели устойчивые к ошибкам вычисления для них. Ааронова и Бен-Ор [2] построили недвоичные коды с использованием интересного метода, основанного на полиномах над конечными полями, и также рассмотрели устойчивые к ошибкам вычисления для таких кодов. Еще одна тема, которой мы не касались — *приближенное* квантовое исправление ошибок. Как показали Леунг, Нильсен, Чанг и Ямamoto [258], такое исправление ошибок может привести к улучшению квантовых кодов.

Большой и интересный класс квантовых кодов, исправляющих ошибки (не описанный в этой главе) — так называемые *бесшумные квантовые коды*, или *подпространства* без потери когерентности. Этой теме посвящено большое количество работ: для начала можно порекомендовать работы Занарди и Расетти [436, 431], Лидара, Чанга и Уэйли [238], Бэкона, Кемпа, Лидара и Уэйли [59, 236], Нилла, Лафлама и Виолы [219].

Известно множество неравенств для квантовых кодов, исправляющих ошибки. Часть из них получена из аналогичных классических неравенств. Экерт и Макчиавелло [142] указали на возможность доказательства квантового аналога границы Хэмминга. Эта конструкция и роль вырожденных квантовых кодов были последовательно объяснены Готтесманом [165]. Шор и Лафлам [361] доказали квантовый аналог классических тождеств Маквилльяма. Более общий подход к этим вопросам описан в работах [17], [13], [333, 336, 334].

Теория устойчивого к ошибкам вычисления для классических компьютеров разработана фон Нейманом [404] и обсуждается в монографии Винограда и Коуэна [412]. Шор [356] ввел понятие устойчивости к ошибкам для квантового вычисления и привел устойчивые к ошибкам схемы для всех основных этапов вычисления (приготовление состояний, квантовая логика, исправление ошибок и измерения). Китаев [213, 214] независимо разработал много аналогичных идей, включая устойчивые к ошибкам конструкции для многих основных квантовых логических элементов. Сирак, Пеллицари и Цоллер [101], а также Зурек и Лафлан [434] тоже сделали несколько шагов к устойчивым к ошибкам вычислениям. Дивинченцо и Шор показали, как можно выполнить устойчивое к ошибкам измерение синдрома для любого симплектического кода [132]. Готтесман [168], обобщив устойчивые к ошибкам конструкции, показал, как можно выполнять устойчивое к ошибкам вычисление для любого симплектического кода. С общим обзором этой работы и другими материалами, включая конструкцию для решения задачи 10.5, можно познакомиться в [166]. Устойчивые к ошибкам схемы для элементов Тоффоли и $\pi/8$ основаны на идеях, разработанных Готтесманом и Чангом [161], а также Жу и Чангом [435]. Схема для устойчивого к ошибкам элемента Тоффоли из упражнения 10.68 разработана Шором [356]. Стин [374] создал много оригинальных конструкций для процедур, устойчивых к ошибкам.

Китаев [212, 213] предложил множество замечательных идей о том, как получить устойчивость к ошибкам с использованием топологических методов. Основная идея заключается в том, чтобы хранить информацию в топологии системы. Такая информация очень устойчива к шуму. Эти и многие другие красивые идеи были в дальнейшем развиты Бравым и Китаевым [57], а также Фридманом и Майером [153]. Прескилл [327] сделал очень хороший обзор по теме квантового исправления ошибок в целом, который включает замечательное описание топологического исправления ошибок, а также интригующие рассуждение о его связи с фундаментальными вопросами черных дыр и квантовой гравитации.

Многие группы установили различные пороговые значения для квантовых вычислений. Эти результаты получены при различных предположениях и приводят к существенно разным пороговым теоремам. Пороговые теоремы Аароновой и Бен-Ора [1, 2], а также Китаева [214, 213] не требуют быстрых или надежных классических вычислений. Ааронова и Бен-Ор также показали, что для выполнения пороговой теоремы в каждый момент времени необходимо проведение параллельных вычислений [1]. При доказательстве пороговой теоремы Готтесман [166] и Прескилл [330, 169] провели детальную оптимизацию пороговой величины. Нилл, Лафлам и Зурек [220, 221] доказали пороговую теорему для широкого класса моделей ошибки. Ааронова, Бен-Ор, Импальяццо и Нисан [3] также показали, что для выполнения пороговой теоремы необходим постоянный расход свежих кубитов. Дальнейшие ссылки и исторические материалы могут быть найдены в перечисленных работах. В частности, каждая группа ссылается на работу Шора [356] об устойчивых к ошибкам квантовых вычислениях.

Существует множество отличных обзоров квантовых вычислений, устойчивых к ошибкам, в которых основные идеи описываются гораздо более детально, чем мы, и с различных точек зрения. В диссертация Аароновой [8] рассматриваются пороговая теорема и связанные с ней вопросы. Диссертация Готтесмана [166] также содержит обзор устойчивых к ошибкам квантовых вычислений, причем особое внимание уделяется свойствам квантовых кодов и построению устойчивых к ошибкам конструкций для множества различных кодов. Нилл, Лафлам и Зурек сделали популярный обзор, посвященный пороговой теореме [220]. Прескилл написал две замечательные статьи [330, 328] о квантовом исправлении ошибок и об устойчивых к ошибкам квантовых вычислениях.

Глава 11

ЭНТРОПИЯ И ИНФОРМАЦИЯ

Энтропия является ключевым понятием в квантовой теории информации, которое позволяет определить степень неопределенности в состоянии физической системы. В настоящей главе мы рассмотрим основные определения и свойства энтропии в классической и квантовой теории информации. В главе встречаются разделы, содержащие подробные и довольно длинные математические доказательства. При первом чтении через эти разделы можно перескочить, возвращаясь к ним по мере необходимости.

11.1 Шенноновская энтропия

Важнейшим понятием классической теории информации является *шенноновская энтропия*. Предположим, что нам стало известно значение случайной величины X . Шенноновская энтропия H является мерой количества информации, которое мы получаем, узнав значение X . Можно также сказать, что энтропия H является мерой *неопределенности* величины X до того, как нам стало известно ее значение. Эти две точки зрения дополняют друг друга; мы можем рассматривать энтропию как меру неопределенности *до* того как мы узнали значение X , или как меру количества информации, которое мы получим *после* того, как узнаем значение X .

Интуитивно ясно, что энтропия случайной величины не должна зависеть от того, какие символы мы используем для описания множества значений, принимаемых случайной величиной. Например, ясно, что случайная величина, принимающая значения «орел» и «решка» (монета) с вероятностями $1/4$ и $3/4$, содержит то же самое количество информации, что и случайная величина принимающая значения 0 и 1 с вероятностями $1/4$ и $3/4$. По этой причине, энтропия случайной величины определяется как функция от вероятностей ее возможных значений и не зависит от выбора символов для описания этих значений. Часто мы записываем энтропию как функцию распределения вероятностей p_1, \dots, p_n . *Шенноновская энтропия* этого распределения вероятностей определяется как

$$H(X) \equiv H(p_1, \dots, p_n) \equiv - \sum_x p_x \log p_x \quad (11.1)$$

Заметим, что в этом определении (также как и во всей книге) логарифм « \log » берется по основанию два (тогда как \ln обозначает натуральный логарифм). Этот выбор основания логарифма эквивалентен условию, что энтропия измеря-

ется в «битах». Может возникнуть вопрос, что произойдет при $p_x = 0$, поскольку $\log 0$ неопределен. Интуитивно понятно, что событие, которое никогда не

Вставка 11.1. Соотношение неопределенности с использованием энтропии

Существует изящный способ переформулировать принцип неопределенности квантовой механики с помощью энтропии. Напомним, что соотношение неопределенностей Гайзенберга (вставка 2.4) для стандартных отклонений $\Delta(C)$ и $\Delta(D)$ наблюдаемых C и D имеет вид

$$\Delta(C)\Delta(D) \geq \frac{|\langle\psi|[C, D]|\psi\rangle|}{2}, \quad (11.2)$$

где $|\psi\rangle$ — состояние квантовой системы.

Пусть $C = \sum_c c|c\rangle\langle c|$ и $D = \sum_d d|d\rangle\langle d|$ — спектральные разложения C и D . Определим $f(C, D) \equiv \max_{c,d} |\langle c|d\rangle|$ как максимальную степень совпадения между собственными векторами операторов $|c\rangle$ и $|d\rangle$. Например, для матриц Паули X и Z мы имеем $f(X, Z) = 1/\sqrt{2}$.

Предположим, что квантовая система находится в состоянии $|\psi\rangle$. Пусть $p(c)$ и $p(d)$ — распределения вероятностей результатов измерения C и D , а $H(C)$ и $H(D)$ — их энтропии. Соотношение неопределенности через энтропию имеет вид

$$H(C) + H(D) \geq 2 \log \left(\frac{1}{f(C, D)} \right). \quad (11.3)$$

Доказательство этого результата довольно сложно (см. ссылки в разд. «История и дополнительная литература»), поэтому мы ограничимся доказательством более слабого неравенства

$$H(C) + H(D) \geq -2 \log \frac{1 + f(C, D)}{2}. \quad (11.4)$$

Для доказательства заметим, что

$$H(C) + H(D) = - \sum_{cd} p(c)p(d) \log(p(c)p(d)). \quad (11.5)$$

Оценим сверху величину $p(c)p(d) = |\langle c|\psi\rangle\langle\psi|d\rangle|^2$. Пусть $|\tilde{\psi}\rangle$ — проекция $|\psi\rangle$ на плоскость векторов $|c\rangle$ и $|d\rangle$, $\lambda \leq 1$ — норма вектора $|\psi\rangle$, θ — угол между $|c\rangle$ и $|d\rangle$, а φ — угол между $|\psi\rangle$ и $|d\rangle$, так что $p(c)p(d) = |\langle c|\tilde{\psi}\rangle\langle\tilde{\psi}|d\rangle|^2 = \lambda^2 \cos^2(\theta - \varphi) \cos^2(\varphi)$. Максимум этого выражения $p(c)p(d) = \cos^4(\theta/2)$ достигается при $\lambda = 1$ и $\varphi = \theta/2$, что можно записать в виде

$$p(c)p(d) = \left(\frac{1 + |\langle c|d\rangle|}{2} \right)^2. \quad (11.6)$$

С учетом (11.5) мы получаем

$$H(C) + H(D) \geq -2 \log \frac{1 + f(C, D)}{2}, \quad (11.7)$$

что и требовалось.

происходит, не дает вклада в энтропию, поэтому мы условимся, что $0 \log 0 = 0$. Это равенство можно также получить, заметив, что $\lim_{x \rightarrow 0} x \log x = 0$.

Почему энтропия определяется именно так? В упр. 11.2, предложенном далее в этом разделе, дается интуитивное подтверждение определения энтропии (11.1), основанное на «разумных» аксиомах, постулирующих свойства мер информации. Это интуитивное подтверждение достаточно убедительно, однако определение (11.1) имеет более глубокую мотивацию. Дело в том, что энтропия, определенная таким образом, может быть использована для количественной оценки физических ресурсов, необходимых для хранения информации. Предположим, что имеется некоторый источник (скажем, радиоантенна), который выдает информацию, например, в виде последовательности битов. Если X — случайная величина, можно рассмотреть источник информации, который генерирует последовательность X_1, X_2, \dots независимых одинаково распределенных случайных величин. Хотя реальные источники информации не всегда можно описать таким образом, эта модель часто является хорошим приближением. Шеннон предложил следующую задачу: какие минимальные физические ресурсы необходимы для того, чтобы сохранять информацию, получаемую из такого источника, так, чтобы впоследствии можно было восстановить ее? Оказывается, что для хранения последовательности длины n требуется (в среднем) $nH(X)$ битов, где $H(X) \equiv H(X_1) = H(X_2) = \dots$ — энтропия случайной величины X , входящей в определение источника. Этот результат известен как теорема Шеннона о кодировании для канала без шума. Ее доказательство как для классического, так и для квантового случая приведено в гл. 12.

Проиллюстрируем теорему Шеннона следующим примером. Пусть источник на каждом шаге генерирует один из символов 1, 2, 3 или 4. Если не пытаться сжать данные, можно просто отвести два бита памяти для хранения символа, полученного на каждом шаге. Предположим теперь, что символы 1, 2, 3, 4 генерируются с вероятностями $1/2, 1/4, 1/8, 1/8$ соответственно. Мы можем сжать полученные из источника данные, отводя меньшее число бит для запоминания наиболее часто встречающихся символов и используя большее число бит для запоминания редко встречающихся символов. Один из вариантов сжатия выглядит так: символ 1 кодируется одним битом 0, символ 2 кодируется битами 10, символ 3 кодируется битами 110, символ 4 кодируется битами 111. Если из источника была получена последовательность длины n , то после сжатия будем иметь строку бит средней длины $\frac{n}{2} \cdot 1 + \frac{n}{4} \cdot 2 + \frac{n}{8} \cdot 3 + \frac{n}{8} \cdot 3 = (7/4) \cdot n$. Заметим, что без сжатия мы имели бы строку длины $2n$. Удивительно, что наш вариант сжатия согласуется с энтропией источника

$H(X) = -1/2 \log(1/2) - 1/4 \log(1/4) - 1/8 \log(1/8) - 1/8 \log(1/8) = 7/4!$ Оказывается, что любые попытки дальнейшего сжатия информации, полученной из источника, приведут к тому, что часть информации окажется безвозвратно утерянной, т. е. энтропия определяет оптимальное сжатие, которое может быть достигнуто.

Приведенное выше *функциональное* определение энтропии в терминах сжатия данных является очень характерным для теории информации, как классической так и квантовой. Общее правило состоит в том, что *любую фундаментальную меру информации можно определить как количественную оценку физических ресурсов, необходимых для решения некоторой задачи по обработке данных*.

Упражнение 11.1 (вычисление энтропии). Найдите энтропию, связанную с подбрасыванием (а) «честной» монеты, (б) «честной» игральной кости. Что произойдет с энтропией, если монета или кость «нечестные»?

Упражнение 11.2 (интуитивное подтверждение определения энтропии). Предположим, что мы хотим измерить количество информации, которое получаем, узнав, что в результате некоторого случайного эксперимента произошло событие E . Для этого будем использовать «информационную функцию» $I(E)$, определенную на множестве возможных событий. Сделаем следующие предположения:

1. $I(E)$ зависит только от вероятности события E , так что можно записать $I = I(p)$, где $p \in [0, 1]$ — вероятность.
2. $I(p)$ — гладкая функция.
3. $I(pq) = I(p) + I(q)$, где $p, q > 0$. (Если есть два независимых события, вероятности которых p и q , то информация о том, что произошли оба события, равна сумме количеств информации о том, что произошло каждое из них.)

Покажите что $I(p) = k \log p$, где k — произвольная константа. Если теперь рассмотреть множество взаимно-исключающих событий с вероятностями p_1, \dots, p_n , то средняя информация, которую мы получаем, узнав о том, какое именно из этих событий произошло, равна $k \sum_i p_i \log p_i$. С точностью до постоянного коэффициента оно совпадает с шенноновской энтропией.

11.2 Основные свойства энтропии

11.2.1 Двоичная энтропия

Энтропия случайной величины, принимающей только два различных значения, настолько полезна, что мы дадим ей специальное название *двоичная энтропия* и определим как

$$H_{\text{дв}}(p) \equiv -p \log p - (1-p) \log(1-p), \quad (11.8)$$

где p и $1 - p$ — вероятности двух возможных значений. Если из контекста ясно, что речь идет о двоичной энтропии, мы будем обозначать ее просто $H(p)$. График двоичной энтропии изображен на рис. 11.1. Заметьте, что $H(p) = H(1-p)$, а максимальное значение $H(p)$, равное 1, достигается в точке $p = 1/2$.

На примере двоичной энтропии можно понять многие общие свойства энтропии. Одно из особенно интересных свойств касается поведения энтропии при смешивании двух или более распределений вероятностей. Пусть, например, у Алисы есть две монеты: серебряная и золотая, причем вероятность того, что выпадет «орел» равна p_{Au} для золотой монеты и p_{Ag} для серебряной монеты. Предположим, что Алиса выбирает с вероятностью q серебряную монету и с вероятностью $1 - q$ золотую, после чего подбрасывает монету и сообщает Бобу результаты подбрасывания («орел» или «решка»). Какое количество информации при этом получает Боб? Интуитивно ясно, что оно не может быть меньше, чем среднее от количеств информаций, полученных при подбрасывании каждой из монет. Формально это можно выразить так:

$$H(qp_{Au} + (1 - p)p_{Ag}) \geq qH(p_{Au}) + (1 - q)H(p_{Ag}). \quad (11.9)$$

Как правило, это неравенство является строгим, поскольку Боб получает не только информацию о том, как упала монета («орел» или «решка»), но также некоторую дополнительную информацию, а именно какую монету бросала Алиса. Например, если $p_{Au} = 5/6$, а $p_{Ag} = 1/3$, и Боб узнал, что выпал «орел», то ему естественно предположить, что была брошена золотая монета.

Несложно убедиться, что (11.9) действительно выполняется. Это соотношение является примером более общего свойства **вогнутости**, с которым мы встретимся в гл. 9 при обсуждении различных мер информации. Напомним, что вещественная функция называется вогнутой, если для любого p в интервале от 0 до 1 мы имеем

$$f(px + (1 - p)y) \geq pf(x) + (1 - p)f(y). \quad (11.10)$$

То, что двоичная энтропия является вогнутой функцией, легко увидеть из рис. 11.1; если соединить любые две точки на графике отрезком, то график обязательно пройдет *над* этим отрезком. Мы будем часто использовать свойство вогнутости энтропии, как классической, так и квантовой. Может показаться, что приведенные выше рассуждения слишком тривиальны, чтобы привести к интересным выводам; однако, множество весьма глубоких результатов теории квантовой информации основано на искусном применении свойств вогнутости классической и квантовой энтропии. Более того, в квантовом случае интуиция часто не позволяет понять, какими именно свойствами вогнутости должна обладать энтропия.

Упражнение 11.3. Докажите, что двоичная энтропия $H_{дв}(p)$ принимает максимальное значение при $p = 1/2$.

Упражнение 11.4 (вогнутость двоичной энтропии). Из рис. 11.1 видно, что двоичная энтропия является вогнутой функцией. Докажите, что это действительно так, т. е. что

$$H_{дв}(px_1 + (1-p)x_2) \geq pH_{дв}(x_1) + (1-p)H_{дв}(x_2), \quad (11.11)$$

где $0 \leq p, x_1, x_2 \leq 1$. Докажите также, что двоичная энтропия *строго вогнутая* функция, т. е. что (11.11) превращается в равенство только в тривиальных случаях $x_1 = x_2, p = 0, p = 1$.

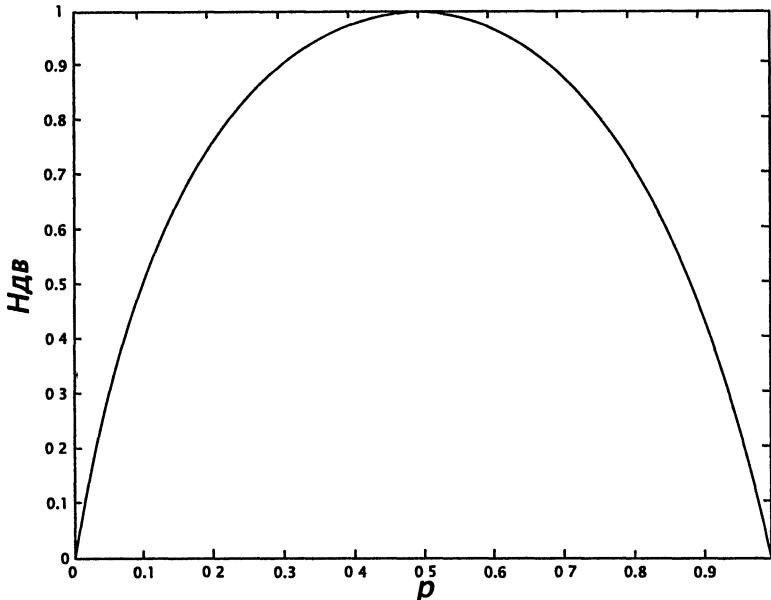


Рис. 11.1. График двоичной энтропии $H(p)$

11.2.2 Относительная энтропия

Существует очень полезный аналог энтропии, который является мерой различия двух распределений вероятностей одной и той-же переменной x . Это — *относительная энтропия*. Пусть имеются два распределения вероятностей $p(x)$ и $q(x)$ переменной x . Определим *относительную энтропию* $p(x)$ по отношению к $q(x)$ как

$$H(p(x)||q(x)) \equiv \sum_x p(x) \log \frac{p(x)}{q(x)} \equiv -H(X) - \sum_x p(x) \log q(x). \quad (11.12)$$

Имеется в виду что $-0 \log 0 \equiv 0$ при $p(x) > 0$ и $-p(x) \log 0 = \infty$.

В чем состоит полезность относительной энтропии и почему она является хорошей мерой различия двух распределений? Приведенная ниже теорема позволяет понять, почему выражение (11.12) можно рассматривать как меру различия.

Теорема 11.1 (неотрицательность относительной энтропии). Относительная энтропия неотрицательна, $H(p(x)||q(x)) \geq 0$, причем равенство имеет место тогда и только тогда, когда $p(x) = q(x)$ для всех x .

Доказательство.

В теории квантовой информации часто применяется неравенство $\log x \ln 2 = \ln x \leqslant x - 1$, $x > 0$. Оно превращается в равенство тогда и только тогда, когда $x = 1$. Перепишем его в виде $-\log x \geqslant (1-x)/\ln 2$ и заметим, что

$$H(p(x)||q(x)) = -\sum_x p(x) \log \frac{q(x)}{p(x)} \quad (11.13)$$

$$\geqslant \frac{1}{\ln 2} \sum_x p(x) \left(1 - \frac{q(x)}{p(x)}\right) \quad (11.14)$$

$$= \frac{1}{\ln 2} \sum_x (p(x) - q(x)) \quad (11.15)$$

$$= \frac{1}{\ln 2} (1-1) = 0. \quad (11.16)$$

Равенство в (11.14) имеет место тогда и только тогда, когда $q(x)/p(x) = 1$ для всех x , т. е. когда два распределения совпадают. ■

Полезность относительной энтропии связана еще с тем, что многие другие энтропийные величины можно рассматривать как частные случаи относительной энтропии, а ее свойства можно использовать для нахождения свойств других энтропийных величин. Например, неотрицательность относительной энтропии можно использовать для доказательства следующего фундаментального факта. Пусть $p(x)$ — распределение вероятностей случайной величины X , которая принимает d различных значений. Обозначим через $q(x) \equiv 1/d$ равномерное распределение вероятностей той же величины X . Тогда

$$H(p(x)||q(x)) = H(p(x)||1/d) = -H(X) - \sum_x p(x) \log \frac{1}{d} = \log d - H(X). \quad (11.17)$$

Применяя теорему 11.1, получаем $\log d - H(X) \geqslant 0$, причем равенство имеет место тогда и только тогда, когда X — равномерно распределенная случайная величина. Хотя этот факт и элементарен, он весьма важен и мы сформулируем его в виде теоремы.

Теорема 11.2. Пусть X — случайная величина, принимающая d различных значений. Тогда $H(X) \leqslant \log d$, причем равенство имеет место тогда и только тогда, когда X — равномерно распределенная случайная величина.

При изучении классической и квантовой энтропии мы часто будем выражать интересующие нас энтропийные величины через относительную энтропию.

Упражнение 11.5 (субаддитивность шенноновской энтропии). Докажите, что $H(p(x,y)||p(x)p(y)) = H(p(x)) + H(p(y)) - H(p(x,y))$. Используя этот результат, покажите, что $H(X,Y) \leqslant H(X) + H(Y)$, где равенство имеет место тогда и только тогда, когда X и Y — независимые случайные величины.

11.2.3 Условная энтропия и взаимная информация

Пусть X и Y — две случайные величины. Как связано количество информации, содержащееся в X , с количеством информации, содержащимся в Y ? В этом разделе мы введем два понятия — *условную энтропию* и *взаимную информацию*, которые помогут ответить на этот вопрос. Их определения выглядят достаточно формально, а интерпретация не всегда очевидна. Заметим, что основная мотивация этих определений состоит в том, что указанные величины позволяют рассматривать вопрос о потребляемых ресурсах, который более подробно обсуждается в гл. 12, а их интерпретация зависит от рассматриваемого ресурса.

Мы уже использовали *совместную энтропию* пары случайных величин в предыдущем разделе. Нам будет удобно дать ее явное определение. *Совместная энтропия* величин X и Y определяется как

$$H(X, Y) \equiv - \sum_{x,y} p(x, y) \log p(x, y). \quad (11.18)$$

Это определение можно естественным образом обобщить на любое число случайных величин. Совместная энтропия является мерой полной неопределенности относительно пары величин (X, Y) . Предположим, что мы узнали значение Y . Это значит, что мы приобрели $H(Y)$ бит информации о паре (X, Y) . При этом все равно остается некоторая неопределенность относительно пары (X, Y) , поскольку мы не знаем значение X . *Энтропия X при условии, что значение Y известно*, определяется как

$$H(X|Y) \equiv H(X, Y) - H(Y). \quad (11.19)$$

Условная энтропия является мерой неопределенности X при известном значении Y .

Взаимная информация между X и Y измеряет количество информации, которое является общим для X и Y . Давайте сложим количество информации, содержащееся в X , $H(X)$, и количество информации, содержащееся в Y . Та информация, которая является общей для X и Y , будет при этом учтена дважды, а информация содержащаяся только в X или только в Y , — лишь один раз. Поэтому, вычитая из полученной суммы совместную энтропию пары (X, Y) , $H(X, Y)$, получим общую, или *взаимную информацию* X и Y :

$$H(X:Y) \equiv H(X) + H(Y) - H(X, Y). \quad (11.20)$$

Отметим полезное равенство $H(X:Y) = H(X) - H(X|Y)$, связывающее условную энтропию с взаимной информацией.

Чтобы получить представление о том, как ведет себя шенноновская энтропия, мы приводим ниже некоторые простые соотношения между различными энтропиями.

Теорема 11.3 (основные свойства шенноновской энтропии).

- (1) $H(X, Y) = H(Y, X)$, $H(X:Y) = H(Y:X)$.
- (2) $H(Y|X) \geq 0$ и, таким образом, $H(X:Y) \leq H(Y)$, причем равенство имеет место тогда и только тогда, когда Y является функцией от X , $Y = f(X)$.
- (3) $H(X) \leq H(X, Y)$, причем равенство имеет место тогда и только тогда, когда Y является функцией от X .
- (4) **Субаддитивность.** $H(X, Y) \leq H(X) + H(Y)$, причем равенство имеет место тогда и только тогда, когда X и Y являются независимыми случайными величинами.
- (5) $H(Y|X) \leq H(Y)$ и, таким образом, $H(X:Y) \geq 0$, причем равенство имеет место тогда и только тогда, когда X и Y являются независимыми случайными величинами.
- (6) **Сильная субаддитивность.** $H(X, Y, Z) + H(Y) \leq H(X, Y) + H(Y, Z)$, причем равенство имеет место тогда и только тогда, когда $Z \rightarrow Y \rightarrow X$ является марковской цепью.
- (7) **Введение дополнительных условий уменьшает энтропию.** $H(X|Y, Z) \leq H(X|Y)$.

Многие из этих утверждений являются либо очевидными, либо доказываются элементарно, поэтому мы приведем лишь некоторые соображения.

Доказательство.

- (1) Очевидно из определений.
- (2) Поскольку $p(x, y) = p(x)p(y|x)$, можно записать

$$H(X, Y) = - \sum_{xy} p(x, y) \log p(x)p(y|x) \quad (11.21)$$

$$= - \sum_x p(x) \log p(x) - \sum_{xy} p(x, y) \log p(y|x) \quad (11.22)$$

$$= H(X) - \sum_{xy} p(x, y) \log p(y|x) \quad (11.23)$$

Таким образом, $H(Y|X) = - \sum_{xy} p(x, y) \log p(y|x)$. Поскольку $-\log p(y|x) \geq 0$, то $H(Y|X) \geq 0$. Равенство здесь имеет место тогда и только тогда, когда Y является однозначной функцией X .

- (3) Следует из (2).
- (4) Для доказательства субаддитивности можно опять использовать тот факт, что $\log x \leq (x-1)/\ln 2$, $x > 0$, где равенство имеет место тогда и только тогда, когда $x = 1$. Мы находим, что

$$\sum_{x,y} p(x, y) \log \frac{p(x)p(y)}{p(x, y)} \leq \frac{1}{\ln 2} \sum_{x,y} p(x, y) \left(\frac{p(x)p(y)}{p(x, y)} - 1 \right) \quad (11.24)$$

$$= \frac{1}{\ln 2} \sum_{x,y} (p(x)p(y) - p(x, y)) = \frac{1-1}{\ln 2} = 0. \quad (11.25)$$

Субаддитивность доказана. Равенство достигается тогда и только тогда, когда

$p(x,y) = p(x)p(y)$ для всех x и y . Таким образом, неравенство субаддитивности превращается в равенство тогда и только тогда, когда X и Y независимые величины.

(5) Следует из (4) и (1).

(6) Сильная субаддитивность шенноновской энтропии доказывается аналогично обычной субаддитивности, хотя ее доказательство несколько сложнее. Мы предлагаем его в качестве упражнения (упр. 11.6).

(7) Интуитивно ясно, что неопределенность X при известных значениях Y и Z меньше чем неопределенность X при известном Y . Для формального доказательства, нужно взять определения входящих в неравенство величин (1) и переписать его в виде

$$H(X,Y,Z) - H(Y,Z) \leq H(X,Y) - H(Y). \quad (11.26)$$

Это не что иное, как неравенство сильной субаддитивности, с точностью до перестановки слагаемых. ■

Упражнение 11.6 (доказательство классической сильной субаддитивности). Докажите что $H(X,Y,Z) + H(Y) \leq H(X,Y) + H(Y,Z)$, причем равенство имеет место тогда и только тогда, когда $Z \rightarrow Y \rightarrow X$ является марковской цепью.

Упражнение 11.7. Из упр. 11.5 следует, что взаимную информацию $H(X:Y)$ можно рассматривать как относительную энтропию двух распределений вероятностей, $H(X:Y) = H(p(x,y)||p(x)p(y))$. Представьте условную энтропию $H(Y|X)$ как относительную энтропию для двух распределений вероятностей. Используя полученное выражение, докажите, что $H(Y|X) \geq 0$, и определите условия, при которых имеет место равенство.

Различные соотношения между энтропиями удобно представить графически при помощи диаграммы Венна для энтропии (рис. 11.2). К этой диаграмме следует относиться лишь как к мнемоническому правилу для запоминания различных определений и свойств энтропии.

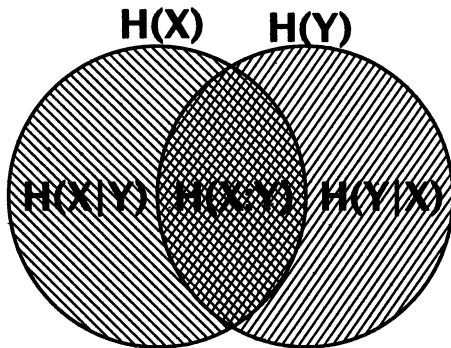


Рис. 11.2. Соотношения между различными энтропиями.

Прежде чем завершить изучение основных свойств условной энтропии и взаимной информации, рассмотрим цепное правило для условных энтропий.

Теорема 11.4 (цепное правило для условных энтропий). Пусть X_1, \dots, X_n и Y — произвольные случайные величины. Тогда

$$H(X_1, \dots, X_n | Y) = \sum_{i=1}^n H(X_i | Y, X_1, \dots, X_{i-1}). \quad (11.27)$$

Доказательство.

Рассмотрим сначала случай $n = 2$, а затем применим индукцию по n . Используя определение условной энтропии, можно сделать следующие преобразования:

$$H(X_1, X_2 | Y) = H(X_1, X_2, Y) - H(Y) \quad (11.28)$$

$$= H(X_1, X_2, Y) - H(X_1, Y) + H(X_1, Y) - H(Y) \quad (11.29)$$

$$= H(X_2 | Y, X_1) + H(X_1 | Y), \quad (11.30)$$

что доказывает цепное правило для $n = 2$. Предположим, что для некоторого n правило доказано и докажем его для $n+1$. Используя полученный результат для $n = 2$, находим

$$H(X_1, \dots, X_{n+1} | Y) = H(X_2, \dots, X_{n+1} | Y, X_1) + H(X_1 | Y). \quad (11.31)$$

Перепишем первый член справа, используя предположение индукции

$$H(X_1, \dots, X_{n+1} | Y) = \sum_{i=2}^{n+1} H(X_i | Y, X_1, \dots, X_{i-1}) + H(X_1 | Y) \quad (11.32)$$

$$= \sum_{i=1}^{n+1} H(X_i | Y, X_1, \dots, X_{i-1}), \quad (11.33)$$

что доказывает цепное правило для $n+1$. ■

Упражнение 11.8 (взаимная информация не является субаддитивной). Допустим, что X и Y — независимые случайные величины, принимающие значения 0 и 1 с вероятностью $1/2$. Пусть $Z = X \oplus Y$, где операция \oplus — сложение по модулю два. Покажите, что в этом случае взаимная информация не является субаддитивной, т. е., что

$$H(X, Y : Z) \not\leq H(X : Z) + H(Y : Z). \quad (11.34)$$

Упражнение 11.9 (взаимная информация не является супераддитивной). Рассмотрим случайные величины $X_1 \equiv X_2 \equiv Y_1 \equiv Y_2$, принимающие значения 0 и 1 с вероятностью $1/2$. Покажите что в этом случае взаимная информация не является супераддитивной, т. е., что

$$H(X_1 : Y_1) + H(X_2 : Y_2) \not\leq H(X_1, X_2 : Y_1, Y_2). \quad (11.35)$$

11.2.4 Неравенство обработки данных

Во многих приложениях информация, которую мы должны обрабатывать, уже была подвергнута воздействию каких-либо шумов и, таким образом, дошла до нас в искаженном виде. В теории информации существует важное неравенство — *неравенство обработки данных*, которое выражает тот факт, что информация, полученная из источника, с течением времени может только уменьшаться; потеря информации является необратимым процессом. В этом разделе мы придадим этому утверждению более точную форму.

Интуитивное понятие *обработки данных* можно формализовать при помощи *марковских цепей* случайных величин. Марковская цепь представляет собой последовательность случайных величин $X_1 \rightarrow X_2 \rightarrow \dots$, такую, что X_{n+1} не зависит от X_1, \dots, X_{n-1} при условии, что величина X_n фиксирована. Можно записать

$$p(X_{n+1} = x_{n+1} | X_n = x_n, \dots, X_1 = x_1) = p(X_{n+1} = x_{n+1} | X_n = x_n). \quad (11.36)$$

При каких условиях в марковской цепи происходит потеря информации, имевшейся в начальный момент? *Неравенство обработки данных* позволяет ответить на этот вопрос в терминах квантовой теории информации.

Теорема 11.5 (неравенство обработки данных). Пусть $X \rightarrow Y \rightarrow Z$ — марковская цепь. Тогда

$$H(X) \geq H(X:Y) \geq H(X : Z). \quad (11.37)$$

При этом $H(X) = H(X:Y)$ тогда и только тогда, когда по значению Y можно восстановить значение X .

Этот результат интуитивно выглядит правдоподобно. Фактически утверждается, что если случайная величина X под воздействием шума перешла в Y , а затем величина Y поступила на вход некоторого обрабатывающего данные устройства со случайной величиной Z на выходе, взаимная информация между Z и X будет всегда меньше, чем взаимная информация между Y и X .

Доказательство.

Первое неравенство в (11.37) уже было доказано в теореме 11.3. Используя определения взаимной информации и условной энтропии, мы замечаем, что $H(X:Z) \leq H(X:Y)$ эквивалентно $H(X|Y) \leq H(X|Z)$. Из того, что $X \rightarrow Y \rightarrow Z$ является марковской цепью, следует (упр. 11.10), что $Z \rightarrow Y \rightarrow X$ также является марковской цепью и, таким образом, $H(X|Y) = H(X|Y, Z)$. Поэтому достаточно доказать, что $H(X, Y, Z) - H(Y, Z) = H(X|Y, Z) \leq H(X|Z) = H(X, Z) - H(Z)$. Это не что иное, как неравенство сильной субаддитивности, доказанное ранее.

Предположим, что $H(X:Y) < H(X)$. Тогда по значению Y восстановить X невозможно. Действительно, если в результате восстановления мы получили случайную величину Z , то поскольку $X \rightarrow Y \rightarrow Z$ является марковской цепью, из неравенства обработки данных следует, что $H(X) > H(X:Z)$. Но это значит, что $Z \neq X$. Если же $H(X:Y) = H(X)$, то $H(X|Y) = 0$. Из теоремы 11.3,

часть (2), следует что X является функцией от Y , так что, зная Y , мы можем восстановить X . ■

Как мы отмечали выше, если $X \rightarrow Y \rightarrow Z$ — марковская цепь, то $Z \rightarrow Y \rightarrow X$ также марковская цепь. Поэтому как следствие неравенства обработки данных мы получаем для марковской цепи $X \rightarrow Y \rightarrow Z$ неравенство

$$H(Z : Y) \geq H(Z : X). \quad (11.38)$$

Будем называть этот результат *неравенством передачи данных*. На интуитивном уровне оно достаточно понятно: информация, являющаяся общей для Z и X , является также общей для Z и Y , поскольку вся информация от X к Z проходит через Y .

Упражнение 11.10. Покажите, что если $X \rightarrow Y \rightarrow Z$ является марковской цепью, то $Z \rightarrow Y \rightarrow X$ также является марковской цепью.

11.3 Энтропия фон Неймана

Шенноновская энтропия является мерой неопределенности, связанной с классическим распределением вероятностей. При переходе к квантовым состояниям мы должны заменить распределения вероятностей на матрицы плотности. В настоящем разделе определение шенноновской энтропии будет обобщено на квантовые состояния.

Фон Нейман определил *энтропию* квантового состояния ρ следующей формулой:

$$S(\rho) \equiv -\text{tr}(\rho \log \rho). \quad (11.39)$$

Здесь логарифм, как обычно, берется по основанию два. Если λ_x — собственные значения ρ , то определение фон Неймана можно переписать в виде

$$S(\rho) = - \sum_x \lambda_x \log \lambda_x, \quad (11.40)$$

где мы считаем $0 \log 0 \equiv 0$, как и в случае шенноновской энтропии. Последняя формула более удобна для вычислений. Например, однородное смешанное состояние I/d в d -мерном пространстве имеет энтропию $\log d$.

В дальнейшем из контекста всегда будет ясно, когда речь идет о шенноновской энтропии, а когда об энтропии фон Неймана.

Упражнение 11.11 (примеры вычисления энтропии). Вычислите $S(\rho)$ для

$$\rho = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad (11.41)$$

$$\rho = \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \quad (11.42)$$

$$\rho = \frac{1}{3} \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}. \quad (11.43)$$

Упражнение 11.12 (сравнение квантовой энтропии и классической энтропии). Пусть $\rho = p|0\rangle\langle 0| + (1-p)\frac{(|0\rangle+|1\rangle)(\langle 0|+\langle 1|)}{2}$. Вычислите $S(\rho)$ и сравните результат с $H(p, 1-p)$.

11.3.1 Квантовая относительная энтропия

Как и для шенноновской энтропии, в квантовом случае очень важно определить относительную энтропию. Пусть ρ и σ — матрицы плотности. *Относительная энтропия* ρ по отношению к σ определяется как

$$S(\rho||\sigma) \equiv \text{tr}(\rho \log \rho) - \text{tr}(\rho \log \sigma). \quad (11.44)$$

Как и в классическом случае, квантовая относительная энтропия иногда может быть бесконечной. В частности, она равна $+\infty$, если ядро σ (пространство, порожденное собственными векторами σ с нулевыми собственными значениями) имеет ненулевое пересечение с носителем ρ (пространство, порожденное собственными векторами ρ с ненулевыми собственными значениями), и принимает конечное значение во всех остальных случаях. Квантовая относительная энтропия неотрицательна, этот результат иногда называют *неравенством Клейна*.

Теорема 11.6 (неравенство Клейна). Квантовая относительная энтропия неотрицательна:

$$S(\rho||\sigma) \geq 0, \quad (11.45)$$

причем равенство имеет место тогда и только тогда, когда $\rho = \sigma$.

Вставка 11.2. Непрерывность энтропии

Как изменяется $S(\rho)$, если изменение состояния ρ достаточно мало? *Неравенство Фанне* показывает, что изменение $S(\rho)$ «небольшое» и дает нам оценку этого изменения.

Теорема 11.7 (неравенство Фанне). Пусть ρ и σ — матрицы плотности, такие, что для следовой метрики $T(\rho, \sigma)$ удовлетворяет условию $T(\rho, \sigma) \leq 1/e$. Тогда

$$|S(\rho) - S(\sigma)| \leq T(\rho, \sigma) \log d + \eta(T(\rho, \sigma)), \quad (11.46)$$

где d — размерность Гильбертова пространства, а $\eta(x) \equiv -x \log x$. Если опустить ограничение $T(\rho, \sigma) \leq 1/e$, то имеет место более слабое неравенство

$$|S(\rho) - S(\sigma)| \leq T(\rho, \sigma) \log d + \frac{1}{e}. \quad (11.47)$$

Доказательство.

Для доказательства неравенства Фанне нужно связать следовое расстояние между двумя операторами с собственными значениями этих операторов. Пусть $r_1 \geq r_2 \geq \dots \geq r_d$ — собственные значения ρ в порядке убывания, а $s_1 \geq s_2 \geq \dots \geq s_d$ — собственные значения σ в порядке убывания. Спектральное разложение оператора $\rho - \sigma$ позволяет представить его в виде $\rho - \sigma = Q - R$, где Q и R — положительные операторы носители которых ортогональны. Таким образом, $T(\rho, \sigma) = \text{tr}(R) + \text{tr}(Q)$. Если ввести оператор $V \equiv R + \rho = Q + \sigma$, то $T(\rho, \sigma) = \text{tr}(R) + \text{tr}(Q) = \text{tr}(2V) - \text{tr}(\rho) - \text{tr}(\sigma)$. Пусть $t_1 \geq t_2 \geq \dots \geq t_d$ — собственные значения T . Заметим, что $t_i \geq \max(r_i, s_i)$, так что $2t_i \geq r_i + s_i + |r_i - s_i|$. Поэтому имеем

$$T(\rho, \sigma) \geq \sum_i |r_i - s_i|. \quad (11.48)$$

Несложно проверить, что при $|r - s| \leq 1/2$ справедливо неравенство $|\eta(r) - \eta(s)| \leq \eta(|r - s|)$. Поскольку $|r_i - s_i| \leq 1/2$ для всех i , получаем

$$|S(\rho) - S(\sigma)| = \left| \sum_i (\eta(r_i) - \eta(s_i)) \right| \leq \sum_i \eta(|r_i - s_i|). \quad (11.49)$$

Введем обозначение $\Delta \equiv \sum_i |r_i - s_i|$. Поскольку $\eta(|r_i - s_i|) = \Delta \eta(|r_i - s_i|/\Delta) - |r_i - s_i| \log \Delta$, мы видим, что

$$|S(\rho) - S(\sigma)| \leq \Delta \sum_i \eta(|r_i - s_i|/\Delta) + \eta(\Delta) \leq \Delta \log d + \eta(\Delta). \quad (11.50)$$

Второе неравенство получается исходя из теоремы 11.2. Используя монотонность $\eta(\cdot)$ на интервале $[0, 1/e]$ и неравенство $\Delta \leq T(\rho, \sigma)$, см. (11.48), заключаем, что

$$|S(\rho) - S(\sigma)| \leq T(\rho, \sigma) \log d + \eta(T(\rho, \sigma)) \quad (11.51)$$

при $T(\rho, \sigma) \leq 1/e$. Это не что иное как неравенство Фанне. Более слабая форма неравенства Фанне для произвольного $T(\rho, \sigma)$ доказывается аналогично. ■

Доказательство.

Используем разложения ρ и σ в базисе их собственных векторов: $\rho = \sum_i p_i |i\rangle\langle i|$, $\sigma = \sum_j q_j |j\rangle\langle j|$. В соответствии с определением относительной энтропии имеем

$$S(\rho||\sigma) = \sum_i p_i \log p_i - \sum_i \langle i | \rho \log \sigma | i \rangle. \quad (11.52)$$

Учитывая, что $\langle i | \rho = p_i \langle i |$ и

$$\langle i | \log \sigma | i \rangle = \langle i | \left(\sum_j \log(q_j) | j \rangle \langle j | \right) | i \rangle = \sum_j \log(q_j) P_{ij}, \quad (11.53)$$

где $P_{ij} \equiv \langle i | j \rangle \langle j | i \rangle \geq 0$, получаем

$$S(\rho || \sigma) = \sum_i p_i \left(\log p_i - \sum_j P_{ij} \log(q_j) \right). \quad (11.54)$$

Заметим, что P_{ij} обладает следующими свойствами: $P_{ij} \geq 0$, $\sum_i P_{ij} = 1$ и $\sum_j P_{ij} = 1$ (матрица с такими свойствами называется *двойжды стохастической*). Поскольку $\log(\cdot)$ является строго возрастающей функцией, справедливо неравенство $\sum_j P_{ij} \log q_j \leq \log r_i$, где $r_i \equiv \sum_j P_{ij} q_j$, причем равенство имеет место тогда и только тогда, когда существует такое j , для которого $P_{ij} = 1$. Таким образом,

$$S(\rho || \sigma) \geq \sum_i p_i \log \frac{p_i}{r_i} \quad (11.55)$$

причем равенство имеет место тогда и только тогда, когда для каждого i существует такое j , что $P_{ij} = 1$, т. е. если P_{ij} — матрица перестановки. Выражение (11.55) совпадает с классической относительной энтропией. Применяя теорему 11.1 о неотрицательности классической относительной энтропии, получаем

$$S(\rho || \sigma) \geq 0, \quad (11.56)$$

причем равенство имеет место тогда и только тогда, когда $p_i = r_i$ для всех i , а P_{ij} — матрица перестановки. Мы можем перенумеровать собственные состояния σ так чтобы матрица P_{ij} стала единичной. Условие $p_i = r_i$ тогда свидетельствует о том, что ρ и σ диагональны в одном базисе и имеют одинаковые собственные значения, т. е., что $\rho = \sigma$. ■

11.3.2 Основные свойства энтропии

Энтропия фон Неймана имеет много интересных и полезных свойств.

Теорема 11.8 (основные свойства энтропии фон Неймана). (1) Энтропия неотрицательна, причем она обращается в нуль тогда и только тогда, когда состояние чистое.

(2) Если размерность гильбертова пространства равна d , то энтропия не превышает $\log d$. Энтропия равна $\log d$ тогда и только тогда, когда система находится в однородном состоянии I/d .

(3) Пусть составная система AB находится в чистом состоянии. Тогда $S(A) = S(B)$.

(4) Пусть p_i — произвольное распределение вероятностей, а ρ_i — набор состояний, носители которых ортогональны. Тогда

$$S\left(\sum_i p_i \rho_i\right) = H(p_i) + \sum_i p_i S(\rho_i). \quad (11.57)$$

(5) **Теорема о совместной энтропии.** Пусть p_i — произвольное распределение вероятностей, $|i\rangle$ — набор ортогональных состояний для системы A , ρ_i — произвольный набор состояний для другой системы B . Тогда

$$S\left(\sum_i p_i |i\rangle\langle i| \oplus \rho_i\right) = H(p_i) + \sum_i p_i S(\rho_i). \quad (11.58)$$

Доказательство.

- (1) Очевидно из определения.
- (2) Эти утверждения следуют из свойства неотрицательности относительной энтропии, $0 \leq S(\rho||I/d) = -S(\rho) + \log d$.
- (3) Из разложения Шмидта мы знаем, что собственные значения матриц плотности систем A и B совпадают. (Вспомните обсуждение теоремы 2.7.) Поскольку энтропия полностью определяется собственными значениями, то $S(A) = S(B)$.
- (4) Обозначим через λ_i^j и $|e_i^j\rangle$ собственные значения и собственные векторы ρ_i . Заметим, что собственные значения и собственные векторы оператора $\sum_i p_i \rho_i$ имеют вид $p_i \lambda_i^j$ и $|e_i^j\rangle$. Таким образом,

$$S\left(\sum_i p_i \rho_i\right) = -\sum_{ij} p_i \lambda_i^j \log p_i \lambda_i^j \quad (11.59)$$

$$= -\sum_i p_i \log p_i - \sum_i p_i \sum_j \lambda_i^j \log \lambda_i^j \quad (11.60)$$

$$= H(p_i) + \sum_i p_i S(\rho_i), \quad (11.61)$$

что и требовалось.

(5) Следует из (4). ■

Упражнение 11.13 (энтропия тензорного произведения). Используя теорему о совместной энтропии, покажите что $S(\rho \otimes \sigma) = S(\rho) + S(\sigma)$. Докажите эту формулу непосредственно из определения энтропии.

По аналогии с шенноновской энтропией, для составных систем можно определить квантовую совместную энтропию и условную энтропию, а также взаимную информацию. Совместная энтропия для составной системы из двух компонент A и B определяется очевидным образом: $S(A, B) \equiv -\text{tr}(\rho^{AB} \log (\rho^{AB}))$, где ρ^{AB} — матрица плотности системы AB . Условная энтропия и взаимная информация определяются как

$$S(A|B) \equiv S(A, B) - S(B) \quad (11.62)$$

$$S(A : B) \equiv S(A) + S(B) - S(A, B) \quad (11.63)$$

$$= S(A) - S(A|B) = S(B) - S(B|A). \quad (11.64)$$

Некоторые свойства шенноновской энтропии оказываются нарушенными для энтропии фон Неймана, что представляет большой интерес для квантовой теории информации. Например, для любых случайных величин X и Y справедливо неравенство $H(X) \leq H(X, Y)$. Оно совпадает с нашим интуитивным представлением: неопределенность состояния X не может быть больше неопределенности совместного состояния X и Y . Однако в квантовом случае такое интуитивное представление ошибочно. Рассмотрим составную систему из двух кубитов AB , находящуюся в запутанном состоянии $(|00\rangle + |11\rangle)/\sqrt{2}$. Поскольку это состояние чистое, то $S(A, B) = 0$. Однако система A находится в смешанном состоянии $I/2$, энтропия которой равна 1. Другими словами, для данной системы условная энтропия отрицательна, $S(B|A) = S(A, B) - S(A) < 0$.

Упражнение 11.14 (запутанность и отрицательная условная энтропия). Пусть $|AB\rangle$ — чистое состояние составной системы, принадлежащей Алисе и Бобу. Покажите, что $|AB\rangle$ является запутанным состоянием тогда и только тогда, когда $S(B|A) < 0$.

11.3.3 Измерения и энтропия

Попробуем понять, что происходит с энтропией, когда над системой производится измерение. Естественно, что ответ на этот вопрос зависит от того, какого типа измерение выполняется. Однако, существуют и довольно общие закономерности, регламентирующие поведение энтропии при измерениях.

Предположим, например, что над квантовой системой производится проективное измерение с проекторами P_i , причем результат измерения нам не сообщается. Если до измерения система находилась в состоянии ρ , то после измерения она будет в состоянии

$$\rho' = \sum_i P_i \rho P_i. \quad (11.65)$$

Как мы сейчас увидим, в результате этой процедуры энтропия не может уменьшиться. Кроме того, энтропия остается неизменной, если состояние не меняется при измерении.

Теорема 11.9 (проективные измерения увеличивают энтропию). Пусть P_i — полный набор ортогональных проекторов, а ρ — некоторая матрица плотности. Тогда энтропия состояния системы после измерения $\rho' \equiv \sum_i P_i \rho P_i$ не может быть меньше энтропии начального состояния ρ ,

$$S(\rho') \geq S(\rho), \quad (11.66)$$

причем равенство имеет место тогда и только тогда, когда $\rho' = \rho$.

Доказательство.

Доказательство основывается на неравенстве Клейна для ρ и ρ' :

$$0 \leq S(\rho||\rho') = -S(\rho) - \text{tr}(\rho \log \rho'). \quad (11.67)$$

Нам достаточно доказать, что $-\text{tr}(\rho \log \rho') = S(\rho')$. Преобразуем правую часть этого равенства, используя свойство полноты $\sum_i P_i = I$, соотношение $P_i^2 = P_i$ и инвариантность следа относительно циклических перестановок:

$$-\text{tr}(\rho \log \rho') = -\text{tr}\left(\sum_i P_i \rho \log \rho'\right) \quad (11.68)$$

$$= -\text{tr}\left(\sum_i P_i \rho \log \rho' P_i\right). \quad (11.69)$$

Заметим, что $\rho' P_i = P_i \rho P_i = P_i \rho'$. Таким образом, P_i коммутирует с ρ' , а значит, и с $\log \rho'$, так что получаем

$$-\text{tr}(\rho \log \rho') = -\text{tr}\left(\sum_i P_i \rho P_i \log \rho'\right) \quad (11.70)$$

$$= -\text{tr}(\rho' \log \rho') = S(\rho'). \quad (11.71)$$

Теорема доказана. ■

Упражнение 11.15 (обобщенные измерения могут уменьшить энтропию). Рассмотрим обобщенное измерение, описываемое операторами $M_1 = |0\rangle\langle 0|$ и $M_2 = |0\rangle\langle 1|$. Если измерение производится над кубитом в состоянии ρ и результат измерения нам не известен, то после измерения состояние кубита будет $M_1 \rho M_1^\dagger + M_2 \rho M_2^\dagger$. Покажите, что такая процедура может уменьшить энтропию кубита.

11.3.4 Субаддитивность

Рассмотрим составную квантовую систему AB , находящуюся в состоянии ρ^{AB} . Мы покажем, что для совместной энтропии этой системы выполняются следующие неравенства:

$$S(A, B) \leq S(A) + S(B), \quad (11.72)$$

$$S(A, B) \geq |S(A) - S(B)|. \quad (11.73)$$

Первое из этих неравенств выражает свойство *субаддитивности* энтропии фон Неймана. Оно превращается в равенство тогда и только тогда, когда системы A и B нескоррелированы, т. е. $\rho^{AB} = \rho^A \otimes \rho^B$. Соотношение (11.73) называется неравенством *треугольника*, или неравенством *Араки-Либа*. Оно является квантовым аналогом классического неравенства $H(X, Y) \geq H(X)$ для шенноновской энтропии.

Для доказательства неравенства субаддитивности воспользуемся неравенством Клейна $S(\rho) \leq -\text{tr}(\rho \log \sigma)$. Положив $\rho \equiv \rho^{AB}$, а $\sigma \equiv \rho^A \otimes \rho^B$, мы замечаем, что

$$-\text{tr}(\rho \log \sigma) = -\text{tr}(\rho^{AB} (\log \rho^A + \log \rho^B)) \quad (11.74)$$

$$= -\text{tr}(\rho^A \log \rho^A) - \text{tr}(\rho^B \log \rho^B) \quad (11.75)$$

$$= S(A) + S(B). \quad (11.76)$$

Из неравенства Клейна следует, что $S(A, B) \leq S(A) + S(B)$. Заметим, что неравенство Клейна превращается в равенство при $\rho = \sigma$ и, следовательно, неравенство субаддитивности превращается в равенство при $\rho^{AB} = \rho^A \otimes \rho^B$.

Для доказательства неравенства треугольника введем вспомогательную систему R , расширяющую составную систему AB до чистого состояния (разд. 2.5). Используя свойство субаддитивности, получаем

$$S(R) + S(A) \geq S(A, R). \quad (11.77)$$

Поскольку составная система ABR находится в чистом состоянии, то $S(A, R) = S(B)$, а $S(R) = S(A, B)$. Поэтому неравенство (11.77) может быть переписано как

$$S(A, B) \geq S(B) - S(A). \quad (11.78)$$

Условия, при которых оно превращается в равенство, устанавливаются не так просто, как для неравенства субаддитивности. Формально условие равенства состоит в том, что $\rho^{AB} = \rho^A \otimes \rho^B$. Интуитивно понятно, что это означает то, что система A запутана с внешним миром за счет корреляций с системой B . Строгая математическая формулировка этого условия предлагается читателю ниже в качестве упражнения 11.16.

В силу симметрии между системами A и B справедливо также неравенство $S(A, B) \geq S(A) - S(B)$, что с учетом неравенства $S(A, B) \geq S(B) - S(A)$ доказывает неравенство треугольника.

Упражнение 11.16 (условие равенства $S(A, B) = S(B) - S(A)$). Рассмотрим спектральное разложение $\rho^{AB} = \sum_i \lambda_i |i\rangle\langle i|$ матрицы плотности ρ^{AB} . Покажите, что $S(A, B) = S(B) - S(A)$ тогда и только тогда, когда операторы $\rho_i^A \equiv \text{tr}_B(|i\rangle\langle i|)$ имеют общий набор собственных векторов, а носители операторов $\rho_i^B \equiv \text{tr}_A(|i\rangle\langle i|)$ ортогональны.

Упражнение 11.17. Приведите нетривиальный пример состояния ρ^{AB} составной системы AB , для которого $S(A, B) = S(B) - S(A)$.

11.3.5 Вогнутость энтропии

Энтропия является *вогнутой* функцией своего аргумента. Это значит, что если дано распределение вероятностей p_i (неотрицательных вещественных чисел, таких, что $\sum_i p_i = 1$) и набор матриц плотности ρ_i , то энтропия удовлетворяет неравенству

$$S\left(\sum_i p_i \rho_i\right) \geq \sum_i p_i S(\rho_i). \quad (11.79)$$

Интуитивно понятно, что $\sum_i p_i \rho_i$ описывает квантовую систему, которая находится в состоянии ρ_i с вероятностью p_i , и что неопределенность относительно этой смеси состояний должна быть больше, чем средняя неопределенность по всем состояниям ρ_i , поскольку неопределенность состояния $\sum_i p_i \rho_i$ имеет два источника неопределенности: неопределенность состояния ρ_i и неопределенность индекса i .

Пусть ρ_i являются состояниями системы A . Введем вспомогательную систему B , базисные состояния $|i\rangle$ которой нумеруются индексом i , тем же самым что и у ρ_i . Определим совместное состояние системы AB формулой

$$\rho^{AB} \equiv \sum_i p_i \rho_i \oplus |i\rangle\langle i|. \quad (11.80)$$

Теперь для доказательства вогнутости мы можем применить субаддитивность энтропии. Для составной системы AB в состоянии ρ^{AB} можно записать

$$S(A) = S\left(\sum_i p_i \rho_i\right), \quad (11.81)$$

$$S(B) = S\left(\sum_i p_i |i\rangle\langle i|\right) = H(p_i), \quad (11.82)$$

$$S(A, B) = H(p_i) + \sum_i p_i S(\rho_i). \quad (11.83)$$

Применяя неравенство субаддитивности $S(A, B) \leq S(A) + S(B)$, получаем

$$\sum_i p_i S(\rho_i) \leq S\left(\sum_i p_i \rho_i\right). \quad (11.84)$$

Это то, что нам нужно. Заметим, что равенство имеет место тогда и только тогда, когда все состояния ρ_i , для которых $p_i > 0$, совпадают друг с другом. Таким образом, энтропия является строго вогнутой функцией своего аргумента.

Следует сказать несколько слов относительно стратегии, которую мы использовали при доказательстве вогнутости энтропии, а также неравенства треугольника. Мы вводили вспомогательную систему B для того, чтобы доказать некоторое утверждение о системе A . Введение вспомогательных систем в квантовой теории информации используется довольно часто, и мы будем это делать еще много раз. Система B вводится потому, что мы хотим найти систему, одна из частей которой находится в состоянии $\sum_i p_i \rho_i$, причем значение i не известно. Система B служит для хранения «истинного» значения i . Если «истинное» состояние A есть ρ_i , то система B находится в состоянии $|i\rangle\langle i|$, причем мы можем узнать i , производя измерение над B . Использование вспомогательных систем позволяет превратить интуитивные соображения в строгие доказательства и является очень полезным инструментом в квантовой теории информации.

Упражнение 11.18. Докажите, что (11.79) превращается в равенство тогда и только тогда, когда все состояния ρ_i совпадают.

Упражнение 11.19. Предложите набор унитарных операторов U_j и распределение вероятностей p_j , такие, что для любого оператора A выполняется равенство

$$\sum_i p_i U_i U_i^\dagger = \text{tr}(A) \frac{I}{d}, \quad (11.85)$$

где d — размерность пространства состояний, на котором действует A . Используя этот факт и строгую вогнутость энтропии, докажите еще одним способом, что однородное состояние I/d в пространстве размерности d является единственным состоянием с максимальной энтропией.

Упражнение 11.20. Пусть P и $Q = I - P$ — два проектора на дополняющие друг друга подпространства. Докажите, что существуют такие унитарные операторы U_1 , U_2 и вероятность p , что для любого ρ выполняется равенство $P\rho P + Q\rho Q = pU_1\rho U_1^\dagger + (1-p)U_2\rho U_2^\dagger$. Используя этот факт и вогнутость энтропии, докажите теорему 11.9.

Упражнение 11.21 (вогнутость шенноновской энтропии). Докажите вогнутость шенноновской энтропии исходя из вогнутости энтропии фон Неймана.

Упражнение 11.22 (другое доказательство вогнутости). Положим $f(p) \equiv S(p\rho + (1-p)\sigma)$. Покажите что для вогнутости энтропии достаточно выполнения условия $f''(p) \leq 0$. Докажите, что $f''(p) \leq 0$, сначала считая, что ρ и σ обратимы, а затем для случая, когда они не обратимы.

11.3.6 Энтропия смеси квантовых состояний

С помощью свойства вогнутости можно получить полезную теорему, которая устанавливает верхнюю оценку для энтропии смеси квантовых состояний $\sum_i p_i \rho_i$. Объединяя этот результат с полученной ранее нижней оценкой, мы получаем следующие неравенства для энтропии смеси $\sum_i p_i \rho_i$ квантовых состояний ρ_i :

$$\sum_i S(\rho_i) \leq S\left(\sum_i p_i \rho_i\right) \leq \sum_i p_i S(\rho_i) + H(p_i). \quad (11.86)$$

Неравенство справа выражает то, что неопределенность состояния $\sum_i p_i \rho_i$ не может быть больше, чем сумма средней неопределенности по всем состояниям ρ_i и величины $H(p_i)$, представляющей максимально возможную неопределенность относительно значения индекса i . Теперь докажем это неравенство.

Теорема 11.10. Пусть $\rho = \sum_i p_i \rho_i$, где p_i — произвольное распределение вероятностей, а ρ_i — любые матрицы плотности. Тогда

$$S(\rho) \leq \sum_i p_i S(\rho_i) + H(p_i), \quad (11.87)$$

причем равенство имеет место тогда и только тогда, когда носители всех операторов ρ_i ортогональны.

Доказательство.

Предположим сначала что все состояния ρ_i чистые, $\rho_i = |\psi_i\rangle\langle\psi_i|$. Считая, что ρ_i — состояния системы A , введем вспомогательную систему B , базисные ортонормированные состояния $|i\rangle$ которой нумеруются тем же индексом i , что и вероятность p_i . Положим

$$|AB\rangle \equiv \sum_i \sqrt{p_i} |\psi\rangle |i\rangle. \quad (11.88)$$

Поскольку $|AB\rangle$ является чистым состоянием, мы заключаем, что

$$S(B) = S(A) = S\left(\sum_i p_i |\psi\rangle\langle\psi|\right) = S(\rho). \quad (11.89)$$

Выполним проективное измерение над системой B в базисе $|i\rangle$. После измерения состояние системы B оказывается равным

$$\rho^{B'} = \sum_i p_i |i\rangle\langle i|. \quad (11.90)$$

Согласно теореме 11.9, энтропия не уменьшается при проективных измерениях, так что $S(\rho) = S(B) \leq S(B') = H(p_i)$. Поскольку состояния ρ_i чистые и $S(\rho_i) = 0$, можно записать

$$S(\rho) \leq H(p_i) + \sum_i p_i S(\rho_i). \quad (11.91)$$

Равенство в (11.91) имеет место тогда и только тогда, когда $B = B'$. Как легко увидеть, это означает, что состояния $|\psi_i\rangle$ должны быть ортогональными.

Рассмотрения случая смешанных состояний теперь не представляет труда. Пусть $\rho_i = \sum_j p_j^i |e_j^i\rangle\langle e_j^i|$ — спектральное разложение состояний ρ_i , так что $\rho = \sum_{ij} p_i p_j^i |e_j^i\rangle\langle e_j^i|$ для состояния ρ . Применяя полученный выше результат для чистого состояния и учитывая, что $\sum_j p_j^i = 1$ для всех i , получаем

$$S(\rho) \leq - \sum_{ij} p_i p_j^i \log(p_i p_j^i) \quad (11.92)$$

$$= - \sum_i p_i \log p_i - \sum_i p_i \sum_j p_j^i \log p_j^i \quad (11.93)$$

$$= H(p_i) + \sum_i p_i S(\rho_i), \quad (11.94)$$

что и требовалось. Условия равенства для смеси состояний получаются из условий равенства для чистого состояния. ■

11.4 Сильная субаддитивность

В этом разделе мы рассмотрим неравенство субаддитивности и неравенство треугольника для систем, состоящих из трех частей. Основной результат, который будет получен, это неравенство *сильной субаддитивности*, являющееся

чрезвычайно важным и полезным для квантовой теории информации:

$$S(A, B, C) + S(B) \leq S(A, B) + S(B, C). \quad (11.95)$$

Здесь A, B, C — произвольная тройка квантовых систем. К сожалению, в отличие от классического аналога квантовая субаддитивность доказывается довольно сложно. Однако она настолько полезна для квантовой теории информации, что мы сочли нужным привести доказательство этого результата. Общая схема доказательства дана в подразд. 11.4.1, а некоторые его детали приведены в Приложении 6.

11.4.1 Доказательство сильной субаддитивности

Для доказательства сильной субаддитивности мы привлечем глубокий математический результат, известный как *теорема Либа*. Прежде, чем сформулировать ее, введем одно новое определение.

Пусть $f(A, B)$ — вещественная функция от двух матриц A, B . Будем называть f *совместно вогнутой* по A и B , если для $0 \leq \lambda \leq 1$ выполняется неравенство

$$f(\lambda A_1 + (1-\lambda)A_2, \lambda B_1 + (1-\lambda)B_2) \geq \lambda f(A_1, B_1) + (1-\lambda)f(A_2, B_2). \quad (11.96)$$

Упражнение 11.23 (совместная вогнутость и вогнутость по каждой переменной). Докажите, что совместно вогнутая функция $f(A, B)$ является также вогнутой по переменной A при фиксированной переменной B . Найдите пример функции двух переменных, которая вогнута по каждой из переменных, но не является совместно вогнутой.

Теорема 11.11 (теорема Либа). Пусть X — произвольная матрица и $0 \leq t \leq 1$. Тогда функция

$$f(A, B) \equiv \text{tr}(X^\dagger A^t X B^{1-t}), \quad (11.97)$$

определенная на множестве неотрицательных определенных матриц, является совместно вогнутой по A и B .

Доказательство этой теоремы приводится в Приложении 6.

Используя теорему Либа мы выведем последовательность утверждений, приводящую в конечном счете к доказательству сильной субаддитивности. В то же время эти утверждения интересны и сами по себе. Первое из них — это выпуклость относительной энтропии.

Теорема 11.12 (выпуклость относительной энтропии). Относительная энтропия $S(\rho||\sigma)$ является совместно выпуклой по ρ и σ .

Доказательство.

Рассмотрим функцию

$$I_t(A, X) \equiv \text{tr}(X^\dagger A^t X B^{1-t}) - \text{tr}(X^\dagger X A), \quad (11.98)$$

где A и X — произвольные операторы, определенные на одном и том же пространстве. Первое слагаемое является вогнутой функцией от A по теореме Либа, второе слагаемое линейно по A , следовательно, $I_t(A, X)$ является вогнутой функцией от A . Пусть

$$I_t(A, X) \equiv \frac{d}{dt}|_{t=0} I_t(A, X) = \text{tr}(X^\dagger(\log A)XA) - \text{tr}(X^\dagger X(\log A)A). \quad (11.99)$$

Замечая, что $I_0(A, X) = 0$ и используя вогнутость $I_t(A, X)$ по A , получаем

$$I(\lambda A_1 + (1-\lambda)A_2, X) = \lim_{\Delta \rightarrow 0} \frac{I_\Delta(\lambda A_1 + (1-\lambda)A_2, X)}{\Delta} \quad (11.100)$$

$$\geq \lambda \lim_{\Delta \rightarrow 0} \frac{I_\Delta(A_1, X)}{\Delta} + (1-\lambda) \lim_{\Delta \rightarrow 0} \frac{I_\Delta(A_2, X)}{\Delta} \quad (11.101)$$

$$= \lambda I(A_1, X) + (1-\lambda)I(A_2, X). \quad (11.102)$$

Таким образом, $I(A, X)$ является вогнутой функцией от A . Определим блочные матрицы

$$A \equiv \begin{bmatrix} \rho & 0 \\ 0 & \sigma \end{bmatrix}, X \equiv \begin{bmatrix} 0 & 0 \\ I & 0 \end{bmatrix}. \quad (11.103)$$

Как несложно проверить, $I(A, X) = -S(\rho||\sigma)$, поэтому совместная выпуклость $S(\rho||\sigma)$ следует из вогнутости $I(A, X)$ по A . ■

Следствие 11.13 (вогнутость квантовой условной энтропии) Рассмотрим составную квантовую систему AB , состоящую из компонент A и B . Условная энтропия $S(A|B)$ является вогнутой функцией от состояния ρ^{AB} составной системы AB .

Доказательство.

Пусть d — размерность пространства состояний системы A . Заметим, что

$$S\left(\rho^{AB} \parallel \frac{I}{d} \otimes \rho^B\right) = -S(A, B) - \text{tr}\left(\rho_{AB} \log\left(\frac{I}{d} \otimes \rho^B\right)\right) \quad (11.104)$$

$$= -S(A, B) - \text{tr}(\rho^B \log \rho^B) + \log d \quad (11.105)$$

$$= -S(A|B) + \log d. \quad (11.106)$$

Таким образом, $S(A|B) = \log d - S(\rho^{AB}||I/d \otimes \rho^B)$. Вогнутость $S(A|B)$ следует из совместной выпуклости относительной энтропии. ■

Теорема 11.14 (сильная субаддитивность). Для любой тройки квантовых систем A, B, C справедливы неравенства

$$S(A) + S(B) \leq S(A, C) + S(B, C), \quad (11.107)$$

$$S(A, B, C) + S(B) \leq S(A, B) + S(B, C). \quad (11.108)$$

Доказательство.

Мы докажем первое неравенство, используя вогнутость условной энтропии, а затем покажем, что второе неравенство следует из первого (как несложно увидеть из доказательства, эти два неравенства эквивалентны друг другу). Рассмотрим функцию $T(\rho^{ABC})$, определенную на состояниях составной системы ABC :

$$T(\rho^{ABC}) \equiv S(A) + S(B) - S(A, C) - S(B, C) = -S(C|A) - S(C|B). \quad (11.109)$$

Из вогнутости условной энтропии следует, что $T(\rho^{ABC})$ является выпуклой функцией от состояния ρ^{ABC} . Далее, рассмотрим спектральное разложение состояния составной системы $\rho^{ABC} = \sum_i p_i |i\rangle\langle i|$. Из выпуклости функции T следует, что $T(\rho^{ABC}) \leq \sum_i p_i T(|i\rangle\langle i|)$. Но для любого чистого состояния системы ABC мы имеем $S(A, C) = S(B)$, $S(B, C) = S(A)$ и, таким образом, $T(|i\rangle\langle i|) = 0$. Следовательно, $T(\rho^{ABC}) \leq 0$, т. е.

$$S(A) + S(B) - S(A, C) - S(B, C) \leq 0, \quad (11.110)$$

что совпадает с первым неравенством, которое нужно было доказать.

Чтобы доказать второе неравенство, введем вспомогательную систему R , расширяющую ABC до чистого состояния. Применяя уже доказанное неравенство, получаем

$$S(R) + S(B) \leq S(R, C) + S(B, C). \quad (11.111)$$

Но поскольку $ABCR$ находится в чистом состоянии, то $S(R) = S(A, B, C)$, $S(R, C) = S(A, B)$, поэтому неравенство (11.111) принимает вид

$$S(A, B, C) + S(B) \leq S(A, B) + S(B, C), \quad (11.112)$$

что и требовалось доказать. ■

Упражнение 11.24. Мы доказали сильную субаддитивность как следствие неравенства $S(A) + S(B) \leq S(A, C) + S(B, C)$. Покажите, что это неравенство в свою очередь является следствием сильной субаддитивности.

Упражнение 11.25. Мы доказали сильную субаддитивность как следствие вогнутости условной энтропии $S(A|B)$. Покажите, что вогнутость условной энтропии в свою очередь является следствием сильной субаддитивности. (*Указание.* Для решения этой задачи удобно ввести вспомогательную систему.)

11.4.2 Сильная субаддитивность: основные применения

Сильная субаддитивность и связанные с ней результаты имеют много полезных приложений для квантовой теории информации. В этом разделе мы рассмотрим несколько таких приложений.

Во первых, следует подчеркнуть, что неравенство $S(A) + S(B) \leq S(A, C) + S(B, C)$ является весьма тонким свойством квантовой энтропии. Данное неравенство выполняется и для шенноновской энтропии, но по несколько другим

причинам. Для шенноновской энтропии справедливы соотношения $H(A) \leq H(A,C)$ и $H(B) \leq H(B,C)$, и неравенство получается сложением этих двух соотношений. В квантовом случае, возможно, $S(A) > S(A,C)$ или $S(B) > S(B,C)$. Тем не менее Природа почему-то выбрала соотношение $S(A) + S(B) \leq S(A,C) + S(B,C)$, так что ситуация, когда одновременно $S(A) > S(A,C)$ и $S(B) > S(B,C)$, запрещена. Сильную субаддитивность можно также сформулировать и с использованием понятия условной энтропии и взаимной информации:

$$0 \leq S(C|A) + S(C|B), \quad (11.113)$$

$$S(A:B) + S(A:C) \leq 2S(A). \quad (11.114)$$

Глядя на формулу (11.114), возникает желание написать также неравенство $0 \leq S(A|C) + S(B|C)$. Однако, как можно убедиться, взяв в качестве состояния ABC произведение чистого состояния для A и ЭПР состояния для BC , это неверно.

Упражнение 11.26. Докажите что $S(A:B) + S(A:C) \leq 2S(A)$. Отметим, что для шенноновской энтропии это неравенство является следствием $H(A:B) \leq H(A)$ и $H(A:C) \leq H(A)$. Найдите пример состояния, для которого $S(A:B) > S(A)$.

Для практических применений свойство сильной субаддитивности удобно формулировать именно через условную энтропию и взаимную информацию. В следующей теореме приводятся три очень простые формулировки сильной субаддитивности, которые дают некоторое интуитивное представление о свойствах квантовой энтропии.

Теорема 11.15. (1) Дополнительные условия уменьшают энтропию. Пусть ABC – составная квантовая система. Тогда $S(A|B,C) \leq S(A|B)$.

(2) Выбрасывание компонент квантовой системы не может увеличить взаимную информацию. Пусть ABC – составная квантовая система. Тогда $S(A:B) \leq S(A:B,C)$.

(3) Квантовые преобразования не могут увеличить взаимную информацию. Допустим, что AB – составная квантовая система, а \mathcal{E} – преобразование, сохраняющее след и действующее только на систему B . Пусть $S(A:B)$ – взаимная информация между системами A и B до применения \mathcal{E} , а $S(A':B')$ – взаимная информация после применения \mathcal{E} . Тогда $S(A':B') \leq S(A:B)$.

Доказательство.

(1) Доказывается также как и в классическом случае (см. теорему 11.3). Для удобства приведем доказательство еще раз. Неравенство $S(A|B,C) \leq S(A|B)$ эквивалентно $S(A,B,C) - S(B,C) \leq S(A,B) - S(B)$ или $S(A,B,C) + S(B) \leq S(A,B) + S(B,C)$. Это условие сильной аддитивности.

(2) Неравенство $S(A:B) \leq S(A:B,C)$ эквивалентно $S(A) + S(B) - S(A,B) \leq S(A) + S(B,C) - S(A,B,C)$ или $S(A,B,C) + S(B) \leq S(A,B) + S(B,C)$. Это условие сильной аддитивности.

(3) Вспомогательная система C , находящаяся в чистом состоянии $|0\rangle$, и унитарный оператор U , действующий на пространстве составной системы BC , позво-

ляют промоделировать действие преобразования \mathcal{E} на систему B (гл. 8). Действие \mathcal{E} на систему B эквивалентно применению унитарного оператора U и выбрасыванию системы C . До применения U мы имели $S(A:B) = S(A:B,C)$, поскольку система C находится в чистом состоянии. После применения U мы имеем $S(A':B',C') = S(A:B,C)$ (буквы со штрихами относятся к состоянию системы после применения U). Поскольку выбрасывание системы не увеличивает взаимную информацию, то $S(A':B') \leq S(A':B',C')$. Подставляя сюда $S(A':B',C')$, найденное выше, мы получаем $S(A':B') \leq S(A:B)$, что и требовалось доказать. ■

Существует также ряд интересных вопросов, связанных со свойствами субаддитивности квантовых условных энтропий. Как мы уже видели, шенноновская взаимная информация не субаддитивна, а, следовательно, и квантовая взаимная информация не субаддитивна. Субаддитивна ли квантовая условная энтропия, т. е. выполняется ли неравенство:

$$S(A_1, A_2|B_1, B_2) \leq S(A_1|B_1) + S(A_2|B_2) \quad (11.115)$$

для произвольных квантовых систем A_1, A_2, B_1 и B_2 ? Оказывается, что это неравенство справедливо. Более того, условная энтропия субаддитивна по первой (A_1, A_2) и второй (B_1, B_2) паре аргументов. Доказательство этих фактов является хорошим упражнением по применению свойства сильной субаддитивности.

Теорема 11.16 (субаддитивность условной энтропии). Для составной квантовой системы $ABCD$ условная энтропия $S(A, B|C, D)$ является совместно субаддитивной по аргументам AB и CD :

$$S(A, B|C, D) \leq S(A|C) + S(B|D). \quad (11.116)$$

Для составной квантовой системы ABC условные энтропии $S(A, B|C)$ и $S(A|B, C)$ являются субаддитивными:

$$S(A, B|C) \leq S(A|C) + S(B|C), \quad (11.117)$$

$$S(A|B, C) \leq S(A|B) + S(A|C). \quad (11.118)$$

Доказательство.

Для доказательства совместной субаддитивности заметим, что из сильной субаддитивности следует неравенство

$$S(A, B, C, D) + S(C) \leq S(A, C) + S(B, C, D). \quad (11.119)$$

Прибавляя к правой и левой частям $S(D)$, получаем

$$S(A, B, C, D) + S(C) + S(D) \leq S(A, C) + S(B, C, D) + S(D). \quad (11.120)$$

Применяя свойство сильной субаддитивности еще раз, преобразуем два последних слагаемых в правой части:

$$S(A, B, C, D) + S(C) + S(D) \leq S(A, C) + S(B, D) + S(C, D). \quad (11.121)$$

Это неравенство эквивалентно следующему:

$$S(A, B|C, D) \leq S(A|C) + S(B|D), \quad (11.122)$$

что доказывает совместную субаддитивность условной энтропии.

Субаддитивность условной энтропии по первому аргументу, $S(A, B|C) \leq S(A|C) + S(B|C)$, эквивалентна сильной субаддитивности. Доказательство субаддитивности по второму аргументу несколько сложнее. Нужно доказать, что $S(A|B, C) \leq S(A|B) + S(A|C)$. По определению условной энтропии, это эквивалентно неравенству

$$S(A, B, C) + S(B) + S(C) \leq S(A, B) + S(B, C) + S(A, C). \quad (11.123)$$

Для его доказательства заметим, что должно выполняться хотя бы одно из неравенств $S(C) \leq S(A, C)$ или $S(B) \leq S(A, B)$, поскольку согласно теореме 11.14 мы имеем $S(A|B) + S(A|C) \geq 0$ (первое утверждение теоремы). Допустим, что $S(C) \leq S(A, C)$. Если прибавить к этому неравенству неравенство сильной аддитивности $S(A, B, C) + S(B) \leq S(A, B) + S(B, C)$, то получим неравенство (11.123). Случай $S(B) \leq S(A, B)$ рассматривается аналогично. ■

При нашем первом знакомстве с относительной энтропией мы упомянули, что ее можно рассматривать как меру различия между двумя распределениями вероятностей, или между двумя матрицами плотности. Допустим, что квантовая система состоит из двух частей A, B и рассмотрим произвольные матрицы плотности ρ^{AB} и σ^{AB} , описывающие состояние всей системы. Если $S(\cdot||\cdot)$ действительно является хорошей мерой различия, можно ожидать что она уменьшается при выбрасывании части системы, т. е. что

$$S(\rho^A||\sigma^A) \leq S(\rho^{AB}||\sigma^{AB}). \quad (11.124)$$

Это неравенство выражает **монотонность** относительной энтропии. Его смысл состоит в том, что выбрасывание части составной системы (т. е. игнорирование части информации о системе) затрудняет различие двух состояний системы (см. также подразд. 9.2.1), и, следовательно, уменьшает любую разумную меру различия состояний.

Теорема 11.17 (монотонность относительной энтропии). Пусть ρ^{AB} и σ^{AB} — произвольные состояния составной системы AB . Тогда

$$S(\rho^A||\sigma^A) \leq S(\rho^{AB}||\sigma^{AB}). \quad (11.125)$$

Доказательство.

Согласно упр. 11.19, мы можем подобрать такие унитарные операторы U_j и вероятности p_j , что для всех ρ^{AB} будет выполняться равенство

$$\rho^A \otimes \frac{I}{d} = \sum_j p_j U_j \rho^{AB} U_j^\dagger. \quad (11.126)$$

Из выпуклости относительной энтропии следует что

$$S\left(\rho^A \otimes \frac{I}{d} \middle\| \sigma^A \otimes \frac{I}{d}\right) \leq \sum_j p_j S\left(U_j \rho^{AB} U_j^\dagger \middle\| U_j \sigma^{AB} U_j^\dagger\right). \quad (11.127)$$

Относительная энтропия инвариантна относительно унитарных преобразований, поэтому

$$S\left(\rho^A \otimes \frac{I}{d} \middle\| \sigma^A \otimes \frac{I}{d}\right) \leq \sum_j p_j S(\rho^{AB} \middle\| \sigma^{AB}) = S(\rho^{AB} \middle\| \sigma^{AB}). \quad (11.128)$$

Как несложно убедиться,

$$S\left(\rho^A \otimes \frac{I}{d} \middle\| \sigma^A \otimes \frac{I}{d}\right) \leq \sum_j p_j S(\rho^{AB} \middle\| \sigma^{AB}) = S(\rho^A \middle\| \sigma^A), \quad (11.129)$$

и, таким образом, монотонность относительной энтропии доказана. ■

Задача 11.1 (обобщенное неравенство Клейна). Пусть $f(\cdot)$ — произвольная выпуклая вещественная функция от вещественной переменной. Как объяснялось в подразд. 2.1.8, $f(\cdot)$ можно также рассматривать как функцию на множестве эрмитовых операторов. Докажите, что

$$\text{tr}(f(A) - f(B)) \geq \text{tr}((A - B)f'(B)). \quad (11.130)$$

Используя этот результат, покажите, что относительная энтропия неотрицательна.

Задача 11.2 (обобщенная относительная энтропия). Определение относительной энтропии $S(r \middle\| s)$ можно рассматривать в более широком смысле, считая что r и s — произвольные положительные операторы,

$$S(r \middle\| s) \equiv \text{tr}(r \log r) - \text{tr}(r \log s). \quad (11.131)$$

Данное выше доказательство совместной выпуклости относительной энтропии непосредственно применимо к этому обобщенному определению.

1. Покажите, что для любых $\alpha, \beta > 0$

$$S(\alpha r \middle\| \beta s) = \alpha S(r \middle\| s) + \alpha \text{tr}(r) \log(\alpha/\beta). \quad (11.132)$$

2. Исходя из совместной выпуклости относительной энтропии, докажите субаддитивность относительной энтропии, т. е. что

$$S(r_1 + r_2 \middle\| s_1 + s_2) \leq S(r_1 \middle\| s_1) + S(r_2 \middle\| s_2). \quad (11.133)$$

3. Исходя из субаддитивности относительной энтропии, докажите совместную выпуклость относительной энтропии.

4. Пусть p_i и q_i — произвольные распределения вероятностей. Покажите, что

$$S\left(\sum_i p_i r_i \parallel \sum_i q_i s_i\right) \leq \sum_i p_i S(r_i \parallel s_i) + \sum_i p_i \text{tr}(r_i) \log(p_i/q_i). \quad (11.134)$$

Заметим, что если операторы r_i нормированы так, что $\text{tr}(r_i) = 1$, это выражение принимает очень простой вид

$$S\left(\sum_i p_i r_i \parallel \sum_i q_i s_i\right) \leq \sum_i p_i S(r_i \parallel s_i) + H(p_i \parallel q_i), \quad (11.135)$$

—где $H(\cdot \parallel \cdot)$ — шенноновская относительная энтропия.

Задача 11.3 (аналог неравенства треугольника для условной энтропии).

1. Покажите что $H(X, Y|Z) \geq H(X|Z)$.
2. Покажите что неравенство $S(A, B|C) \geq S(A|C)$ не всегда верно.
3. Докажите аналог неравенства треугольника для условной энтропии, т. е. что

$$S(A, B|C) \geq S(A|C) - S(B|C). \quad (11.136)$$

Задача 11.4 (условные формы сильной субаддитивности). (1) Докажите, что $S(A, B, C|D) + S(B|D) \leq S(A, B|D) + S(B, C|D)$.

(2) Покажите на примере, что неравенство $H(D|A, B, C) + H(D|B) \leq H(D|A, B) + H(D|B, C)$ не всегда верно.

Задача 11.5 (исследование сильной субаддитивности). Предложите простое доказательство сильной субаддитивности для квантовой энтропии.

Краткое содержание главы

- Любую фундаментальную меру информации можно определить как количество физических ресурсов, необходимое для решения некоторой задачи по обработке данных.
- Основные определения:

(энтропия)	$S(A) = -\text{tr}(\rho^A \log \rho^A),$
(относительная энтропия)	$S(\rho \parallel \sigma) = -S(\rho) - \text{tr}(\rho \log \sigma),$
(условная энтропия)	$S(A B) = S(A, B) - S(B),$
(взаимная информация)	$S(A:B) = S(A) + S(B) - S(A, B).$

- **Сильная субаддитивность:** $S(A, B, C) + S(B) \leq S(A, B) + S(B, C)$. Другие неравенства для энтропии выводятся из этого неравенства и свойства совместной выпуклости относительной энтропии.
- **Относительная энтропия является совместно выпуклой функцией от своих аргументов.**
- **Относительная энтропия монотонна:** $S(\rho^A || \sigma^A) \leq S(\rho^{AB} || \sigma^{AB})$.

История и дополнительная литература

Исторически, понятие энтропии возникло в исследованиях по термодинамике и статистической физике. Современный теоретико-информационный интерес к энтропии был инициирован работами Шеннона по теории информации [353]. Для общего ознакомления со свойствами шенноновской энтропии (и другими вопросами теории информации) хорошо подходит учебник Ковера и Томаса [106], главы 2 и 16. Всестороннее обсуждение энтропии фон Неймана можно найти в обзоре Верля [413], а также в книге Огия и Пеца [308].

Энтропийный принцип неопределенности рассматривался в работе Дойча [116]. Энтропийные соотношения неопределенностей изучались также во многих других работах, и здесь мы упомянем лишь два интересных результата. Соотношение неопределенностей, усилившее неравенство Дойча для некоторых специальных измерений, было предложено Краусом [230] и затем доказано в работе Маассена и Уффинка [297]. Понятие относительной энтропии было введено Куллбэком и Лейблером [215], а его квантовый аналог был предложен Юмагаки [396]. Неравенству Фанне посвящена работа [145]. Неравенство Клейна доказано в работе [218]. Неравенство треугольника доказали Араки и Либ [11]. Интересную историю имеет неравенство сильной субаддитивности. Впервые важность классической сильной субаддитивности для *статистической физики* была отмечена Робинсоном и Рюэллем [341]. Квантовая версия сильной субаддитивности появилась в 1968 г. в качестве гипотезы в работе Ланфорда и Робинсона [264]. Однако доказать этот факт не удавалось довольно долго. Соответствующая теорема была доказана только в 1973 г. в двух работах: в работе Либа [243] — теорема Либа, и в работе Либа и Рускаи [266] — неожиданная связь между сильной субаддитивностью и теоремой Либа; см. также [265]. Теорема Либа является обобщением гипотезы *Вигнера-Янасе-Дайсона*, которую предложили в 1963 г. Вигнер и Янасе [422], а затем обобщил Дайсон (неопубликовано). Удивительно, что вплоть до 1973 г. никто не предполагал существование связи между гипотезой Вигнера-Янасе-Дайсона и сильной субаддитивностью. Обсуждение гипотезы Вигнера-Янасе-Дайсона содержится в работе Верля [413]. Приведенное в данной главе доказательство теоремы Либа принадлежит Саумону [358] и является вариантом доказательства предложенного Ульманом [395]. Существуют и другие доказательства этой

теоремы, см. например Эпштейна [144], Андо [16] и Пец [321]. Субаддитивность относительной энтропии по первому и второму аргументу была доказана в работе Либа [244]. Доказательство совместной субаддитивности квантовой условной энтропии содержится в работе Нильсена [303]. Монотонность относительной энтропии была впервые замечена Линдбладом [245]. Задача 11.2 предложена Рускаи [343].

Глава 12

КВАНТОВАЯ ТЕОРИЯ ИНФОРМАЦИИ

Классическая теория информации в основном изучает проблему передачи классической информации — букв алфавита, речи, битовых строк — по *каналам связи*, работающим по законам классической физики. Как изменится картина, если мы сможем построить квантовомеханические каналы связи? Сможем ли передавать информацию более эффективно? Можем ли мы применить квантовую механику для передачи секретной информации так, чтобы секретные данные не перехватили? Это только два вопроса из тех, которые возникают, если считать, что каналы связи квантовомеханические. При таком определении канала мы вынуждены пересмотреть фундаментальные вопросы, поставленные классической теорией информации в поисках новых ответов. В этой главе будет дан обзор того, что известно о квантовой теории информации, в том числе некоторые неожиданные и интригующие возможности, появляющиеся при использовании квантовых каналов связи.

Изучение каналов связи способствует развитию квантовой теории информации, но область ее применения гораздо шире. Как показано в разд. 1.6, можно выделить три фундаментальные цели, придающие единство работе над квантовой теорией информации: определение элементарных классов статических ресурсов в квантовой механике (которые мы называем типами «информации»); определение элементарных классов динамических процессов в квантовой механике (методов «обработки информации»); определение количества ресурсов, необходимых для выполнения элементарных динамических процессов. Квантовая теория информации гораздо богаче, чем классическая теория информации, поскольку квантовая механика оперирует множеством элементарных классов статических и динамических ресурсов — не только знакомыми всем классическими типами, но и абсолютно новыми классами, как например, статический ресурс запутанности.

Глава называется «Квантовая теория информации», и может показаться удивительным, что мы надеемся представить все аспекты теории квантовой информации в одной главе? В самом деле, квантовая теория информации охватывает не только рассмотренные здесь вопросы, но и множество тем, подробно изложенных в предыдущих главах, включая изучение квантовых преобразований, определение и изучение мер различия квантовой информации, квантовые коды, исправляющие ошибки, и различные представления энтропии. Цель этой главы — описать квантовую теорию информации в ее «чистом» виде; остальные главы посвящены разработке специальных средств, тогда как здесь мы имеем дело с самыми общими формулировками, которыми можно определить свойства квантовой информации.

В разд. 12.1 мы начнем с обсуждения на языке теории информации некоторых свойств квантовых состояний, уникальных по сравнению с классическими состояниями. Квантовые состояния не только невозможно копировать, их вообще невозможно точно различить! Количественно это описывается с помощью границы Холево. В разд. 12.2 мы рассмотрим элементарную теоретико-информационную задачу *сжатия данных* и покажем, что квантовые состояния можно сжимать подобно классическим. При этом будут параллельно использоваться теорема о типичных последовательностях и теорема о типичном подпространстве, чтобы доказать теорему Шумахера о *кодировании для квантового канала без шума*, аналогичную теореме Шеннона о кодировании для классического канала без шума. Естественным обобщением этой проблемы является задача о пропускной способности квантового канала с шумом для классической информации и в разд. 12.3 мы докажем теорему Холево–Шумахера–Вестморланда, аналогичную теореме Шеннона о кодировании для классического канала с шумом. Самой сложной является задача о пропускной способности квантового канала с шумом для квантовой информации. Это тема разд. 12.4, в котором дается определение обмennой энтропии, рассматриваются квантовое неравенство Фано и квантовое неравенство обработки данных, однако, вопрос о пропускной способности так и остается открытым. В этом разделе также представлены квантовая граница Синглтона и «заклинание» демона Максвелла. В начале следующего раздела дается сводка основных результатов первой половины этой главы. Два вопроса — запутанность и неортогональность — обсуждаются на протяжении всего нашего исследования квантовой информации и являются объектами изучения двух последних разделов этой главы. В разд. 12.5 запутанность состояний рассматривается как *физический ресурс* и объясняется, каким образом можно преобразовать, очистить и разбавить запутанность. И, наконец, разд. 12.6 посвящен *квантовой криптографии*, обеспечивающей безопасную связь на основе многих свойств квантовой информации, рассмотренных в этой главе.

12.1 Различие квантовых состояний и доступная информация

Есть простая игра, в которую мы можем сыграть, чтобы проиллюстрировать значительные различия между квантовой и классической информацией. Опишем эту игру, используя два вымышленных персонажа, Алису и Боба; конечно, результаты можно выразить более абстрактно, но антропоцентрический язык делает результаты более легкими для осмысления (и описания!).

Предположим, что у Алисы есть источник классической информации, выдающий символы $X = 0, \dots, n$ в соответствии с распределением вероятностей p_0, \dots, p_n . Цель Боба — как можно лучше определить значение X . Алиса приготавливает квантовое состояние ρ_X , выбранное из некоторого фиксированного набора ρ_0, \dots, ρ_n , и предоставляет это состояние Бобу, который производит квантовое измерение над полученным состоянием, а затем пытается как можно лучше определить X на основе результата измерения Y .

Как установлено в гл. 11, хорошей мерой информации, полученной Бобом об X с помощью измерения, является взаимная информация $H(X:Y)$ между X и результатом измерения Y . Из неравенства обработки данных мы знаем, что Боб может определить X из Y тогда и только тогда, когда $H(X:Y) = H(X)$ (в общем случае $H(X:Y) \leq H(X)$); далее мы увидим, что близость $H(X:Y)$ к $H(X)$ действительно обеспечивает количественную меру того, насколько хорошо Боб может определить X . Цель Боба — выбрать измерение, с помощью которого можно достичь максимального значения $H(X:Y)$, наиболее близкого к $H(X)$. Поэтому мы определяем *доступную* Бобу *информацию* как максимум взаимной информации $H(X:Y)$ по всем возможным схемам измерения. Доступная информация — мера того, насколько хорошо Боб может определить состояние, которое подготовила Алиса.

В классической теории информации доступная информация не так интересна; на практике бывает сложно различить два классических состояния (вспомним неудобства при чтении письма, написанного плохим почерком), хотя, в принципе, это всегда возможно. В противоположность классической теории в квантовой механике не всегда возможно различить отдельные состояния даже в принципе. Например, во вставке 2.3 показано, что не существует квантово-механической процедуры надежного различения двух неортогональных квантовых состояний. В терминах доступной информации это означает, что если Алиса приготавливает состояние $|\psi\rangle$ с вероятностью p и другое неортогональное состояние $|\varphi\rangle$ с вероятностью $1 - p$, то доступная информация строго меньше, чем $H(p)$, поскольку Боб не может определить данное состояние совершенно точно. Если в классическом варианте Алиса приготавливает одно из двух классических состояний, например, бит в состоянии 0 с вероятностью p или в состоянии 1 с вероятностью $1 - p$, то в этом случае нет особой причины, по которой Боб не может различить эти два состояния, и, следовательно, доступная информация совпадает с энтропией $H(p)$.

Однако, существует ситуация, когда понятие доступной информации приобретает классический смысл. Речь о идет различии распределений вероятностей. Предположим, что Алиса приготавливает состояние 0 или 1 в соответствии с одним из двух распределений вероятностей: $(p, 1 - p)$ или $(q, 1 - q)$. Получив состояние, Боб должен определить, какое распределение вероятностей использовала Алиса для приготовления состояния. Очевидно, что Боб не всегда может это сделать с большой точностью! Однако, этот пример (аналогичный случаю квантовой системы, приготовленной в одном из смешанных состояний) имеет второстепенное значение. Более важно то, что основные объекты квантовой механики — чистые квантовые состояния — обладают свойствами различимости, которые и сильно отличаются от соответствующих свойств основных объектов классической теории информации, таких как «0» или «1», и гораздо богаче их.

Теорема о невозможности копирования — это другое объяснение трудности доступа к квантовой информации по сравнению с классической. Классическую информацию, конечно, можно скопировать. Это может быть выполнено точно с цифровой информацией подобно тому, как был многократно скопирован

ЛАTeX-файл, использованный для создания этой книги, или приблизительно, как аналоговые изображения, появляющиеся на каждой странице этой книги, были скопированы печатной машиной перед тиражированием. Удивительно, но теорема о невозможности копирования устанавливает, что квантовая механика не разрешает точно скопировать неизвестные квантовые состояния, и жестко ограничивает наши возможности делать приближенные копии. Доказательство теоремы о невозможности копирования приведено во вставке 12.1.

С первого взгляда теорема о невозможности копирования кажется довольно странной. В конце концов, разве классическая физика не является частным случаем квантовой механики? Как можно копировать классическую информацию, если мы не можем копировать квантовые состояния? Ответ таков: теорема о невозможности копирования не запрещает копирование *всех* квантовых состояний, а просто утверждает, что не могут быть скопированы неортогональные квантовые состояния. Более точно это можно выразить следующим образом. Предположим, что $|\psi\rangle$ и $|\varphi\rangle$ — неортогональные квантовые состояния. Теорема о невозможности копирования утверждает, что невозможно построить квантовое устройство так, чтобы в случае ввода $|\psi\rangle$ или $|\varphi\rangle$ на выходе получались две копии входного состояния $|\psi\rangle|\psi\rangle$ или $|\varphi\rangle|\varphi\rangle$. С другой стороны, если $|\psi\rangle$ и $|\varphi\rangle$ ортогональны, то теорема о невозможности копирования не запрещает их копирование. Действительно, довольно легко спроектировать квантовые схемы, копирующие такие состояния! Это наблюдение разрешает явное противоречие между теоремой о невозможности копирования и возможностью копировать классическую информацию; различные состояния классической информации можно рассматривать просто как ортогональные квантовые состояния.

Упражнение 12.1. Предположим, что $|\psi\rangle$ и $|\varphi\rangle$ — два ортогональных квантовых состояния одного кубита. Постройте квантовую схему с двумя входными кубитами — кубитом данных в состоянии $|\psi\rangle$ или $|\varphi\rangle$ и целевым кубитом, подготовленным в стандартном состоянии $|0\rangle$ — которая выдает на выходе $|\psi\rangle|\psi\rangle$ или $|\varphi\rangle|\varphi\rangle$ в зависимости от того, был ли кубит данных на входе в состоянии $|\psi\rangle$ или $|\varphi\rangle$.

Какая связь между копированием и доступной информацией? Предположим, что Алиса приготавливает одно из двух неортогональных квантовых состояний $|\psi\rangle$ или $|\varphi\rangle$ с соответствующими вероятностями p и $1 - p$. Пусть это тот случай, когда доступная Бобу информация об этих состояниях есть $H(p)$, т. е. законы квантовой механики позволяют Бобу получить с помощью измерения достаточно информации для того, чтобы определить, какое из двух состояний $|\psi\rangle$ или $|\varphi\rangle$ было приготовлено Алисой. Определив состояние, приготовленное Алисой, он мог бы затем создать множество копий этого состояния. Таким образом, теорему о невозможности копирования можно рассматривать как следствие того факта, что доступная информация для данных состояний строго меньше $H(p)$. И наоборот, тот факт, что доступная информация меньше $H(p)$, есть следствие теоремы о невозможности копирования! В этом можно убедиться следующим образом. Предположим, что можно копировать неортогональные состояния. После получения от Алисы состояния $|\psi\rangle$ или $|\varphi\rangle$ Боб мог бы использовать копирующее устройство, чтобы получить состояние $|\psi\rangle^{\otimes n}$ или

$|\varphi\rangle^{\otimes n}$. В пределе больших n эти два состояния становятся почти ортогональными и их можно со сколь угодно большой точностью различить с помощью проективного измерения. Итак, если бы эти состояния можно было копировать, Боб со сколь угодно большой вероятностью успеха мог бы определить, какое из состояний $|\psi\rangle$ или $|\varphi\rangle$ было приготовлено, и, следовательно, доступная информация была бы $H(p)$. Поэтому можно рассматривать теорему о невозможности копирования как эквивалент утверждения, что в квантовой механике доступная информация для неортогональных состояний, вообще говоря, меньше энтропии приготовления.

На протяжении всей книги мы повторяем, что скрытая природа квантовой информации обеспечивает эффективность квантовых вычислений, и доступная информация фиксирует в количественном виде эту скрытую природу квантовой информации. К сожалению, общий метод вычисления доступной информации не известен; однако, можно доказать ряд неравенств, важнейшим из которых является граница Холево.

12.1.1 Граница Холево

Граница Холево — чрезвычайно полезная верхняя оценка доступной информации, которая играет важную роль во многих применениях квантовой теории информации.

Теорема 12.1 (граница Холево). Предположим, что Алиса приготавливает состояние ρ_X , где $X = 0, \dots, n$ с вероятностями p_0, \dots, p_n . Боб проводит измерение над данным состоянием, описываемое с помощью POVM-элементов $\{E_y\} = \{E_0, \dots, E_m\}$, получая результат Y . Граница Холево устанавливает, что для любого такого измерения Боба выполняется неравенство

$$H(X : Y) \leq S(\rho) - \sum_x p_x S(\rho_x), \quad (12.6)$$

где $\rho = \sum_x p_x \rho_x$.

Величина, которая стоит в правой части неравенства (12.6), настолько полезна в квантовой теории информации, что получила название *энтропии Холево*, и иногда обозначается как χ .

Вставка 12.1. Теорема о невозможности копирования

Можно ли сделать копию неизвестного квантового состояния? Как это ни странно, нельзя. Здесь мы приводим элементарное доказательство этого факта, которое раскрывает существенную причину, почему это невозможно.

Предположим, что у нас есть квантовая машина с двумя слотами, обозначенными как A и B . Слот A , слот данных, вначале находится в неизвест-

ном, но чистом квантовом состоянии $|\psi\rangle$. Это то самое состояние, которое должно быть скопировано в слот B , *целевой слот*. Мы предполагаем, что целевой слот изначально находится в некотором стандартном чистом состоянии $|s\rangle$. Следовательно, начальное состояние копирующего устройства имеет вид

$$|\psi\rangle \otimes |s\rangle. \quad (12.1)$$

Некоторое унитарное преобразование U производит процедуру копирования, которая в идеальном виде выглядит так

$$|\psi\rangle \otimes |s\rangle \xrightarrow{U} U(|\psi\rangle \times |s\rangle) = |\psi\rangle \times |\psi\rangle. \quad (12.2)$$

Пусть данная процедура копирования выполняется для двух чистых состояний, $|\psi\rangle$ и $|\varphi\rangle$. Тогда имеем

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle, \quad (12.3)$$

$$U(|\varphi\rangle \otimes |s\rangle) = |\varphi\rangle \otimes |\varphi\rangle. \quad (12.4)$$

Взяв скалярное произведение этих двух уравнений, получим

$$\langle\psi|\varphi\rangle = (\langle\psi|\varphi\rangle)^2. \quad (12.5)$$

Но уравнение $x = x^2$ имеет только два решения, $x = 0$ и $x = 1$, так что, либо $|\psi\rangle = |\varphi\rangle$, либо $|\psi\rangle$ и $|\varphi\rangle$ ортогональны. Следовательно, устройство копирования может копировать только те состояния, которые ортогональны друг другу и поэтому универсальное квантовое устройство копирования невозможно. Потенциальное квантовое устройство копирования не может, например, копировать кубитовые состояния $|\psi\rangle = |0\rangle$ и $|\varphi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, поскольку эти состояния не ортогональны.

Итак, мы показали, что невозможно точно копировать неизвестное квантовое состояние, используя унитарное преобразование. Естественно возникает несколько вопросов. Что будет, если мы попробуем копировать смешанные состояния? Что произойдет, если допустить существование копирующих устройств, которые не унитарны? Что будет, если мы захотим допустить неточные копии, которые, тем не менее, «хорошо» соответствуют некоторым интересным мерам различия информации. Все эти вопросы уже были предметом многих исследований, см. разд. «История и дополнительная литература» в конце главы. Краткий вывод этих работ таков: даже при использовании неунитарных копирующих устройств, копирование неортогональных чистых состояний невозможно без определенной потери информации. Подобные выводы верны также для смешанных состояний, хотя необходим более сложный подход для определения понятия копирования смешанного состояния.

Доказательство.

Границу Холево можно доказать с помощью простого и красивого построения, включающего три квантовые системы, которые мы обозначим как P , Q и M . Система Q — квантовая система, которую Алиса предоставляет Бобу; P и M — вспомогательные системы, которые вводятся, чтобы облегчить доказательство, как это сделано при доказательстве многих энтропийных неравенств в гл. 11. Систему P можно интуитивно рассматривать как систему «приготовления». По определению, она имеет ортонормированный базис $|x\rangle$, элементы которого соответствуют возможным вариантам $0, \dots, n$ приготовления квантовой системы Q . Система M интуитивно может быть представлена как «измерительное устройство» Боба с базисом $|y\rangle$, элементы которого соответствуют возможным результатам измерения $1, \dots, n$, которое делает Боб. Предполагается, что начальное состояние общей системы можно представить в виде

$$\rho^{PQM} = \sum_x p_x |x\rangle\langle x| \otimes \rho_x \otimes |0\rangle\langle 0|, \quad (12.7)$$

где мы записываем разложение тензорного произведения в порядке PQM . Интуитивно понятно, что это состояние соответствует ситуации, когда Алиса выбрала значение x с вероятностью p_x , приготовила соответствующее ρ_x и передала его Бобу, который собирается использовать свою измеряющую аппаратуру, изначально находящуюся в стандартном состоянии $|0\rangle$, для проведения измерений. Введем квантовое преобразование \mathcal{E} , которое действует только на системы Q и M (но не на P), обеспечивая измерение с POVM элементами $\{E_y\}$ над системой Q и запоминание результата этого измерения в системе M :

$$\mathcal{E}(\sigma \otimes |0\rangle\langle 0|) \equiv \sum_y \sqrt{E_y} \sigma \sqrt{E_y} \otimes |y\rangle\langle y|, \quad (12.8)$$

где σ — любое состояние системы Q и $|0\rangle$ — начальное состояние измеряющей аппаратуры. В следующем упражнении вы увидите, что \mathcal{E} является квантовым преобразованием, сохраняющим след.

Упражнение 12.2. Определим U_y как унитарный оператор, действующий на систему M следующим образом: $U_y|y'\rangle \equiv |y'+y\rangle$, где сложение производится по модулю $n+1$. Покажите, что $\{\sqrt{E_y} \otimes U_y\}$ — набор элементов, определяющих сохраняющее след квантовое преобразование \mathcal{E} , действие которого на состояния вида $\sigma \otimes |0\rangle\langle 0|$ согласуется с (12.8).

Докажем границу Холево следующим образом. Используя штрихи для обозначения состояния PQM после применения \mathcal{E} и обозначения без штрихов для состояний до применения \mathcal{E} , имеем $S(P:Q) = S(P:Q, M)$, так как M изначально некоррелирована ни с P , ни с Q , и $S(P:Q, M) \geq S(P':Q', M')$, поскольку применение квантового преобразования \mathcal{E} к QM не может увеличить взаимную информацию P с QM (теорема 11.15), и, наконец, $S(P':Q', M') \geq S(P':M')$, так как исключение систем не может увеличить взаимную информацию (тоже теорема 11.15). Соединяя все результаты, получаем

$$S(P':M') \leq S(P:Q). \quad (12.9)$$

Это неравенство после несложных алгебраических преобразований превращается в границу Холево.

Сначала рассмотрим правую часть неравенства. Заметим, что

$$\rho^{PQ} = \sum_x p_x |x\rangle\langle x| \otimes \rho_x, \quad (12.10)$$

откуда следует, что $S(P) = H(p_x)$, $S(Q) = S(\rho)$ и $S(P, Q) = H(p_x) + \sum_x p_x S(\rho_x)$ (в соответствии с теоремой 11.10). Таким образом,

$$S(P:Q) = S(P) + S(Q) - S(P, Q) = S(\rho) - \sum_x p_x S(\rho_x), \quad (12.11)$$

а это и есть энтропия Холево! Теперь рассмотрим левую часть (12.9). Заметим, что

$$\rho^{P'Q'M'} = \sum_{xy} p_x |x\rangle\langle x| \otimes \sqrt{E_y} \rho_x \sqrt{E_y} \otimes |y\rangle\langle y|. \quad (12.12)$$

Взяв след по системе Q' и используя то, что совместное распределение вероятностей $p(x, y)$ для пары (X, Y) удовлетворяет равенствам $p(x, y) = p_x p(y|x) = p_x \text{tr}(\rho_x E_y) = p_x \text{tr}(\sqrt{E_y} \rho_x \sqrt{E_y})$, получаем

$$\rho^{P'M'} = \sum_{xy} p(x, y) |x\rangle\langle x| \otimes |y\rangle\langle y|, \quad (12.13)$$

откуда $S(P':M') = H(X:Y)$, а это как раз то, что нам нужно! Итак, граница Холево доказана! ■

12.1.2 Примеры применения границы Холево

Граница Холево — краеугольный камень в доказательстве множества результатов квантовой теории информации. Рассмотрим несколько примеров использования этого важного неравенства. Напомним теорему 11.10, которая утверждает, что

$$S(\rho) - \sum_x p_x S(\rho_x) \leq H(X), \quad (12.14)$$

причем равенство имеет место тогда и только тогда, когда носители состояний ρ_x ортогональны. Допустим, что носители состояний ρ_x не ортогональны, так что неравенство в (12.14) строгое. Тогда из границы Холево следует, что $H(X:Y)$ строго меньше $H(X)$, и поэтому Боб не может точно определить X на основе своего результата измерения Y . Таким образом, мы еще раз убеждаемся, что если состояния, приготовленные Алисой, не ортогональны, то Боб не может с уверенностью определить, какое состояние приготовила Алиса.

Пусть, например, Алиса приготовливает единственный кубит в одном из двух квантовых состояний в зависимости от того, что выпадет при бросании монеты. Если выпадет «орел», Алиса приготовливает состояние $|0\rangle$, а если выпадет «решка», Алиса приготовливает состояние $\cos \theta |0\rangle + \sin \theta |1\rangle$, где θ — некоторый вещественный параметр. Отсюда следует, что в базисе $|0\rangle, |1\rangle$ ρ можно записать в виде

$$\rho = \frac{1}{2} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \frac{1}{2} \begin{bmatrix} \cos^2 \theta & \cos \theta \sin \theta \\ \cos \theta \sin \theta & \sin^2 \theta \end{bmatrix}. \quad (12.15)$$

Простое вычисление показывает, что собственные значения ρ есть $(1 \pm \cos \theta)/2$ и, следовательно, энтропия Холево совпадает с двоичной энтропией $H((1 + \cos \theta)/2)$ (рис. 12.1). Отметим, что энтропия Холево достигает максимума (1 бит) при $\theta = \pi/2$, что соответствует случаю, когда Алиса приготавливает состояния, выбранные из ортогонального набора, и Боб может точно определить, какое состояние приготовила Алиса. Для остальных значений θ энтропия Холево строго меньше, чем 1 бит, и Боб не может точно определить, какое состояние приготовила Алиса.

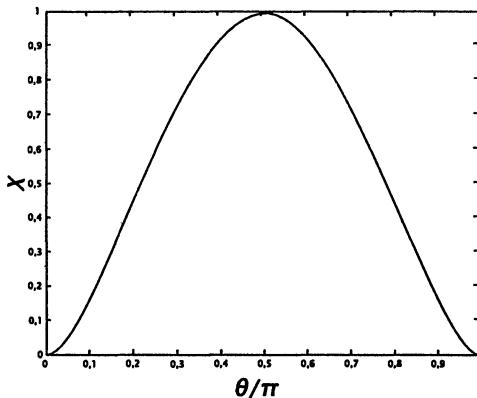


Рис. 12.1. Энтропия Холево χ как функция θ , когда состояния $|0\rangle$ и $\cos \theta|0\rangle + \sin \theta|1\rangle$ приготовлены с равными вероятностями. Отметим, что энтропия Холево достигает максимума при $\theta = \pi/2$, что соответствует ортогональным состояниям. Только в этой точке Боб может с уверенностью определить, какое состояние приготовила Алиса.

Границу Холево можно сделать более удобной для применения, используя неравенство Фано (во вставке 12.2 приведен вывод неравенства). Допустим, что Боб делает предположение $\tilde{X} = f(Y)$ о том, какое состояние приготовила Алиса, основываясь на результате своего измерения Y и некотором правиле построения предположения, описываемом функцией $f(\cdot)$. Тогда в соответствии с неравенством Фано и границей Холево,

$$\begin{aligned} H(p(\tilde{X} \neq X)) + p(\tilde{X} \neq X) \log(|X| - 1) &\geq H(X|Y) \\ &= H(X) - H(X:Y) \\ &\geq H(X) - \chi, \end{aligned} \quad (12.19)$$

что позволяет установить, с какой точностью Боб может определить значение X . Эвристически, чем меньше χ , тем труднее Бобу установить, какое состояние подготовила Алиса. Это проиллюстрировано на рис. 12.2 для случая, когда Алиса приготавливает $|0\rangle$ с вероятностью $1/2$ и $\cos \theta|0\rangle + \sin \theta|1\rangle$ с вероятностью $1/2$. При этом неравенство (12.19) сводится к $H(p(\tilde{X} \neq X)) \geq 1 - \chi$ и

$\chi = H((1 + \cos(\theta))/2)$, как уже ранее отмечалось. Заметим, что когда $\theta \neq \pi/2$, существует некоторая конечная вероятность того, что Боб сделает ошибку в своем предположении. Эта вероятность становится тем больше, чем ближе θ к нулю. Наконец, когда $\theta = 0$ и два состояния неразличимы, нижняя граница показывает, что, как мы и ожидали, вероятность ошибки Боба, по крайней мере, $\frac{1}{2}$, что не лучше, чем если бы он действовал наугад.

Упражнение 12.3. Используйте границу Холево для доказательства того, что n кубитов не могут быть использованы для передачи более чем n битов классической информации.

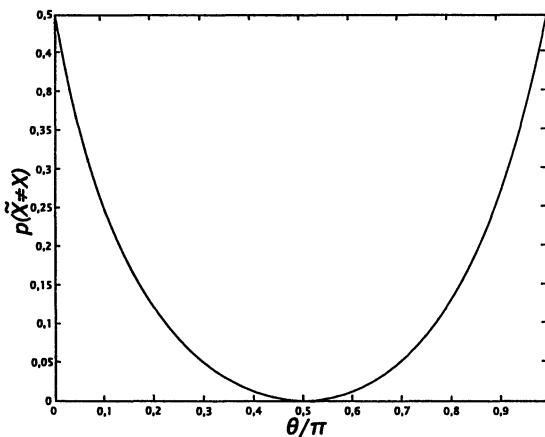


Рис. 12.2. Нижняя граница вероятности ошибки Боба в случае, когда Алиса приготавливает состояние $|0\rangle$ или $\cos\theta|0\rangle + \sin\theta|1\rangle$. Нижняя граница получена с использованием неравенства Фано и границы Холево. Эта граница равна нулю при $\theta = \pi/2$, когда состояния можно надежно различить.

Упражнение 12.4. Предположим, что Алиса посыпает Бобу равномерную смесь четырех чистых состояний

$$|X_1\rangle = |0\rangle, \quad (12.20)$$

$$|X_2\rangle = \sqrt{\frac{1}{3}} \left[|0\rangle + \sqrt{2}|1\rangle \right], \quad (12.21)$$

$$|X_3\rangle = \sqrt{\frac{1}{3}} \left[|0\rangle + \sqrt{2}e^{2\pi i/3}|1\rangle \right], \quad (12.22)$$

$$|X_4\rangle = \sqrt{\frac{1}{3}} \left[|0\rangle + \sqrt{2}e^{4\pi i/3}|1\rangle \right]. \quad (12.23)$$

Покажите, что максимум взаимной информации между результатом измерения Боба и состоянием, приготовленным Алисой, меньше одного бита. Известна POVM, которая достигает $\approx 0,415$ бит. Можете ли вы построить ее или даже лучшую, которая достигает границы Холево?

Вставка 12.2. Неравенство Фано

Допустим, что мы хотим узнать значение случайной величины X , основываясь на знании другой случайной величины Y . Интуитивно мы предполагаем, что условная энтропия $H(X|Y)$ определяет, насколько точно мы можем это сделать. *Неравенство Фано* делает наше интуитивное предположение строгим и устанавливает границу точности, с которой мы можем определить X при известном Y .

Предположим, что $\tilde{X} \equiv f(Y)$ — некоторая функция Y , которую мы используем в качестве нашего наилучшего предположения об X . Пусть $p_e \equiv p(X \neq \tilde{X})$ — вероятность того, что наше предположение неверно. Тогда неравенство Фано устанавливает, что

$$H(p_e) + p_e \log(|X| - 1) \geq H(X|Y), \quad (12.16)$$

где $H(\cdot)$ — двоичная энтропия и $|X|$ — число возможных значений X . Количественно неравенство показывает, что если $H(X|Y)$ велика (т. е. сравнима по величине с $\log(|X| - 1)$), то вероятность p_e совершения ошибки должна быть также велика.

Чтобы доказать неравенство Фано, определим «переменную ошибки», $E \equiv 1$, если $X \neq \tilde{X}$ и $E \equiv 0$, если $X = \tilde{X}$. Заметим, что $H(E) = H(p_e)$. Используя цепное правило для условных энтропий, получаем $H(E, X|Y) = H(E|X, Y) + H(X|Y)$. Но E полностью определена, если известны X и Y , так что $H(E|X, Y) = 0$ и, следовательно, $H(E, X|Y) = H(X|Y)$. Вновь используя цепное правило для энтропий, находим $H(E, X|Y) = H(X|E, Y) + H(E|Y)$. Применение дополнительных условий уменьшает энтропию, так что $H(E|Y) \leq H(E) = H(p_e)$, и, следовательно, $H(X|Y) = H(E, X|Y) \leq H(X|E, Y) + H(p_e)$. Доказательство неравенства Фано завершается оцениванием $H(X|E, Y)$ следующим образом (мы опустили несколько простых алгебраических деталей, которые вы легко восстановите):

$$H(X|E, Y) = p(E = 0)H(X|E = 0, Y) + p(E = 1)H(X|E = 1, Y), \quad (12.17)$$

$$\leq p(E = 0) \times 0 + p_e \log(|X| - 1) = p_e \log(|X| - 1), \quad (12.18)$$

где неравенство $H(X|E = 1, Y) \leq \log(|X| - 1)$ следует из того факта, что при $E = 1$ имеем $X \neq Y$ и X может принимать не больше, чем $|X| - 1$ значений, что ограничивает энтропию X , и, следовательно, условную энтропию X величиной $\log(|X| - 1)$. Подставляя $H(X|E, Y) \leq p_e \log(|X| - 1)$ в $H(X|Y) \leq H(X|E, Y) + H(p_e)$, получаем неравенство Фано $H(X|Y) \leq H(p_e) + p_e \log(|X| - 1)$.

12.2 Сжатие данных

Элементарный динамический процесс — сжатие данных — рассматривается как в классической, так и в квантовой теории информации. В самом общем виде

проблема сжатия данных заключается в том, чтобы определить, *какие минимальные физические ресурсы требуются для хранения информации источника?* Это одна из фундаментальных проблем теории информации. Оказывается, что методы решения этой проблемы как в классической, так и в квантовой теории информации имеют гораздо большую область применения, чем собственно сжатие данных. В этом разделе мы детально изучим как квантовое, так и классическое сжатие данных.

12.2.1 Теорема Шеннона о кодировании для канала без шума

Теорема Шеннона о кодировании для канала без шума количественно определяет степень, до которой можно сжать информацию, создаваемую источником классической информации.¹ Что мы понимаем под источником классической информации? Возможны разные модели такого источника. Простая и очень важная модель источника — это последовательность случайных величин X_1, X_2, \dots , значения которых представляют собой данные на выходе источника. Удобно предположить, что эти случайные величины принимают значения из конечного алфавита символов, хотя обобщения на бесконечные алфавиты тоже возможны. Более того, будем считать, что случайные величины X_i независимы и одинаково распределены; такой источник информации называется *стационарным*. В реальном мире подобные источники не часто встречаются. Легко увидеть, что буквы в английском тексте не располагаются независимо друг от друга; между буквами существует сильная корреляция. Например, буква «h» встречается после буквы «t» гораздо чаще, чем можно ожидать, основываясь на общей частоте, с которой буква «h» встречается в обычном английском тексте. Мы говорим, что появления букв «t» и «h» не являются независимыми, между ними есть корреляция. Тем не менее, на практике многие источники информации (включая английский текст) можно рассматривать как стационарные, и методы, разработанные для стационарного источника, могут быть обобщены на более сложные источники.

Прежде чем перейти к техническим деталям теоремы Шеннона, используем простой пример, чтобы интуитивно понять результат. Пусть стационарный источник информации выдает биты X_1, X_2, X_3, \dots , каждый из которых может быть равен нулю с вероятностью p и единице с вероятностью $1 - p$. Основная идея, на которой основана теорема Шеннона, разделить возможные последовательности значений x_1, \dots, x_n случайных величин X_1, \dots, X_n , на *типичные последовательности*, которые встречаются с большой вероятностью, и *нетипичные последовательности*, которые встречаются редко. Как это делается? Мы предполагаем, что при больших n с большой вероятностью доля символов «0» на выходе источника будет равна p , а доля символов «1» будет равна $1 - p$. Последовательности x_1, \dots, x_n , для которых это предположение справедливо,

¹ Задача о сжатии информации эквивалентна задаче о кодировании информации для передачи по каналу без шума. При этом степень сжатия соответствует скорости передачи. В дальнейшем более общий термин «скорость передачи» будет использоваться для количественного описания степени сжатия — Прим. ред.

называются *типовыми последовательностями*. Используя предположение о стационарности для данного источника, получим

$$p(x_1, \dots, x_n) = p(x_1)p(x_2) \dots p(x_n) \approx p^{np}(1-p)^{(1-p)n} \quad (12.24)$$

для типовых последовательностей. Возьмем логарифм от обеих частей выражения:

$$-\log p(x_1, \dots, x_n) \approx -np \log p - n(1-p) \log(1-p) = nH(X), \quad (12.25)$$

где X — случайная величина, распределенная в соответствии с распределением источника, и $H(X) = -p \log(p) - (1-p) \log(1-p)$ — энтропия данного источника, называемая *скоростью создания сообщений*. Таким образом, $p(x_1, \dots, x_n) \approx 2^{-nH(X)}$, откуда видно, что может быть не больше $2^{nH(X)}$ типовых последовательностей, поскольку полная вероятность всех типовых последовательностей не может быть больше единицы.

Теперь у нас есть средства, чтобы понять простую схему сжатия данных. Предположим, что данные на выходе источника x_1, \dots, x_n . Чтобы сжать эти данные, мы должны убедиться, действительно ли последовательность x_1, \dots, x_n типовая. Если нет, мы считаем, что произошла ошибка. К счастью, при больших n это случается очень редко, поскольку почти все последовательности типовые в пределе больших n . Если на выходе типовая последовательность, мы ее сжимаем. Поскольку существует не больше $2^{nH(X)}$ типовых последовательностей, требуется только $nH(X)$ битов, чтобы однозначно задать типовую последовательность. Мы выбираем некоторую схему кодирования типовых последовательностей и производим сжатие выходных данных источника до соответствующей строки $nH(X)$ битов, описывающей встретившуюся типовую последовательность; позже эта строка может быть развернута. При больших n данная схема работает корректно с вероятностью, приближающейся к единице.

Эта схема вызывает несколько критических замечаний: (а) Схема имеет маленькую, но конечную вероятность сбоя. В немного более сложных схемах используются похожие идеи, чтобы исключить возможность совершения ошибки. (б) Чтобы произвести сжатие, мы должны подождать до тех пор, пока источник не выдаст большое число n символов. Существуют варианты данной схемы, которые позволяют производить обработку по мере того, как источник выдает символы. (в) Не предложена явная схема, преобразующая выходные данные источника в сжатые последовательности. Однако небольшим усложнением алгоритма эта проблема может быть решена. (г) Конкретная процедура сжатия данных зависит от распределения выходных данных источника. А если это распределение неизвестно? В этом случае можно воспользоваться алгоритмами *универсального сжатия*. Читателю, интересующемуся этими и другими вопросами, мы рекомендуем обратиться к книге Ковера и Томаса, ссылка на которую дана в разд. «История и дополнительная литература» в конце главы.

Расширим понятие типовых последовательностей за рамки двоичного случая. Пусть X_1, X_2, X_3, \dots — стационарный источник информации. Обычно частота появления данной буквы x в последовательности на выходе источника

близка к вероятности $p(x)$ этой буквы. Имея это в виду, мы дадим следующее строгое определение понятия типичной последовательности. Задавая $\varepsilon > 0$, мы говорим, что строка символов x_1, x_2, \dots, x_n источника ε -типичная, если

$$2^{-n(H(X)+\varepsilon)} \leq p(x_1, \dots, x_n) \leq 2^{-n(H(X)-\varepsilon)}, \quad (12.26)$$

и обозначаем набор всех таких ε -типичных последовательностей длины n как $T(n, \varepsilon)$. Это определение может быть переформулировано в следующем эквивалентном виде

$$\left| \frac{1}{n} \log \frac{1}{p(x_1, \dots, x_n)} - H(X) \right| \leq \varepsilon. \quad (12.27)$$

Используя закон больших чисел (сформулированный и доказанный во вставке 12.3), мы можем доказать *теорему о типичных последовательностях*, которая строго выражает идею о том, что в пределе больших n большинство последовательностей на выходе источника информации являются типичными.

Теорема 12.2 (теорема о типичных последовательностях).

1. Пусть $\varepsilon > 0$. Тогда для любого $\delta > 0$ при достаточно больших n вероятность того, что последовательность ε -типичная, не меньше, чем $1 - \delta$.
2. Для любого фиксированного $\varepsilon > 0$ и $\delta > 0$ при достаточно больших n число $|T(n, \varepsilon)|$ ε -типичных последовательностей удовлетворяет неравенствам

$$(1 - \delta)2^{n(H(X)-\varepsilon)} \leq |T(n, \varepsilon)| \leq 2^{n(H(X)+\varepsilon)}. \quad (12.28)$$

3. Пусть $S(n)$ — набор не более, чем 2^{nR} последовательностей длины n с выхода источника, где $R < H(x)$ — фиксированное число. Тогда для любых $\delta > 0$ и достаточно больших n

$$\sum_{x \in S(n)} p(x) \leq \delta. \quad (12.29)$$

Доказательство.

Часть 1. Непосредственное применение закона больших чисел. Заметим, что $\log p(X_i)$ — независимые, одинаково распределенные случайные величины. Согласно закону больших чисел, для любого $\varepsilon > 0$ и $\delta > 0$ при достаточно больших n имеем

$$p \left(\left| \sum_{i=1}^n \frac{-\log p(X_i)}{n} - \mathbf{E}(-\log p(X)) \right| \leq \varepsilon \right) \geq 1 - \delta. \quad (12.30)$$

Но $\mathbf{E}(\log p(X)) = -H(X)$ и $\sum_{j=1}^n \log p(X_i) = \log(p(X_1, \dots, X_n))$. Таким образом,

$$p(|-\log(p(X_1, \dots, X_n))/n - H(X)| \leq \varepsilon) \geq 1 - \delta, \quad (12.31)$$

т. е. вероятность того, что последовательность ε -типичная, не меньше, чем $1 - \delta$.

Часть 2. Следует из определения типичности и наблюдения, что сумма вероятностей типичных последовательностей должна лежать в интервале от $1 - \delta$ (из части 1) до 1 (поскольку сумма вероятностей не может быть больше 1). Поэтому

$$1 \geq \sum_{x \in T(n, \epsilon)} \geq \sum_{x \in T(n, \epsilon)} 2^{-n(H(X)+\epsilon)} = |T(n, \epsilon)| 2^{-n(H(X)+\epsilon)}, \quad (12.32)$$

откуда получаем $|T(n, \epsilon)| \leq 2^{n(H(X)+\epsilon)}$, и

$$1 - \delta \leq \sum_{x \in T(n, \epsilon)} p(x) \leq \sum_{x \in T(n, \epsilon)} 2^{-n(H(X)+\epsilon)} = |T(n, \epsilon)| 2^{-n(H(X)+\epsilon)}, \quad (12.33)$$

так что $|T(n, \epsilon)| \geq (1 - \delta) 2^{n(H(X)-\epsilon)}$.

Часть 3. Идея заключается в разделении последовательностей в $S(n)$ на типичные и нетипичные последовательности. Нетипичные последовательности имеют малую вероятность в пределе больших n . Число типичных последовательностей в $S(n)$, очевидно, не больше, чем общее число последовательностей в $S(n)$, которое не превышает 2^{nR} , и каждая типичная последовательность имеет вероятность приблизительно $2^{nH(X)}$. Полная вероятность типичных последовательностей в $S(n)$ порядка $2^{n(R-H(X))}$ и стремится к нулю при $R < H(x)$.

Более строго, выберем ϵ так, чтобы $R < H(x) - \delta$ и $0 < \epsilon < \delta/2$. Разделим последовательности в $S(n)$ на ϵ -типичные и ϵ -нетипичные последовательности. Из части 1 следует, что для достаточно больших n полную вероятность нетипичных последовательностей можно сделать меньше $\delta/2$. В $S(n)$ имеется не более 2^{nR} типичных последовательностей, каждая с вероятностью не более $2^{-n(H(X)-\epsilon-R)}$, так что вероятность типичных последовательностей не более $2^{n(H(X)-\epsilon)}$ и стремится к нулю при $n \rightarrow \infty$. Таким образом, полная вероятность последовательностей в $S(n)$ меньше, чем δ , для достаточно больших n . ■

Теорема Шеннона о кодировании для канала без шума является простым примером применения теоремы о типичных последовательностях. Мы приводим здесь очень простую версию теоремы о кодировании для канала без шума. Более сложные версии оставим для упражнений (см. также разд. «История и дополнительная литература» в конце главы). Предположим, что X_1, X_2, \dots — стационарный классический источник информации, определенный на некотором конечном алфавите, содержащем d символов. Схема сжатия в $1/R$ раз (R — скорость передачи) отображает последовательности $x = (x_1, \dots, x_n)$ в битовые строки длины nR , которые мы обозначим как $C^n(x) = C^n(x_1, \dots, x_n)$. (Заметим, что nR может и не быть целым. Мы упростим обозначения, считая, что в данном случае $nR = \lfloor nR \rfloor$.) Соответствующая схема развертывания отображает nR сжатых битов обратно в строку из n букв алфавита $D^n(C^n(x))$. Схема сжатия-развертывания (C^n, D^n) является надежной, если вероятность того, что $D^n(C^n(x)) = x$, стремится к единице, когда n стремится к бесконечности. Теорема Шеннона о кодировании для канала без шума определяет, для каких значений скорости передачи R существует надежная схема сжатия, обнаруживая замечательную интерпретацию энтропии $H(X)$ как минимального

количества физических ресурсов, необходимого и достаточного для надежного хранения данных, создаваемых источником.

Теорема 12.3 (теорема Шеннона о кодировании для канала без шума). Пусть $\{X_i\}$ — стационарный источник информации с энтропией $H(X)$. Предположим, что $R > H(X)$. Тогда для этого источника информации существует надежная схема сжатия в $1/R$ раз. В противном случае, когда $R < H(X)$, любая схема сжатия не является надежной.

Доказательство. Предположим, что $R > H(X)$. Выберем $\varepsilon > 0$, так что $H(X) + \varepsilon < R$. Рассмотрим набор ε -типичных последовательностей $T(n, \varepsilon)$. Для любых $\delta > 0$ и достаточно больших n существует не больше $2^{n(H(X)+\varepsilon)} < 2^{nR}$ таких последовательностей, и вероятность того, что источник создает одну из таких последовательностей, не меньше, чем $1 - \delta$. Следовательно, прежде, чем производить сжатие, нужно определить, являются ли выходные данные источника ε -типичной последовательностью. Если выходные данные не являются такой последовательностью, сжимаем их до некоторой фиксированной nR -битовой строки, которая указывает на сбой. Операция развертывания этой строки дает на выходе случайную последовательность x_1, \dots, x_n как предположение об информации, выданной источником. В этом случае нам не удалось сжать данные. Если выходные данные источника типичные, мы сжимаем выходную информацию, сохраняя nR -битовый номер, соответствующий этой типичной последовательности, что позволяет потом очевидным образом восстановить данные.

Пусть $R < H(X)$. Комбинированная операция сжатия-развертывания обладает не более, чем 2^{nR} возможными выходными наборами данных, так что не больше, чем 2^{nR} последовательностей на выходе источника могут быть подвергнуты операциям сжатия и развертывания без ошибки. Из теоремы о типичных последовательностях следует, что для достаточно больших n вероятность того, что последовательность на выходе источника принадлежит подмножеству 2^{nR} последовательностей, стремится к нулю при $R < H(X)$. Таким образом, любая такая схема сжатия не может быть надежной. ■

Вставка 12.3. Закон больших чисел

Предположим, что мы повторяем эксперимент много раз, каждый раз измеряя значение некоторого параметра X . Обозначим результаты экспериментов как X_1, X_2, \dots . Допуская, что результаты экспериментов независимы, мы интуитивно ожидаем, что значение оценки $S_n \equiv \sum_{i=1}^n X_i/n$ среднего $E(X)$ должно стремиться к $E(X)$ при $n \rightarrow \infty$. Закон больших чисел — строгое подтверждение нашего интуитивного предположения.

Теорема 12.4 (закон больших чисел). Пусть X_1, X_2, \dots — независимые случайные величины, имеющие такое же распределение, что и случайная величина X с конечными первым и вторым моментами: $E(X) < \infty$ и $E(X^2) < \infty$. Тогда для любых $\varepsilon > 0$ имеем $p(S_n - E(X) > \varepsilon) \rightarrow 0$ при $n \rightarrow \infty$.

Доказательство. Предположим сначала, что $\mathbf{E}(X) = 0$, а в конце доказательства теоремы обсудим, что происходит, когда $\mathbf{E}(X) \neq 0$. Поскольку случайные величины независимы и их среднее значение равно нулю, то $\mathbf{E}(X_i X_j) = \mathbf{E}(X_i)\mathbf{E}(X_j) = 0$ при $i \neq j$ и, следовательно,

$$\mathbf{E}(S_n^2) = \frac{\sum_{i,j=1}^n \mathbf{E}(X_i X_j)}{n^2} = \frac{\sum_{i=1}^n \mathbf{E}(X_i^2)}{n^2} = \frac{\mathbf{E}(X^2)}{n}, \quad (12.34)$$

где последнее равенство следует из того факта, что X_1, \dots, X_n распределены так же, как X . Из определения математического ожидания имеем

$$\mathbf{E}(S_n^2) = \int dP S_n^2, \quad (12.35)$$

где dP — мера вероятности. Ясно, что либо $|S_n| \leq \varepsilon$, либо $|S_n| > \varepsilon$, так что можно разделить интеграл на две части, а затем отбросить одну из них, поскольку она неотрицательна,

$$\mathbf{E}(S_n^2) = \int_{|S_n| \leq \varepsilon} dP S_n^2 + \int_{|S_n| > \varepsilon} dP S_n^2 \geq \int_{|S_n| > \varepsilon} dP S_n^2. \quad (12.36)$$

В области интегрирования $S_n^2 > \varepsilon^2$, и, следовательно,

$$\mathbf{E}(S_n^2) \geq \varepsilon \int_{|S_n| > \varepsilon} dP = \varepsilon^2 p(|S_n| > \varepsilon). \quad (12.37)$$

Сравнивая это неравенство с (12.34), мы видим, что

$$p(|S_n| > \varepsilon) \leq \frac{\mathbf{E}(X^2)}{n\varepsilon^2}. \quad (12.38)$$

Положив $n \rightarrow \infty$, завершим доказательство. В случае $\mathbf{E}(X) \neq 0$ легко получить результат, введя величины

$$Y_i \equiv X_i - \mathbf{E}(X), \quad Y \equiv X - \mathbf{E}(X). \quad (12.39)$$

которые независимы и одинаково распределены, причем $\mathbf{E}(Y) = 0$ и $\mathbf{E}(Y^2) < \infty$. Дальнейшее доказательство повторяет рассуждения, приведенные выше. ■

Упражнение 12.5 (сжатие данных переменной длины с нулевой ошибкой). Рассмотрим следующий эвристический подход для схемы сжатия данных переменной длины. Пусть x_1, \dots, x_n — данные на выходе после n обращений к стационарному источнику с энтропией $H(X)$. Если последовательность x_1, \dots, x_n типичная, посылаем $nH(X)$ — битовый номер этой типичной последовательности. Если последовательность x_1, \dots, x_n — нетипичная, посы-

ляем несжатое $\log d^n$ — битовое представление данной последовательности (напомним, что d — размер алфавита). На основе нашего эвристического предположения докажите, что этот источник может быть сжат в среднем до R бит на каждый символ данных на выходе источника для любых $R > H(X)$ с нулевой вероятностью ошибки.

12.2.2 Теорема Шумахера о кодировании для квантового канала без шума

Принципиальной особенностью квантовой теории информации является то, что квантовые состояния рассматриваются как *информация* и изучаются с теоретико-информационной точки зрения. В этом разделе мы дадим определение квантового источника информации и изучим вопрос, до какой степени может быть сжата созданная источником «информация», т. е. квантовые состояния.

Как определить понятие квантового источника информации? Как и в случае классического источника информации, когда совершенно не очевидно, как это сделать наилучшим образом. Можно привести несколько разных определений, не все из которых эквивалентны. Определение, которое мы будем использовать, основано на том, что мы хотим сжимать и развертывать *запутанные состояния*. Более формально (стационарный) квантовый источник будет описываться гильбертовым пространством H и матрицей плотности ρ в этом пространстве. Мы предполагаем, что ρ — состояние системы, являющейся частью большей системы, которая находится в чистом состоянии. *Схема сжатия* в $1/R$ раз для данного источника состоит из двух семейств квантовых преобразований C^n и D^n , аналогичных операциям сжатия и развертывания, используемым в классическом случае. C^n — преобразование сжатия, переводящее состояния из $H^{\otimes n}$ в состояния 2^{nR} -мерного пространства, *сжатого пространства*. Мы можем представить сжатое пространство nR кубитами. D^n — преобразование развертывания, которое переводит состояния сжатого пространства в состояния исходного пространства состояний. Таким образом, комбинированное преобразование «сжатие-развертывание» — это $D^n \circ C^n$. Нашим критерием надежности является то, что в пределе больших n точность воспроизведения запутанности $F(\rho^{\otimes n}, D^n \circ C^n)$ должна стремиться к единице. Основная идея квантового сжатия данных проиллюстрирована на рис. 12.3.

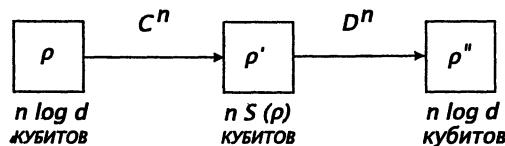


Рис. 12.3. Квантовое сжатие данных. Преобразование сжатия C^n , скимая квантовый источник ρ , переводит $n \log d$ кубитов в $nS(\rho)$ кубитов. Состояние источника корректно восстанавливается с помощью преобразования развертывания D^n .

Основным техническим понятием, на котором основана квантовая теорема о кодировании для канала без шума, является квантовый аналог понятия типичных последовательностей. Приведем оператор плотности ρ , связанный с квантовым источником информации, к диагональному виду

$$\rho = \sum_x p(x) |x\rangle\langle x|, \quad (12.40)$$

где $|x\rangle$ — ортонормированный базис и $p(x)$ — собственные значения ρ . Эти собственные значения имеют те же свойства, что и распределения вероятностей: они неотрицательны и их сумма равна единице. Более того, $H(p(x)) = S(\rho)$. Следовательно, имеет смысл рассмотреть ε -типичную последовательность x_1, \dots, x_n , для которой как и в классическом случае,

$$\left| \frac{1}{n} \log \left(\frac{1}{p(x_1)p(x_2)\dots p(x_n)} \right) - S(\rho) \right| \leq \varepsilon, \quad (12.41)$$

ε -типичное состояние — это состояние $|x_1\rangle|x_2\rangle\dots|x_n\rangle$, для которого последовательность x_1, \dots, x_n — является ε -типичной. Определим ε -типичное подпространство как пространство, порожденное всеми ε -типичными состояниями $|x_1\rangle|x_2\rangle\dots|x_n\rangle$. Обозначим ε -типичное подпространство через $T(n, \varepsilon)$ и проектор на ε -типичное подпространство через $P(n, \varepsilon)$. Отметим, что

$$P(n, \varepsilon) = \sum_{x, \varepsilon - \text{типичная}} |x_1\rangle\langle x_1| \otimes |x_2\rangle\langle x_2| \otimes \dots \otimes |x_n\rangle\langle x_n|. \quad (12.42)$$

Теперь теорема о типичных последовательностях может быть преобразована в эквивалентную квантовую форму, иначе говоря, в теорему о типичном подпространстве.

Теорема 12.5 (теорема о типичном подпространстве).

- Пусть $\varepsilon > 0$. Тогда для любого $\delta > 0$ и достаточно больших n

$$\text{tr}(P(n, \varepsilon)\rho^{\otimes n}) \geq 1 - \delta. \quad (12.43)$$

- Для любого фиксированного $\varepsilon > 0$ и $\delta > 0$ при достаточно больших n размерность $T(n, \varepsilon)$, $|T(n, \varepsilon)| = \text{tr}(P(n, \varepsilon))$ удовлетворяет неравенствам

$$(1 - \delta)2^{n(S(\rho) - \varepsilon)} \leq |T(n, \varepsilon)| \leq 2^{n(S(\rho) + \varepsilon)}. \quad (12.44)$$

- Пусть $S(n)$ — проектор на любое подпространство в $H^{\otimes n}$ размерности не более 2^{nR} , где величина $R < S(\rho)$ фиксированная. Тогда для любого $\delta > 0$ и достаточно больших n

$$\text{tr}(S(n)\rho^{\otimes n}) \leq \delta. \quad (12.45)$$

В каждом случае результат может быть непосредственно получен при помощи закона больших чисел, но мы предпочитаем использовать теорему о типичных последовательностях, чтобы подчеркнуть тесную связь с методами, использованными в доказательстве теоремы Шеннона о кодировании для канала без шума.

Доказательство.

Часть 1. Отметим, что

$$\mathrm{tr}(P(n, \varepsilon) \rho^{\otimes n}) = \sum_{x, \varepsilon - \text{типичная}} p(x_1)p(x_2) \dots p(x_n). \quad (12.46)$$

Результат непосредственно вытекает из части 1 теоремы о типичных последовательностях.

Часть 2. Непосредственно следует из части 2 теоремы о типичных последовательностях.

Часть 3. Разобъем левую часть (12.45) на след по типичному подпространству и след по нетипичному подпространству

$$\mathrm{tr}(S(n) \rho^{\otimes n}) = \mathrm{tr}(S(n) \rho^{\otimes n} P(n, \varepsilon)) + \mathrm{tr}(S(n) \rho^{\otimes n} (I - P(n, \varepsilon))), \quad (12.47)$$

и оценим каждый член отдельно. Для первого члена получаем

$$\rho^{\otimes n} P(n, \varepsilon) = P(n, \varepsilon) \rho^{\otimes n} P(n, \varepsilon), \quad (12.48)$$

поскольку $P(n, \varepsilon)$ — проектор, который коммутирует с $\rho^{\otimes n}$. Однако,

$$\mathrm{tr}(S(n) P(n, \varepsilon) \rho^{\otimes n} P(n, \varepsilon)) \leq 2^{nR} 2^{-n(S(\rho) - \varepsilon)}, \quad (12.49)$$

поскольку собственные значения $P(n, \varepsilon) \rho^{\otimes n} P(n, \varepsilon)$ ограничены сверху значением $2^{n(S(\rho)\varepsilon)}$. Мы видим, что при $n \rightarrow \infty$ первое слагаемое (12.47) стремится к нулю. Отметим, что $S(n) \leq I$. Поскольку $S(n)$ и $\rho^{\otimes n}(I - P(n, \varepsilon))$ — положительные операторы, получаем $0 \leq \mathrm{tr}(S(n) \rho^{\otimes n}(I - P(n, \varepsilon))) \leq \mathrm{tr}(\rho^{\otimes n}(I - P(n, \varepsilon))) \rightarrow 0$ при $n \rightarrow \infty$, так что второе слагаемое тоже стремится к нулю при больших n , что и требовалось доказать. ■

Используя теорему о типичном подпространстве, нетрудно доказать квантовый аналог теоремы Шеннона о кодировании для канала без шума. Основные идеи доказательства аналогичны, однако, оно несколько сложнее из-за появления некоммутирующих операторов, которые не имеют классических аналогов.

Теорема 12.6 (теорема Шумахера о кодировании для канала без шума). Пусть $\{H, \rho\}$ — стационарный квантовый источник. Если $R > S(\rho)$, то существует надежная схема сжатия в $1/R$ раз для источника $\{H, \rho\}$. Если $R < S(\rho)$, то любая такая схема сжатия не надежна.

Доказательство.

Пусть $R > S(\rho)$ и $\varepsilon > 0$ такое, что $S(\rho) + \varepsilon \leq R$. В соответствии с теоремой о типичном подпространстве для любого $\delta > 0$ и при достаточно больших n имеем $\mathrm{tr}(\rho^{\otimes n} P(n, \varepsilon)) \geq 1 - \delta$, и $\dim(T(n, \varepsilon)) \leq 2^{nR}$. Пусть H_c^n — любое 2^{nR} -мерное

гильбертово пространство, содержащее $T(n, \varepsilon)$. Кодирование производится следующим образом. Сначала выполняется измерение, которое описывается полным набором ортогональных проекторов $P(n, \varepsilon)$ и $I - P(n, \varepsilon)$; соответствующие результаты мы обозначаем 0 и 1. Если результат измерения 0, больше ничего не делаем и данное состояние остается в типичном подпространстве. Если на выходе 1, заменяя данное состояние системы некоторым стандартным состоянием $|0\rangle$, выбранным из типичного подпространства; неважно, какое состояние используется. Следовательно, кодирование является отображением $\mathcal{C}^n : H^{\otimes n} \rightarrow H_c^n$ в 2^{nR} -мерное подпространство H_c^n , имеющим представление в виде операторной суммы

$$\mathcal{C}^n(\sigma) \equiv P(n, \varepsilon)\sigma P(n, \varepsilon) + \sum_i A_i \sigma A_i^\dagger, \quad (12.50)$$

где $A_i \equiv |0\rangle\langle i|$ и $|i\rangle$ — ортонормированный базис для ортогонального дополнения к типичному подпространству.

Преобразование декодирования $\mathcal{D}^n : H_c^n \rightarrow H^{\otimes n}$, по определению, тождественно на H_c^n , $\mathcal{D}^n(\sigma) = \sigma$. Из этих определений для кодирования и декодирования следует, что

$$F(\rho^{\otimes n}, \mathcal{D}^n \circ \mathcal{C}^n) = |\text{tr}(\rho^{\otimes n} P(n, \varepsilon))|^2 + \sum_i |\text{tr}(\rho^{\otimes n} A_i)|^2 \quad (12.51)$$

$$\geq |\text{tr}(\rho^{\otimes n} P(n, \varepsilon))|^2 \quad (12.52)$$

$$\geq |1 - \delta|^2 \geq 1 - 2\delta, \quad (12.53)$$

где предпоследнее неравенство следует из теоремы о типичном подпространстве. Однако, δ может быть сколь угодно малым для достаточно больших n , и, следовательно, существует надежная схема сжатия $\{\mathcal{C}^n, \mathcal{D}^n\}$ при скорости передачи R , когда $S(\rho) < R$.

Чтобы доказать обратное утверждение, предположим, что $R < S(\rho)$. Без потери общности допустим, что преобразование сжатия отображает из $H^{\otimes n}$ на 2^{nR} -мерное подпространство с соответствующим проектором $S(n)$. Пусть C_j — элементы преобразования сжатия \mathcal{C}^n и D_k — элементы преобразования развертывания \mathcal{D}^n . Тогда имеем

$$F(\rho^{\otimes n}, \mathcal{D}^n \circ \mathcal{C}^n) = \sum_{jk} |\text{tr}(D_k C_j \rho^{\otimes n})|^2. \quad (12.54)$$

Каждый из операторов C_j действует в подпространстве с проектором $S(n)$, так что $C_j = S(n)C_j$. Пусть $S^k(n)$ — проектор на подпространство, в которое подпространство $S(n)$ отображается при помощи D_k , так что имеем $S^k(n)D_k S(n) = D_k S(n)$ и, следовательно, $D_k C_j = D_k S(n)C_j = S^k(n)D_k S(n)C_j = S^k(n)D_k C_j$, откуда

$$F(\rho^{\otimes n}, \mathcal{D}^n \circ \mathcal{C}^n) = \sum_{jk} |\text{tr}(D_k C_j \rho^{\otimes n} S^k(n))|^2. \quad (12.55)$$

Используя неравенство Коши–Шварца, получаем

$$F(\rho^{\otimes n}, \mathcal{D}^n \circ \mathcal{C}^n) \leq \sum_{jk} \text{tr}(D_k C_j \rho^{\otimes n} C_j^\dagger D_k^\dagger) \text{tr}(S^k(n) \rho^{\otimes n}). \quad (12.56)$$

Применяя часть 3 теоремы о типичном подпространстве, убеждаемся, что $\text{tr}(S^k(n) \rho^{\otimes n}) \leq \delta$ для любого $\delta > 0$ и достаточно больших n . Более того, при доказательстве теоремы о типичном подпространстве подразумевается, что необходимый размер n не зависит от k . Таким образом,

$$F(\rho^{\otimes n}, \mathcal{D}^n \circ \mathcal{C}^n) \leq \delta \sum_{jk} \text{tr}(D_k C_j \rho^{\otimes n} C_j^\dagger D_k^\dagger) \quad (12.57)$$

$$= \delta, \quad (12.58)$$

поскольку \mathcal{C}^n и \mathcal{D}^n сохраняют след. Так как δ может быть произвольным, $F(\rho^{\otimes n}, \mathcal{D}^n \circ \mathcal{C}^n) \rightarrow 0$ при $n \rightarrow \infty$, и поэтому схема сжатия не надежна. ■

Теорема Шумахера не только утверждает *существование* надежной схемы сжатия, но и указывает, как ее построить. Для этого нужно эффективно осуществить отображение $\mathcal{C}^n : H^{\otimes n} \rightarrow H_c^n$ в 2^{nR} -мерное типичное подпространство H_c^n . Классические методы сжатия, такие как кодирование перечислением, кодирование Хафмана и арифметическое кодирование, могут применяться только с одним строгим ограничением: схема кодирования должна быть полностью *обратимой*, а начальное состояние должно быть полностью уничтожено в процессе создания сжатого состояния согласно теореме о невозможности копирования. Простой пример, иллюстрирующий квантовое сжатие, приведен во вставке 12.4.

Вставка 12.4. Сжатие Шумахера

Рассмотрим стационарный квантовый источник, который характеризуется матрицей плотности кубита

$$\rho = \frac{1}{4} \begin{bmatrix} 3 & 1 \\ 1 & 1 \end{bmatrix}. \quad (12.59)$$

Он может быть, например, малой частью большой запутанной системы. Другой подход к рассмотрению данного источника (см. разд. 9.3) состоит в следующем. Источник создает состояние $|\psi_0\rangle = |0\rangle$ или $|\psi_1\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ с одинаковыми вероятностями, равными $\frac{1}{2}$ (см. упр. 12.8). Матрицу плотности ρ можно привести к диагональному виду $p|\bar{0}\rangle\langle\bar{0}| + (1-p)|\bar{1}\rangle\langle\bar{1}|$, где $|\bar{0}\rangle = \cos \frac{\pi}{8}|0\rangle + \sin \frac{\pi}{8}|1\rangle$, $|\bar{1}\rangle = \sin \frac{\pi}{8}|0\rangle + \cos \frac{\pi}{8}|1\rangle$, и $p = [3 + \operatorname{tg}(\pi/8)]/4$. В этом базисе блок из n кубитов может быть записан как состояние

$$\sum_{X \in \{\bar{0}\bar{0}, \bar{0}, \bar{1}, \bar{1}\}} C_X |X\rangle. \quad (12.60)$$

Из теоремы 12.6 следует, что нужно передавать только те $|X\rangle$, для которых вес Хэмминга приблизительно равен pr (т. е. базис для типичного подпространства), чтобы можно было воспроизвести начальное состояние с большой точностью. Это легко понять, поскольку $|\langle\bar{0}|\psi_k\rangle| = \cos(\pi/8)$ (для $k = \{0, 1\}$) намного больше, чем $|\langle\bar{1}|\psi_k\rangle| = \sin(\pi/8)$, и для X с большим весом Хэмминга коэффициенты C_X очень малы.

Как же все-таки реализовать такую схему сжатия? Опишем один приближенный способ. Предположим, что у нас есть квантовая схема U_n , которая переставляет базисные состояния $|X\rangle$, упорядочивая их в соответствии с весом Хэмминга. Например, для $n = 4$ это выглядит так

$0000 \rightarrow 0000$	$1000 \rightarrow 0100$	$1001 \rightarrow 1000$	$1011 \rightarrow 1100$
$0001 \rightarrow 0001$	$0011 \rightarrow 0101$	$1010 \rightarrow 1001$	$1101 \rightarrow 1101$
$0010 \rightarrow 0010$	$0101 \rightarrow 0110$	$1100 \rightarrow 1010$	$1110 \rightarrow 1110$
$0100 \rightarrow 0011$	$0110 \rightarrow 0111$	$0111 \rightarrow 1011$	$1111 \rightarrow 1111$

Такое преобразование, которое можно осуществить, используя только СНОТ и элементы Тоффоли, обратимо упаковывает типичное подпространство в последние (младшие) $\approx nH(p)$ кубитов. Чтобы завершить схему, необходим также квантовый элемент V , который преобразует состояния $|0\rangle$, $|1\rangle$ отдельного кубита в $|\bar{0}\rangle$, $|\bar{1}\rangle$. Тогда схемой сжатия будет $C^n = (V^\dagger)^{\otimes n} U_n V^{\otimes n}$, и необходимо послать только младшие $nH(p)$ кубитов с выхода C^n , чтобы с большой точностью восстановить последовательность состояний из источника, применяя схему, обратную к данной схеме. Более эффективная схема кодирования упаковала бы только состояния с весом Хэмминга $\approx pr$ в младшие $nH(p)$ кубитов пространства; это можно сделать, используя, например, квантовую версию арифметического кодирования.

Упражнение 12.6. Получите в явном виде выражение для C_X через X в обозначениях вставки 12.4. Опишите, как построить квантовую схему для реализации U_n при произвольных n . Сколько элементарных операций для этого потребуется в зависимости от n ?

Упражнение 12.7 (схема сжатия данных). Опишите в общих чертах схему надежного сжатия n кубитов с $\rho = p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1|$ в nR кубитов для любого $R > S(\rho) = H(p)$.

Упражнение 12.8 (сжатие ансамбля квантовых состояний). Предположим, что вместо определения квантового источника на основе матрицы плотности ρ и точности воспроизведения запутанности, мы приняли определение (стационарного) квантового источника как ансамбля $\{p_j, |\psi_j\rangle\}$ квантовых состояний, и что последовательные обращения к данному источнику независимы; источник выдает состояние $|\psi_j\rangle$ с вероятностью p_j . В этом случае говорят, что

схема «сжатие-развертывание» $(\mathcal{C}^n, \mathcal{D}^n)$ надежна, если средняя по ансамблю степень совпадения приближается к 1 при $n \rightarrow \infty$:

$$\bar{F} \equiv \sum_J p_{j_1} \dots p_{j_n} F(\rho_J, (\mathcal{D}^n \circ \mathcal{C}^n)(\rho_J))^2, \quad (12.61)$$

где $J = (j_1, \dots, j_n)$ и $\rho_J \equiv |\psi_{j_1}\rangle\langle\psi_{j_1}| \otimes \dots \otimes |\psi_{j_n}\rangle\langle\psi_{j_n}|$. Пусть $\rho \equiv \sum_j p_j |\psi_j\rangle\langle\psi_j|$. Покажите, что при таком определении степени совпадения существует надежная схема сжатия при скорости передачи R , если $R > S(\rho)$.

12.3 Передача классической информации по квантовым каналам с шумом

Если что-то плохое может случиться, оно случается

Приписывается Эдварду Мёрфи, младшему

Время от времени все мы испытываем некоторые трудности, разговаривая по телефону. Мы говорим «плохая связь», когда не можем понять собеседника на другом конце телефонной линии. Это один из примеров общего явления, называемого *шум*, которое в некоторой степени наблюдается во всех системах обработки информации. Как описано в гл. 10, коды, исправляющие ошибки, могут быть использованы для борьбы с шумом, что позволяет осуществлять надежную связь и точные вычисления даже в присутствии достаточно сильных помех. Если имеется канал связи N с шумом, то возникает интересный вопрос — сколько информации можно надежно передать по этому каналу. Например, может оказаться, что применение подходящего кода, исправляющего ошибки, позволяет передать 500 бит, пересылая по каналу 1000 бит, с большой вероятностью восстановления данных при любой ошибке, вносимой каналом.

Мы говорим, что такой код имеет скорость передачи $500/1000 = \frac{1}{2}$. Основная проблема теории информации состоит в том, чтобы определить *максимум* скорости передачи, обеспечивающей надежную связь по каналу N , т. е. величину, которую называют *пропускной способностью* канала.

Для классических каналов связи с шумом пропускную способность можно вычислить, используя замечательный результат, известный как *теорема Шеннона о кодировании для канала с шумом*. В подразд. 12.3.1 мы начнем рассмотрение приема и передачи классической информации в присутствии шума с обсуждения некоторых основных идей, лежащих в основе теоремы Шеннона о кодировании для канала с шумом. Однако, мы не будем особенно вдаваться в детали, поскольку в подразд. 12.3.2 подробно рассмотрим общие принципы решения проблемы, когда две стороны пытаются осуществить передачу классической информации, используя квантовый канал с шумом!

12.3.1 Связь по классическому каналу с шумом

Многие из основополагающих идей кодирования для канала с шумом, как квантового, так и классического, можно понять, изучая двоичный симметричный

канал. Напомним (разд. 10.1), что двоичный симметричный канал — это канал с шумом, по которому передается один бит информации, причем шум изменяет бит с вероятностью $p > 0$, а с вероятностью $1 - p$ бит передается без ошибки, как показано на рис. 12.4.

Сколько информации мы можем надежно передать, используя двоичный симметричный канал? Применяя коды, исправляющие ошибки, можно надежно передавать информацию по каналу, используя большее количество бит, чем в самом сообщении. Мы докажем, что максимальная скорость, с которой информация может быть надежно передана по каналу, есть $1 - H(p)$, где $H(\cdot)$ — энтропия Шеннона.

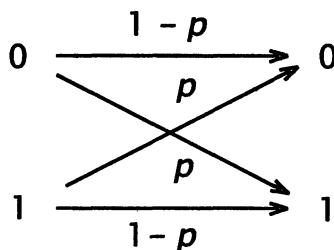


Рис. 12.4. Двоичный симметричный канал

Что понимать под «надежной передачей информации»? Это хороший вопрос, поскольку различные ответы приводят к разным значениям скорости передачи. Мы используем следующее определение надежности: допустим, что входные данные можно закодировать в большие блоки, и потребуем, чтобы вероятность ошибки при использовании данного кода, стремилась к нулю с увеличением размера блока. Другое возможное определение надежности: предположим, что данные можно закодировать в большие блоки так, что вероятность ошибки становится *точно* равной нулю. К сожалению, это определение слишком оптимистично и приводит к нулевой пропускной способности для двоичного симметричного канала! Аналогично, если нельзя кодировать информацию большими блоками, пропускная способность оказывается равной нулю. Удивительно (и совсем не очевидно), что даже при нашем более слабом определении надежности может быть достигнута ненулевая скорость передачи информации. Нужны хорошие идеи, чтобы показать, что это возможно.

Случайное кодирование для двоичного симметричного канала

Предположим, что мы хотим передать nR битов информации, используя n раз двоичный симметричный канал. Мы докажем, что существует код, исправляющий ошибки, который обеспечивает передачу информации с малой вероятностью ошибки при больших n и $R < 1 - H(p)$. Прежде всего используем метод *случайного кодирования* для построения кода, исправляющего ошибки. Пусть $(q, 1 - q)$ — некоторое фиксированное распределение вероятностей для

возможных входных данных канала (0 и 1). (Это распределение часто называется *априорным* распределением данного кода. Выбор данного распределения — всего лишь технический прием, обеспечивающий работу метода случайного кодирования; случайность в распределении не следует путать со случайностью в канале.) Мы выбираем кодовое слово $x = (x_1, \dots, x_n)$, просто взяв $x_j = 0$ с вероятностью q и $x_j = 1$ с вероятностью $1 - q$ независимо для каждого $j = 1, \dots, n$. Повторяем эту процедуру 2^{nR} раз, создавая при этом кодовую книгу C с 2^{nR} записями; обозначим кодовые слова в C как x^j .

Может оказаться, что мы построили плохой код, например такой, в котором все кодовые слова будут состоять из строки, заполненной n нулями, что, очевидно, бесполезно для передачи информации. Тем не менее, оказывается, что в среднем эта процедура случайного кодирования дает достаточно хороший код, исправляющий ошибки. Чтобы понять это, посмотрим, как в канале изменяется *одно* кодовое слово. Поскольку все кодовые слова построены одним и тем же способом, можно рассмотреть первое x^1 .

Какое действие оказывает двоичный симметричный канал на x^1 ? В кодовом слове длины n мы ожидаем приблизительно pr измененных битов, так что с большой вероятностью выходные данные будут иметь расстояние Хэмминга порядка pr от кодового слова x^1 , как показано на рис. 12.5. Мы говорим, что такие выходные данные лежат на сфере Хэмминга радиуса pr вокруг x^1 . Эта сфера состоит приблизительно из $2^{nH(p)}$ элементов $y = x^1 \oplus e$, где e — ошибка, происходящая в канале, \oplus означает побитовое сложение по модулю 2. Согласно теореме о типичных последовательностях, количество таких типичных ошибок e приблизительно равно $2^{nH(p)}$.

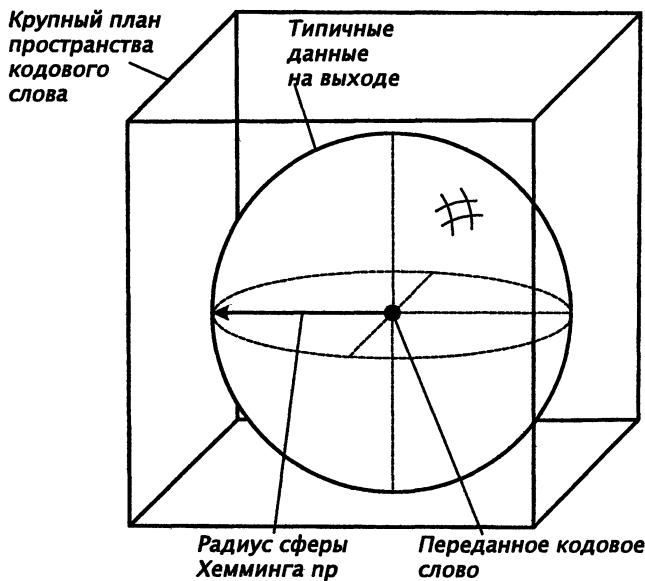


Рис. 12.5. Предположим, что кодовое слово x^1 длины n передается по двоичному симметричному каналу. Тогда типичные данные на выходе из канала являются элементами сферы Хэмминга радиуса pr вокруг кодового слова. (Этот рисунок — крупный план рис. 12.6.)

Мы рассмотрели одно кодовое слово, но, конечно, искажение информации того же типа характерно для всех кодовых слов. Можно представить себе пространство всех кодовых слов и окружающих их сфер Хэмминга (рис. 12.6). Если, как изображено на рисунке, сферы Хэмминга не перекрываются, Боб может легко декодировать данные на выходе из канала. Боб просто проверяет, находятся ли выходные данные на одной из сфер Хэмминга; если это так, Боб выбирает соответствующее кодовое слово, а если нет — значит произошла ошибка. Поскольку мы предположили, что сферы не перекрываются, велика вероятность успешного декодирования любого кодового слова. Действительно, даже если сферы слегка перекрываются, все равно можно провести декодирование с хорошим шансом на успех, поскольку с большой вероятностью данные на выходе из канала будут принадлежать одной (а не нулю, двум или более) из сфер Хэмминга.

Когда имеет место небольшое перекрытие сфер? Чтобы ответить на этот вопрос, нужно лучше понять структуру данных на выходе из канала. Мы получили кодовые слова для нашего кода, сделав 2^{nR} выборок из набора (X_1, \dots, X_n) случайных величин, которые независимы и одинаково распределены, причем $X_j = 0$ с вероятностью q и $X_j = 1$ с вероятностью $1 - q$. Пусть Y_j — результат передачи X_j по двоичному симметричному каналу. Теорема о типичных последовательностях утверждает, что существует приблизительно $2^{nH(Y)}$ типичных значений (Y_1, \dots, Y_n) , где Y имеет такое же распределение как каждое Y_j . Более того, все значения этих типичных данных на выходе имеют приблизительно одинаковую вероятность.

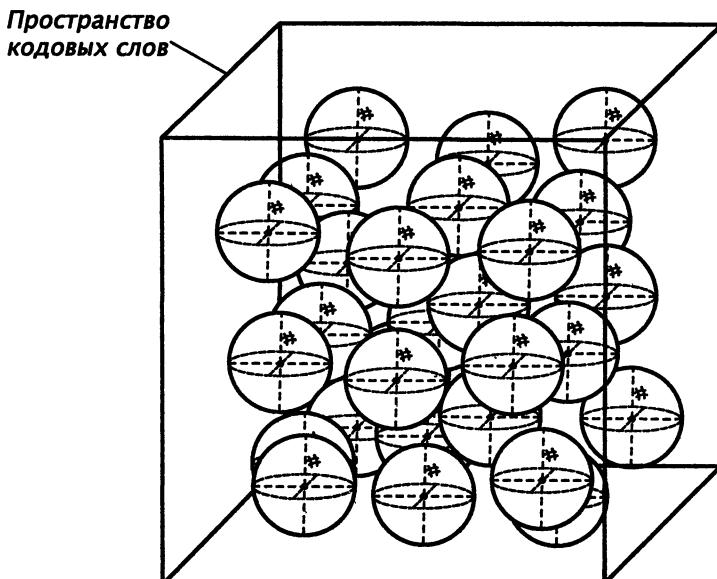


Рис. 12.6. Случайно выбранные кодовые слова для двоичного симметричного канала, окруженные сферами Хэмминга «типичных» данных на выходе. Крупный план для одного кодового слова приведен на рис. 12.5.

Если наугад сделать сто выборок (по одному элементу) из набора размечом один миллион, то маловероятно, что получатся какие-либо повторения. Даже если сделать сто тысяч выборок, количество повторений будет довольно малым. Так будет до тех пор, пока мы не сделаем около миллиона выборок, когда количество повторений начнет увеличиваться с размером выборки. Аналогично, количество перекрытий 2^{nR} сфер Хэмминга радиуса p не начнет увеличиваться до тех пор, пока общее число элементов во всех сферах не приблизится к размеру пространства $2^{nH(Y)}$, из которого мы делали выборки. Поскольку каждая сфера содержит приблизительно $2^{nH(p)}$ элементов, мы с большой вероятностью будем иметь хороший код, исправляющий ошибки, если

$$2^{nR} \times 2^{nH(p)} < 2^{nH(Y)}, \quad (12.62)$$

что соответствует следующему условию:

$$R < H(Y) - H(p). \quad (12.63)$$

Энтропия $H(Y)$ зависит от априорного распределения $(q, 1 - q)$, выбранного для X_j . Чтобы сделать скорость передачи информации по каналу как можно большей, попытаемся получить максимальную энтропию $H(Y)$. Простое вычисление показывает, что это достигается при использовании равномерного априорного распределения, соответствующего $q = \frac{1}{2}$, для которого $H(Y) = 1$, и, следовательно, возможна любая скорость передачи R , меньшая, чем $1 - H(p)$.

Мы только наметили в общих чертах доказательство возможности надежной передачи информации по двоичному симметричному каналу с любой скоростью вплоть до $1 - H(p)$. Рассуждение довольно схематично, но на самом деле содержит многие из ключевых идей, необходимых для строгого рассмотрения даже в квантовом случае. Оказывается, что скорость $1 - H(p)$ является также максимально возможной для передачи информации по двоичному симметричному каналу. При скорости, большей, чем $1 - H(p)$, сферы Хэмминга начинают настолько перекрываться, что невозможно определить, какое кодовое слово было послано, независимо от того, как были выбраны кодовые слова! Таким образом $1 - H(p)$ — пропускная способность двоичного симметричного канала.

Можно ли применять на практике случайное кодирование в качестве метода построения кодов с большой скоростью передачи для двоичного симметричного канала? Если использовать случайный код, то с большой вероятностью получим скорость, близкую к пропускной способности. К сожалению, с этой процедурой связана серьезная трудность. Чтобы произвести кодирование и декодирование, отправитель и получатель (Алиса и Боб) должны сначала договориться о стратегии выполнения этих задач. Для случайных кодов это означает, что Алиса должна послать Бобу список своих случайных кодовых слов. Осуществление этого плана может потребовать более надежной связи, чем способен обеспечить данный канал с шумом. Несомненно, это нежелательно для многих приложений! Метод случайного кодирования — это всего лишь

метод демонстрации *существования* кодов с большой скоростью передачи, а не практический метод их построения. Для широкого практического применения подошел бы метод, который обеспечивает скорости, близкие к пропускной способности канала, и не создает неприемлемые трудности коммуникации для Алисы и Боба. Следует отметить, что методы построения таких кодов даже для классических каналов с шумом были только недавно открыты после многих десятилетий напряженной работы, и интереснейший вопрос, связанный с поиском подобных конструкций для квантовых каналов с шумом, все еще остается открытым.

Теорема Шеннона о кодировании для канала с шумом

Теорема Шеннона о кодировании для канала с шумом обобщает результат о пропускной способности двоичного симметричного канала на случай дискретного канала *без памяти*. Для такого канала заданы конечный входной алфавит \mathcal{I} и конечный выходной алфавит \mathcal{O} . В случае двоичного симметричного канала $\mathcal{I} = \mathcal{O} = \{0, 1\}$. Действие канала описывается множеством *условных вероятностей*, $p(y|x)$, где $x \in \mathcal{I}$ и $y \in \mathcal{O}$. Эти вероятности различных y на выходе из канала при условии, что на входе канала x удовлетворяют соотношениям

$$p(y|x) \geq 0, \quad (12.64)$$

$$\sum_y p(y|x) = 1 \text{ для всех } x. \quad (12.65)$$

Канал не имеет памяти в том смысле, что он действует одинаково каждый раз, когда его используют, т. е. различные обращения к каналу не влияют друг на друга. Мы будем использовать символ \mathcal{N} для обозначения классического канала с шумом.

Конечно, существует много интересных каналов связи, не являющихся дискретными каналами без памяти, например, телефонная линия, которая имеет непрерывный набор входных и выходных данных. Подобные каналы могут быть технически более сложными для понимания, чем дискретные каналы без памяти, однако, многие основополагающие идеи для них одинаковы; список работ по данному вопросу приведен в разд. «История и дополнительная литература» в конце главы.

Рассмотрим формулировку теоремы Шеннона о кодировании для канала с шумом. Мы не будем приводить детали доказательства теоремы, поскольку в следующем разделе докажем более общий результат для квантовых каналов, тем не менее, поучительно рассмотреть формулировку для классического случая. Сначала необходимо несколько уточнить понятие надежной передачи информации. Основная идея проиллюстрирована на рис. 12.7. На первой стадии Алиса создает одно из 2^{nR} возможных сообщений M и кодирует его, используя отображение $C^n : \{1, \dots, 2^{nR}\} \rightarrow \mathcal{I}^n$, которое каждому возможному сообщению Алисы ставит в соответствие строку входных данных, посылаемых Бобу путем использования канала n раз. Боб декодирует данные на выходе

канала, используя отображение $D^n : \mathcal{O}^n \rightarrow \{1, \dots, 2^{nR}\}$, которое каждой возможной строке данных на выходе из канала ставит в соответствие сообщение. Для заданной пары отображений кодирования–декодирования *вероятность ошибки* определяется как максимальная вероятность по всем сообщениям M того, что декодированные данные на выходе из канала $D(Y)$ не совпадают с сообщением M :

$$p(C^n, D^n) \equiv \max_M p(D^n(Y) \neq M | X = C^n(M)). \quad (12.66)$$

Мы говорим, что скорость передачи R является *достижимой*, если существует такая последовательность пар отображений кодирования–декодирования (C^n, D^n) при скорости передачи R , для которой $p(C^n, D^n) \rightarrow 0$ при $n \rightarrow \infty$. *Пропускная способность* $C(\mathcal{N})$ данного канала \mathcal{N} с шумом, по определению, является супремумом по всем скоростям, достижимым для данного канала.



Рис. 12.7. Задача кодирования для классических сообщений при наличии шума. Требуется, чтобы каждое из 2^{nR} возможных сообщений с большой вероятностью прошло по каналу без искажения

Изначально было не очевидно, как вычислить пропускную способность канала. Можно было бы попытаться найти супремум по очень большому (бесконечному!) классу возможных методов кодирования и декодирования, но это не слишком перспективный подход к решению задачи. Теорема Шеннона о кодировании для канала с шумом значительно упрощает вычисление пропускной способности, сводя его к простой и вполне определенной задаче оптимизации, которая может быть точно решена во многих случаях и разрешима на компьютере, даже когда точное решение невозможно.

Теорема 12.7 (теорема Шеннона о кодировании для канала с шумом). Пропускная способность для канала \mathcal{N} с шумом определяется выражением

$$C(\mathcal{N}) = \max_{p(x)} H(X:Y), \quad (12.67)$$

где максимум берется по всем распределениям $p(x)$ входных данных X при однократном использовании канала и Y — случайная величина, полученная на выходе канала.

В качестве примера применения теоремы о кодировании для канала с шумом рассмотрим случай двоичного симметричного канала, изменяющего биты с вероятностью p , и распределением данных на входе $p(0) = q$, $p(1) = 1 - q$.

Имеем

$$H(X:Y) = H(Y) - H(Y|X) \quad (12.68)$$

$$= H(Y) - \sum_x p(x)H(Y|X=x). \quad (12.69)$$

Но $H(Y|X = x) = H(p)$ для каждого x , поэтому взаимная информация $H(Y:X) = H(Y) - H(p)$ становится максимальной при $q = 1/2$, так что $H(Y) = 1$. Согласно теореме Шеннона о кодировании для канала с шумом, $C(\mathcal{N}) = 1 - H(p)$, что совпадает с полученным ранее результатом.

Упражнение 12.9. На вход канала *стирания* подаются 0 или 1, а на выходе получаются 0, 1 и e . С вероятностью $1-p$ данные на входе совпадают с данными на выходе. С вероятностью p входные данные «стираются» и заменяются на e .

1. Покажите, что пропускная способность канала стирания есть $1 - p$.
2. Докажите, что пропускная способность канала стирания больше пропускной способности двоичного симметричного канала. Почему этот результат интуитивно кажется правдоподобным?

Упражнение 12.10. Предположим, что \mathcal{N}_1 и \mathcal{N}_2 — два дискретных канала без памяти, такие, что алфавит на входе канала \mathcal{N}_1 совпадает с алфавитом на выходе канала \mathcal{N}_2 . Покажите, что

$$C(\mathcal{N}_2 \circ \mathcal{N}_1) \leq \min(C(\mathcal{N}_1), C(\mathcal{N}_2)). \quad (12.70)$$

Приведите пример, в котором выполняется строгое неравенство.

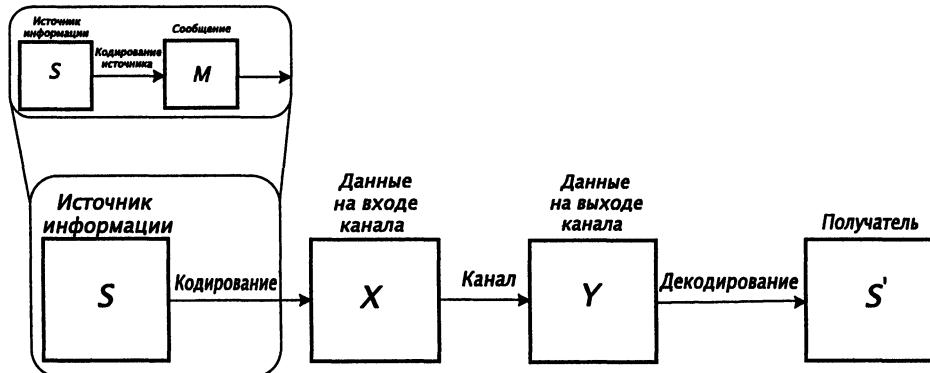


Рис. 12.8. Модель кодирования для классического источника информации при наличии шума, иногда называемая моделью «источник–канал».

Особенностью рассмотренной теоремы о кодировании для канала с шумом является то, что понятие классического источника информации не используется! Напомним, что ранее мы дали определение классического источника информации как последовательности независимых и одинаково распределенных

случайных величин. Можно нетривиально объединить это понятие источника информации с теоремой о кодировании для канала с шумом, чтобы получить так называемую теорему о кодировании «источник–канал». Основная идея проиллюстрирована на рис. 12.8. Предположим, что источник информации имеет энтропию $H(X)$. Используя теорему Шеннона о кодировании для канала без шума, можно сжать информацию от источника так, что потребуется только $nH(X)$ битов для ее представления. Эту операцию иногда называют кодированием источника. Сжатые данные на выходе источника используются, в свою очередь, как сообщение на выходе канала с шумом. Для передачи со скоростью R , меньшей пропускной способности, требуется $nH(X)/R$ обращений к каналу, чтобы без искажений передать сжатые данные получателю, который может развернуть их, чтобы восстановить исходные данные от источника.

Возможна ли более совершенная схема для передачи информации от источника по каналу с шумом? Можно ли предложить что-нибудь более эффективное, чем двухступенчатый метод сжатия–кодирования и декодирования–развертывания? Оказывается, что нет, и описанный метод кодирования «источник–канал», на самом деле, оптимален, но доказательство этого факта не входит в наши намерения. В конце главы в разд. «История и дополнительная литература» можно найти ссылки на работы, в которых проведены более детальные исследования.

12.3.2 Связь по квантовым каналам с шумом

Предположим, что вместо классического канала связи с шумом Алиса и Боб используют квантовый канал связи с шумом. Более точно, у Алисы есть некоторое сообщение M , которое она хочет послать Бобу. Она кодирует это сообщение как и в классическом случае, но теперь сообщение кодируется *квантовым состоянием*, которое посыпается по квантовому каналу с шумом. Только в том случае, если кодирование будет проведено надлежащим образом, можно надеяться, что Боб сможет определить, каково было сообщение Алисы, с малой вероятностью ошибки. Более того, желательно, чтобы *скорость*, с которой Алиса посыпает Бобу информацию, была как можно более высокой. Другими словами, мы хотим вычислить *пропускную способность квантового канала с шумом для классической информации*. Эта задача до сих пор полностью не решена, однако многое уже сделано, и в данном разделе мы рассмотрим некоторые полученные результаты.

Известно, как вычислить пропускную способность для канала \mathcal{E} , если предположить, что Алиса кодирует свое сообщение, используя *факторизованное состояние* вида $\rho_1 \otimes \rho_2 \otimes \dots$, где ρ_1, ρ_2, \dots являются возможными входными состояниями для одного обращения к каналу \mathcal{E} . Мы назовем пропускную способность с таким ограничением *пропускной способностью для факторизованного состояния* и обозначим ее как $C^{(1)}(\mathcal{E})$, чтобы указать, что входные состояния для двух или более обращений к данному каналу не могут быть запутаны. Отметим, что эта ограниченная модель связи между Алисой и Бобом позволяет Бобу декодировать, используя измерения запутанных выходных состояний для

нескольких обращений к каналу, что весьма существенно. Единственным (и весьма досадным) ограничением является то, что Алиса должна приготовить входные данные в виде факторизованного состояния. Многие исследователи полагают, хотя это не доказано, что использование запутанных входных состояний не увеличивает пропускную способность. Пропускную способность для факторизованного состояния можно вычислить с помощью теоремы Холево–Шумахера–Вестморланда (ХШВ). Подобно теореме Шеннона о кодировании для классического канала с шумом теорема ХШВ обеспечивает эффективные средства вычисления пропускной способности канала \mathcal{E} для факторизованного состояния с шумом и в некоторых случаях позволяет даже получить точное выражение.

Теорема 12.8 (теорема Холево–Шумахера–Вестморланда). Пусть \mathcal{E} — квантовое преобразование, сохраняющее след. Введем величину

$$\chi(\mathcal{E}) \equiv \max_{\{p_j, \rho_j\}} \left[S \left(\mathcal{E} \left(\sum_j p_j \rho_j \right) \right) - \sum_j p_j S(\mathcal{E}(\rho_j)) \right], \quad (12.71)$$

где максимум берется по всем ансамблям $\{p_j, \rho_j\}$ возможных входных состояний ρ_j для канала. Тогда $\chi(\mathcal{E})$ — пропускная способность канала \mathcal{E} для факторизованного состояния, т. е. $\chi(\mathcal{E}) = C^{(1)}(\mathcal{E})$.

Максимум в (12.71) берется по неограниченному набору ансамблей состояний. На самом деле, мы используем результаты приведенного ниже упражнения, чтобы ограничить этот набор ансамблями чистых состояний, содержащими не более d^2 элементов, где d — размерность пространства входных состояний канала.

Упражнение 12.11. Покажите, что максимум в выражении (12.71) может быть достигнут при использовании ансамбля чистых состояний. Покажите далее, что достаточно рассмотреть только ансамбли из не более, чем d^2 чистых состояний, где d — размерность пространства входных состояний канала.

Доказательство теоремы ХШВ включает несколько идей и его легко понять, разбив на небольшие части.

Случайное кодирование

Предположим, что ρ_j — набор возможных входных состояний для канала \mathcal{E} и пусть $\sigma_j \equiv \mathcal{E}(\rho_j)$ — соответствующие состояния на выходе. Мы применим метод случайного кодирования, подобный описанному ранее для двоичного симметричного канала, разрешив Алисе и Бобу передавать кодовые слова, которые являются произведениями заданных состояний ρ_j . Пусть p_j — распределение вероятностей по индексам j , т. е. *aприорное распределение*. Алиса хочет послать Бобу сообщение M , выбранное из набора $\{1, \dots, 2^{nR}\}$. Каждому возможному сообщению M Алиса ставит в соответствие кодовое слово $\rho_{M_1} \otimes \rho_{M_2} \otimes \dots \otimes \rho_{M_n}$, где M_1, \dots, M_n выбраны из набора индексов $\{j\}$. (Это не означает, что M_1, \dots, M_n являются десятичным представлением M или чем-нибудь в том же роде!) Для каждого сообщения M Алиса выбирает M_1 случайно с распределением p_j . Аналогичным образом она выбирает M_2 и так далее

до M_n . Введем обозначение $\rho_M \equiv \rho_{M_1} \otimes \dots \otimes \rho_{M_n}$. Соответствующие состояния на выходе просто обозначим как σ вместо ρ , так что, например, $\sigma_{M_1} = \mathcal{E}(\rho_{M_1})$ и $\sigma_M = \mathcal{E}^{\otimes n}(\rho_M)$.

Боб, получив некоторое состояние σ_M (соответствующее посланному Алисой сообщению M), производит измерение, пытаясь определить, что это было за сообщение. Поскольку мы интересуемся лишь статистикой измерений, а не состоянием системы Боба после измерения, достаточно описать данное измерение, используя формализм POVM. Мы предполагаем, что для каждого возможного сообщения M Боб имеет соответствующий POVM-элемент E_M . Боб может иметь один (или более) POVM-элементов, которые не соответствуют ни одному сообщению, посланному Алисой. Очевидно, что все они могут быть суммированы в один POVM-элемент E_0 , удовлетворяющий равенству $E_0 = I - \sum_{M \neq 0} E_M$. Вероятность того, что Боб успешно идентифицирует M , равна $\text{tr}(\sigma_M E_M)$, и, следовательно, вероятность ошибки, сделанной при идентификации сообщения M , $p^{E_M} \equiv 1 - \text{tr}(\sigma_M E_M)$.

Мы хотим доказать существование кодов с большой скоростью передачи, таких, что вероятность ошибки p_M^E мала для *всех* сообщений M . Для этого используем довольно хитрый и противоречавший интуиции трюк, придуманный Шенноном для решения классической задачи. Предположим, что Алиса создает сообщения M , выбирая их случайным образом из набора $\{1, \dots, 2^{nR}\}$, и анализирует среднюю вероятность ошибки

$$p_{\text{ср}} \equiv \frac{\sum_M p_M^E}{2^{nR}} = \frac{\sum_M (1 - \text{tr}(\sigma_M E_M))}{2^{nR}}. \quad (12.72)$$

Первый шаг доказательства — показать, что существуют коды с большой скоростью передачи, для которых $p_{\text{ср}} \rightarrow 0$ при больших n . После того, как это будет сделано, мы используем трюк Шеннона, чтобы показать, что существуют коды, примерно с той же скоростью передачи, для которых p^{E_M} близка к нулю для *всех* M . Мы начнем с построения набора POVM-элементов $\{E_M\}$, который позволяет Бобу очень хорошо (хотя, возможно, не оптимально) декодировать выходные состояния σ_M . Основополагающей идеей нашего построения, как и для классического двоичного симметричного канала, является идея типичности.

Пусть $\epsilon > 0$. Определим $\bar{\sigma}$ как $\bar{\sigma} \equiv \sum_j p_j \sigma_j$ и пусть P — проектор на ϵ -тиpicное подпространство для $\bar{\sigma}^{\otimes n}$. Из теоремы о типичном подпространстве следует, что для любых $\delta > 0$ и достаточно больших n

$$\text{tr}(\bar{\sigma}^{\otimes n}(I - P)) \leq \delta. \quad (12.73)$$

Для заданного сообщения M мы также определим понятие ϵ -тиpicного подпространства для σ_M , основываясь на том, что типичное σ_M является тензорным произведением приблизительно $n p_1$ копий σ_1 , $n p_2$ копий σ_2 и т. д. Введем обозначение $\bar{S} \equiv \sum_j p_j S(\sigma_j)$. Предположим, что σ_j имеет спектральное разложение $\sum_k \lambda_j^{j_k} |E_{j_k}\rangle \langle E_{j_k}|$, так что

$$\sigma_M = \sum_K \lambda_K^M |E_K^M\rangle \langle E_K^M|, \quad (12.74)$$

где $K = (K_1, \dots, K_n)$, и для удобства использованы обозначения $\lambda_K^M \equiv \lambda_{K_1}^{M_1}$ $\lambda_{K_2}^{M_2} \dots \lambda_{K_n}^{M_n}$ и $|E_K^M\rangle \equiv |E_{K_1}^{M_1}\rangle|E_{K_2}^{M_2}\rangle\dots|E_{K_n}^{M_n}\rangle$. Определим P_M как проектор на пространство, порожденное всеми $|E_K^M\rangle$ такими, что

$$\left| \frac{1}{n} \log \frac{1}{\lambda_K^M} - \bar{S} \right| \leq \varepsilon. \quad (12.75)$$

(Полезно обозначить через T_M набор всех K , для которых это условие выполняется.) Аналогично доказательству теоремы о типичных последовательностях закон больших чисел утверждает, что для любых $\delta > 0$ и достаточно больших n мы имеем $E[\text{tr}(\sigma_M P_M)] \geq 1 - \delta$, где математическое ожидание берется по распределению кодовых слов ρ_M (для фиксированного сообщения M), обусловленному случайным кодированием, и, следовательно, для каждого M

$$E[\text{tr}(\sigma_M(I - P_M))] \leq \delta. \quad (12.76)$$

Заметим также, что по определению (12.75) размерность подпространства, на которое проектирует P_M , может быть не более $2^{n(\bar{S}+\varepsilon)}$, и поэтому

$$E[\text{tr}(P_M)] \leq 2^{n(\bar{S}+\varepsilon)}. \quad (12.77)$$

Теперь используем понятие типичности, чтобы построить POVM для операции декодирования Боба. Введем

$$E_M \equiv \left(\sum_{M'} PP_{M'} P \right)^{-1/2} PP_M P \left(\sum_{M'} PP_{M'} P \right)^{-1/2}, \quad (12.78)$$

где $A^{-1/2}$ — обобщенный обратный оператор к $A^{1/2}$, т. е. данный оператор является обратным к $A^{1/2}$ на носителе A и равен нулю в остальном пространстве. Отсюда следует, что $\sum_M E_M \leq I$, и мы можем определить еще один положительный оператор $E_0 \equiv I - \sum_M E_M$, чтобы завершить POVM. Интуитивно понятно, что эта конструкция соответствует методу декодирования, описанному для двоичных симметричных каналов. В частности, с точностью до малых поправок E_M равен проектору P_M , и измерение Боба $\{E_M\}$ соответствует, по существу, проверке, действительно ли состояние на выходе из канала попадает в то пространство, на которое проектирует P_M ; это пространство можно рассматривать как аналог сферы Хэмминга радиуса r_p вокруг кодового слова, использованной для двоичного симметричного канала.

Основной частью доказательства того, что случайное кодирование работает, является получение верхней границы для средней вероятности ошибки $p_{\text{ср}}$. Это подробно изложено во вставке 12.5. Полученный результат имеет вид

$$p_{\text{ср}} \leq \frac{1}{2^{nR}} \sum_M \left[3 \text{tr}(\sigma_M(I - P)) + \sum_{M' \neq M} \text{tr}(P\sigma_M P P_{M'}) + \text{tr}(\sigma_M(I - P_M)) \right]. \quad (12.79)$$

Величина p_{cp} определяется по отношению к конкретному набору кодовых слов. Мы вычислим *математическое ожидание* этой величины по всем случайнм кодам. По построению $\mathbf{E}(\sigma_M) = \bar{\sigma}^{\otimes n}$, а σ_M и $P_{M'}$ — независимы при $M' \neq M$; отсюда получаем

$$\mathbf{E}(p_{\text{cp}}) \leq 3 \operatorname{tr}(\bar{\sigma}^{\otimes n}(I - P)) + (2^{nR} - 1) \operatorname{tr}(P \bar{\sigma}^{\otimes n} P \mathbf{E}(P_1)) + \mathbf{E}(\operatorname{tr}(\sigma_1(I - P_1))). \quad (12.80)$$

Подстановка (12.73) в (12.76) дает

$$\mathbf{E}(p_{\text{cp}}) \leq 4\delta + (2^{nR} - 1) \operatorname{tr}(P \bar{\sigma}^{\otimes n} P \mathbf{E}(P_1)). \quad (12.81)$$

Но $P \bar{\sigma}^{\otimes n} P \leq 2^{n(S(\bar{\sigma}) - \varepsilon)} I$ и из (12.77) имеем $\mathbf{E}(\operatorname{tr}(P_1)) \leq 2^{n(\bar{S} + \varepsilon)}$, откуда

$$\mathbf{E}(p_{\text{cp}}) \leq 4\delta + (2^{nR} - 1) 2^{-n(S(\bar{\sigma}) - \bar{S} - 2\varepsilon)}. \quad (12.82)$$

Если $R < S(\bar{\sigma})\bar{S}$, получаем $\mathbf{E}(p_{\text{cp}}) \rightarrow 0$ при $n \rightarrow \infty$. Действительно, выбрав ансамбль $\{p_j, \rho_j\}$, при котором достигается максимум в (12.71), мы видим, что неравенство должно быть справедливо при $R < \chi(\mathcal{E})$. Следовательно, должна существовать последовательность кодов со скоростью передачи R , такая что $p_{\text{cp}} \rightarrow 0$ при увеличении размера n кодового блока. Отсюда следует, что для любого фиксированного $\varepsilon > 0$ (заметьте, что здесь ε имеет другой смысл по сравнению с тем, что был раньше!) при достаточно больших n

$$p_{\text{cp}} = \frac{\sum_M p_M^\varepsilon}{2^{nR}} < \varepsilon. \quad (12.83)$$

Очевидно, что для того, чтобы это выполнялось, по меньшей мере, половина сообщений M должна удовлетворять условию $p_M^\varepsilon < 2\varepsilon$. Мы строим новый код, удаляя половину кодовых слов (кодовые слова с большой p_M^ε) из кода со скоростью R и $p_{\text{cp}} < \varepsilon$; в результате получается новый код с $2^{nR}/2 = 2^{n(R-1/n)}$ кодовыми словами и с $p_M^\varepsilon < 2\varepsilon$ для всех сообщений M . Очевидно, что этот код также имеет асимптотическую скорость передачи R , и вероятность ошибки может быть сделана сколь угодно малой для *всех* (а не в среднем) кодовых слов при достаточно большом n .

Итак, мы показали, что для любого R , меньшего $\chi(\mathcal{E})$, определенного в (12.71), существует код, использующий факторизованные входные состояния, который позволяет передавать информацию по каналу \mathcal{E} со скоростью R . Наше доказательство имеет тот же недостаток, что и доказательство теоремы Шеннона о кодировании для классического канала с шумом, использующее случайное кодирование, а именно, оно не обеспечивает конструктивную процедуру выполнения кодирования, но тем не менее демонстрирует существование кодов со скоростями вплоть до пропускной способности.

Доказательство верхней границы

Пусть R больше, чем $\chi(\mathcal{E})$, определенной в (12.71). Покажем, что Алиса не может надежно передавать информацию Бобу с такой скоростью по каналу \mathcal{E} . Наша основная стратегия — предположить, что Алиса создает сообщения M , выбирая их случайнм образом из набора $\{1, \dots, 2^{nR}\}$, и показать, что *средняя*, а следовательно и максимальная, вероятность ошибки Алисы ограничена снизу положительным числом.

Вставка 12.5. Теорема ХШВ: оценка величины ошибки

Наиболее технически сложной частью доказательства теоремы ХШВ является оценка $p_{\text{ср}}$. Здесь мы покажем в общих чертах, как это сделать; пропущенные шаги можно рассматривать как упражнения, которые необходимо выполнить, чтобы полностью восстановить доказательство. Введем отображение $|\tilde{E}_K^M\rangle \equiv P|E_K^M\rangle$. Тогда

$$E_M = \left(\sum_{M'} \sum_{K \in T_{M'}} |\tilde{E}_K^{M'}\rangle \langle \tilde{E}_K^{M'}| \right)^{-1/2} \times \sum_{K \in T_M} |\tilde{E}_K^M\rangle \langle \tilde{E}_K^M| \left(\sum_{M'} \sum_{K \in T_{M'}} |\tilde{E}_K^{M'}\rangle \langle \tilde{E}_K^{M'}| \right)^{-1/2}. \quad (12.84)$$

Полагая

$$\alpha_{(M,K),(M',K')} \equiv \langle \tilde{E}_K^M | \left(\sum_{M''} \sum_{K'' \in T_{M''}} |\tilde{E}_{K''}^{M''}\rangle \langle \tilde{E}_{K''}^{M''}| \right)^{-1/2} |\tilde{E}_{K'}^{M'}\rangle, \quad (12.85)$$

среднюю вероятность ошибки можно записать как

$$p_{\text{ср}} = \frac{1}{2^n R} \sum_M \left[1 - \sum_K \sum_{K' \in T_M} \lambda_K^M |\alpha_{(M,K),(M,K')}|^2 \right]. \quad (12.86)$$

Используя $\sum_K \lambda_K^M = 1$ и опуская неположительные члены, мы видим, что

$$p_{\text{ср}} \leq \frac{1}{2^n R} \sum_M \left[\sum_{K \in T_M} \lambda_K^M (1 - \alpha_{(M,K),(M,K')}^2) + \sum_{K \notin T_M} \lambda_K^M \right]. \quad (12.87)$$

Определим матрицу Γ с элементами $\gamma_{(M,K),(M',K')} \equiv \langle \tilde{E}_K^M | E_{K'}^{M'} \rangle$, где индексы $K \in T_M$ и $K' \in T_{M'}$. Удобно работать в пространстве матриц с такими индексами; E обозначает единичную матрицу в этом пространстве, а sp (шпур) — операция взятия следа по этим индексам. Вычисления показывают, что $\Gamma^{1/2} = [\alpha_{(M,K),(M',K')}]$, откуда следует, что $\alpha_{(M,K),(M,K')}^2 \leq \gamma_{(M,K),(M,K')} \leq 1$. Используя (12.87), а также тот факт, что $1 - x^2 = (1 + x)(1 - x) \leq 2(1 - x)$ при $0 \leq x \leq 1$, получаем

$$p_{\text{ср}} \leq \frac{1}{2^n R} \sum_M \left[2 \sum_{K \in T_M} \lambda_K^M (1 - \alpha_{(M,K),(M,K)}) + \sum_{K \notin T_M} \lambda_K^M \right]. \quad (12.88)$$

Введем диагональную матрицу $\Lambda \equiv \text{diag}(\lambda_K^M)$ и заметим, что

$$2(E - \Gamma^{1/2}) = (E - \Gamma^{1/2})^2 + (E - \Gamma) \quad (12.89)$$

$$= (E - \Gamma)^2(E + \Gamma^{-1/2})^{-2} + (E - \Gamma) \quad (12.90)$$

$$\leq (E - \Gamma)^2 + (E - \Gamma). \quad (12.91)$$

Следовательно,

$$2 \sum_M \sum_{K \in T_M} \lambda_K^M (1 - \alpha_{(M,K),(M,K)}) = 2 \text{sp}(\Lambda(E - \Gamma^{-1/2})) \quad (12.92)$$

$$\leq \text{sp}(\Lambda(E - \Gamma)^2) + \text{sp}(\Lambda(E - \Gamma)). \quad (12.93)$$

Вычисляя шпуры в правой части выражений, подставляя результаты в (12.88) и выполняя некоторые простые алгебраические действия, получаем

$$p_{\text{cp}} \leq \frac{1}{2^{nR}} \sum_M \left[\sum_K \lambda_K^M \left(2 - 2\gamma_{(M,K)(M,K)} + \sum_{K' \neq K} |\gamma_{(M,K),(M,K')}|^2 \right. \right. \\ \left. \left. + \sum_{M' \neq M, K' \in T_{M'}} |\gamma_{(M,K)(M',K')}|^2 \right) + \sum_{K \in T_M} \lambda_K^M \right]. \quad (12.94)$$

Используя соответствующие определения и выполняя простые алгебраические действия, находим

$$p_{\text{cp}} \leq \frac{1}{2^{nR}} \sum_M \left[2 \text{tr}(\sigma_M(I - P)) + \text{tr}(\sigma_M(I - P)P_M(I - P)) \right. \\ \left. + \sum_{M' \neq M} \text{tr}(P\sigma_M P P_{M'}) + \text{tr}(\sigma_M(I - P_M)) \right]. \quad (12.95)$$

Второе слагаемое меньше, чем $\text{tr}(\sigma_M(I - P))$, что дает нужную оценку величины ошибки, (12.79).

Предположим, что Алиса кодирует сообщение M как $\rho_M = \rho_1^M \otimes \dots \otimes \rho_n^M$ (соответствующие входные состояния обозначаются через σ вместо ρ), а Боб декодирует это сообщение, используя POVM $\{E_M\}$; без потери общности можно считать, что POVM содержит элемент E_M для каждого сообщения и, возможно, дополнительный элемент E_0 , чтобы выполнялось соотношение полноты $\sum_M E_M = I$. Это дает среднюю вероятность ошибки

$$p_{\text{cp}} = \frac{\sum_M (1 - \text{tr}(\sigma_M E_M))}{2^{nR}}. \quad (12.96)$$

Из упр. 12.3 мы знаем, что $R \leq \log(d)$, где d — размерность пространства состояний на входе канала, и поэтому POVM $\{E_M\}$ содержит не более $d^n + 1$ элементов. Из неравенства Фано следует, что

$$H(p_{cp}) + p_{cp} \log(d^n) \geq H(M|Y), \quad (12.97)$$

где Y — результаты измерения над выходным состоянием Боба, и, таким образом,

$$np_{cp} \log d \geq H(M) - H(M:Y) - H(p_{cp}) = nR - H(M:Y) - H(p_{cp}). \quad (12.98)$$

Используя сначала границу Холево, а затем субаддитивность энтропии, получаем

$$H(M:Y) \leq S(\bar{\sigma}) - \sum_M \frac{S(\sigma_1^M \otimes \cdots \otimes \sigma_n^M)}{2^{nR}} \quad (12.99)$$

$$\leq \sum_{j=1}^n \left(S(\bar{\sigma}^j) - \sum_M \frac{S(\sigma_j^M)}{2^{nR}} \right), \quad (12.100)$$

где $\bar{\sigma}^j \equiv \sum_M \sigma_j^M / 2^{nR}$. Каждый из n членов суммы в правой части не превышает $\chi(\mathcal{E})$, так что

$$H(M:Y) \leq n\chi(\mathcal{E}). \quad (12.101)$$

Подстановка в (12.98) дает $np_{cp} \log d \geq n(R\chi(\mathcal{E})) - H(p_{cp})$, и, следовательно, при большом n получаем

$$p_{cp} \geq \frac{(R - \chi(\mathcal{E}))}{\log(d)}, \quad (12.102)$$

положительную нижнюю границу для средней вероятности ошибки при $R > \chi(\mathcal{E})$, что завершает доказательство того, что $\chi(\mathcal{E})$ является верхней границей пропускной способности для факторизованного состояния.

Примеры

Интересным следствием теоремы ХШВ является то, что *любой* квантовый канал можно использовать для передачи классической информации, если \mathcal{E} не является константой. Если \mathcal{E} не является константой, то существуют такие чистые состояния $|\psi\rangle$ и $|\varphi\rangle$, что $\mathcal{E}(|\psi\rangle\langle\psi|) \neq \mathcal{E}(|\varphi\rangle\langle\varphi|)$. Подставив ансамбль, состоящий из этих двух состояний с равными вероятностями $\frac{1}{2}$, в выражение (12.71) для пропускной способности факторизованного состояния, мы видим, что

$$C^{(1)}(\mathcal{E}) \geq S\left(\frac{\mathcal{E}(|\psi\rangle\langle\psi|) + \mathcal{E}(|\varphi\rangle\langle\varphi|)}{2}\right) - \frac{1}{2}S(\mathcal{E}(|\psi\rangle\langle\psi|)) - \frac{1}{2}S(\mathcal{E}(|\varphi\rangle\langle\varphi|)) > 0, \quad (12.103)$$

где второе неравенство следует из строгой вогнутости энтропии (подразд. 11.3.5).

Рассмотрим простой пример деполяризующего канала с параметром p , когда пропускная способность для факторизованного состояния может быть точно вычислена. Пусть $\{p_j, |\psi_j\rangle\}$ — ансамбль квантовых состояний одного кубита. Тогда имеем

$$\mathcal{E}(|\psi_j\rangle\langle\psi_j|) = (1-p)|\psi_j\rangle\langle\psi_j| + p\frac{I}{2}, \quad (12.104)$$

квантовое состояние с собственными значениями $(1+p)/2$ и $(1-p)/2$, откуда

$$S(\mathcal{E}(|\psi_j\rangle\langle\psi_j|)) = H\left(\frac{1+p}{2}\right), \quad (12.105)$$

где выражение справа не зависит от $|\psi_j\rangle$. Следовательно, максимум в (12.71) достигается при максимальном значении энтропии $S(\sum_j \mathcal{E}(|\psi_j\rangle\langle\psi_j|))$ в один бит, когда $|\psi_j\rangle$ — ортонормированный базис (например, $|0\rangle$ и $|1\rangle$) для пространства состояний одного кубита. При этом пропускная способность деполяризующего канала с параметром p для факторизованного состояния равна

$$C^{(1)}(\mathcal{E}) = 1 - H\left(\frac{1+p}{2}\right). \quad (12.106)$$

Упражнение 12.12. Используя доказательство теоремы ХШВ, докажите теорему Шеннона о кодировании для классического канала с шумом, упрощая доказательство там, где возможно.

12.4 Квантовая информация в квантовых каналах с шумом

Сколько квантовой информации можно надежно передать по квантовому каналу с шумом? Проблема определения *пропускной способности квантового канала* для квантовой информации изучена хуже, чем проблема определения пропускной способности по квантовому каналу с шумом для классической информации. Мы представим здесь некоторые теоретико-информационные средства, которые были разработаны для изучения пропускной способности квантового канала для квантовой информации, включая важные квантовые теоретико-информационные аналоги неравенства Фано (вставка 12.2), неравенства обработки данных (подразд. 11.2.4) и границу Синглтона (упр. 10.21).

Как и в случае сжатия квантовых данных, наша точка зрения на изучение этих проблем состоит в следующем: квантовый источник нужно рассматривать как квантовую систему в смешанном состоянии ρ , которая запутана с другой квантовой системой; мерой надежности передачи квантовой информации, описываемой квантовым преобразованием \mathcal{E} , является точность воспроизведения запутанности $F(\rho, \mathcal{E})$. Полезно, как в гл. 9, обозначить через Q систему, которая находится в состоянии ρ , и через R — вспомогательную систему, которая «расширяет» систему Q до чистого состояния. При этом точность воспроизведения

запутанности является мерой того, насколько хорошо запутанность системы Q с системой R сохраняется после действия \mathcal{E} на систему Q .

12.4.1 Обменная энтропия и квантовое неравенство Фано

Какова интенсивность шума, возникающего при действии квантового преобразования на состояние ρ квантовой системы Q ? Одна из мер шума — это степень того, насколько состояние системы RQ , изначально чистое, становится смешанным в результате квантового преобразования. Мы определяем *обменную энтропию* преобразования \mathcal{E} при входных данных ρ как

$$S(\rho, \mathcal{E}) \equiv S(R', Q'). \quad (12.107)$$

Предположим, что действие квантового преобразования \mathcal{E} моделируется при помощи среды E , которая изначально находится в чистом состоянии, и унитарного взаимодействия Q и E , как описано в гл. 8. Состояние системы RQE после взаимодействия является чистым, поэтому $S(R', Q') = S(E')$, так что обменную энтропию можно отождествить с величиной энтропии, внесенной при преобразовании \mathcal{E} в изначально чистую среду E .

Отметим, что обменная энтропия не зависит от выбора R , при помощи которого начальное состояние ρ системы Q расширяется до чистого RQ . Причина этого заключается в том, что любые два расширения Q до чистого состояния RQ связаны при помощи унитарного преобразования, действующего на систему R , как показано в упр. 2.81. Это унитарное преобразование, очевидно, коммутирует с квантовым преобразованием \mathcal{E} , действующим на систему Q , и, следовательно, конечные состояния $R'Q'$, полученные двумя различными способами очищения, связаны посредством унитарного преобразования над R , и поэтому приводят к одинаковым значениям обменной энтропии. К тому же отсюда следует, что $S(E')$ не зависит от модели среды для \mathcal{E} при условии, что E изначально находится в чистом состоянии.

Простая и полезная формула для обменной энтропии может быть получена на основе представления квантового преобразования операторной суммой. Предположим, что сохраняющее след квантовое преобразование \mathcal{E} имеет элементы $\{E_j\}$. Тогда, как показано в подразд. 8.2.3, унитарная модель для этого преобразования задается унитарным оператором U , действующим на QE так, что

$$U|\psi\rangle|0\rangle = \sum_i E_i |\psi\rangle|i\rangle, \quad (12.108)$$

где $|0\rangle$ — начальное состояние среды, и $|i\rangle$ — ортонормированный базис для данной среды. Отметим, что состояние E' после применения \mathcal{E} имеет вид

$$\rho^{E'} = \sum_{i,j} \text{tr}(E_i \rho E_j^\dagger) |i\rangle\langle j|, \quad (12.109)$$

т. е. $\text{tr}(E_j \rho E_j^\dagger)$ являются матричными элементами E' в базисе $|i\rangle$. Для данного преобразования с элементами $\{E_j\}$ естественно определить матрицу W

(w -матрицу) с матричными элементами $W_{ij} \equiv \text{tr}(E_j \rho E_j^\dagger)$, т. е. W является матрицей E' в подходящем базисе. Это представление для $\rho^{E'}$ позволяет получить полезную для простых вычислений формулу для обменной энтропии

$$S(\rho, \mathcal{E}) = S(W) \equiv -\text{tr}(W \log W). \quad (12.110)$$

Задавая преобразование \mathcal{E} и состояние ρ , всегда можно выбрать элементы $\{F_j\}$ для \mathcal{E} такие, что матрица W будет диагональной; мы говорим, что W имеет *каноническую форму*. Чтобы убедиться, что такой набор элементов существует, вспомним из гл. 8, что квантовое преобразование может иметь множество различных наборов элементов. В частности, два набора операторов $\{E_j\}$ и $\{F_j\}$ являются элементами одного и того же квантового преобразования тогда и только тогда, когда $F_j = \sum_i u_{ij} E_j$, где u — унитарная матрица; кроме того, может понадобиться добавить нулевые операторы к наборам E_j или F_j , чтобы матрица u была квадратной. Пусть W — w -матрица, связанная с определенным набором элементов $\{E_j\}$ преобразования \mathcal{E} . Матрица W является представлением оператора плотности среды, и, следовательно, она неотрицательно определена. Эту матрицу можно привести к диагональному виду при помощи унитарной матрицы v , $D = v W v^\dagger$, где D — диагональная матрица с неотрицательными элементами. Зададим операторы F_j выражением $F_j \equiv \sum_i v_{ij} E_j$, так что $\{F_j\}$ также является набором элементов преобразования \mathcal{E} , приводящим к w -матрице \widetilde{W} с элементами

$$\widetilde{W} = \text{tr}(F_k \rho F_l^\dagger) = \sum_{mn} v_{km} v_{ln}^* W_{mn} = D_{kl}. \quad (12.111)$$

Таким образом, w -матрица диагональна по отношению к элементам преобразования $\{F_j\}$. Говорят, что любой такой набор элементов $\{F_j\}$ преобразования \mathcal{E} , для которого соответствующая w -матрица диагональна, является *каноническим представлением* \mathcal{E} относительно входного состояния ρ . Позднее мы убедимся, что канонические представления имеют особое значение для исправления квантовых ошибок.

Многие свойства обменной энтропии непосредственно следуют из свойств энтропии, рассмотренных в гл. 11. Например, работая в каноническом представлении для сохраняющего след квантового преобразования \mathcal{E} d -мерного пространства, мы сразу же видим, что $S(I/d, \mathcal{E}) = 0$ тогда и только тогда, когда \mathcal{E} — унитарное квантовое преобразование. Поэтому $S(I/d, \mathcal{E})$ можно рассматривать как количественную характеристику некогерентного квантового шума, вносимого в систему. Второй пример: матрица W линейно зависит от ρ , и поскольку энтропия вогнута, то $S(\rho, \mathcal{E})$ вогнута по ρ . Поскольку всегда можно выбрать систему RQ размерности не более d^2 , где d — размерность Q , обменная энтропия ограничена сверху значением $2 \log d$.

Упражнение 12.13. Покажите, что обменная энтропия вогнута относительно квантового преобразования \mathcal{E} .

Интуитивно понятно, что если на квантовый источник Q действует шум, который делает состояние RQ смешанным, то восстановление конечного со-

стояния $R'Q'$ по начальному состоянию RQ не может быть точным. Более того, чем больше шум, тем меньше точность воспроизведения. В подразд. 12.1.1 аналогичная ситуация возникала при изучении классических каналов с использованием неравенства Фано, которое устанавливает связь между неопределенностью $H(X|Y)$ данных X на входе в канал при известных данных на выходе Y и вероятностью восстановления состояния X из Y . Существует очень полезный квантовый аналог описанного результата, который связывает обменную энтропию $S(\rho, \mathcal{E})$ с точностью воспроизведения запутанности состояний $F(\rho, \mathcal{E})$.

Теорема 12.9 (квантовое неравенство Фано). Пусть ρ — квантовое состояние и \mathcal{E} — квантовое преобразование, сохраняющее след. Тогда

$$S(\rho, \mathcal{E}) \leq H(F(\rho, \mathcal{E})) + (1 - F(\rho, \mathcal{E})) \log(d^2 - 1), \quad (12.112)$$

где $H(\cdot)$ — двоичная энтропия Шеннона.

Рассмотрение квантового неравенства Фано позволяет установить интересную закономерность: если обменная энтропия для какого-либо процесса велика, то точность воспроизведения запутанности состояний для этого процесса будет мала, т. е. запутанность систем R и Q плохо сохраняется. Более того, отметим, что в квантовом неравенстве Фано обменная энтропия $S(\rho, \mathcal{E})$ играет роль, аналогичную той, которую играет условная энтропия $H(X|Y)$ в классической теории информации.

Доказательство.

Чтобы доказать квантовое неравенство Фано, предположим, что $|i\rangle$ — ортонормированный базис для системы RQ , выбранный таким образом, чтобы первое состояние в базисе $|1\rangle$ совпадало с начальным состоянием $|RQ\rangle$. Для $p_j \equiv \langle i|\rho^{R'Q'}|i\rangle$ из результатов подразд. 11.3.3 следует, что

$$S(R', Q') \leq H(p_1, \dots, p_{d^2}), \quad (12.113)$$

где $H(p_j)$ — энтропия Шеннона набора $\{p_j\}$. Элементарные алгебраические выкладки дают

$$H(p_1, \dots, p_{d^2}) = H(p_1) + (1 - p_1)H\left(\frac{p_2}{1 - p_1}, \dots, \frac{p_{d^2}}{1 - p_1}\right). \quad (12.114)$$

Используя неравенство $H\left(\frac{p_2}{1 - p_1}, \dots, \frac{p_{d^2}}{1 - p_1}\right) \leq \log(d^2 - 1)$ и тождество $p_1 = F(\rho, \mathcal{E})$, получаем квантовое неравенство Фано

$$S(\rho, \mathcal{E}) \leq H(F(\rho, \mathcal{E})) + (1 - F(\rho, \mathcal{E})) \log(d^2 - 1). \quad (12.115)$$

■

12.4.2 Квантовое неравенство обработки данных

В подразд. 11.2.4 мы рассматривали классическое *неравенство обработки данных*. Напомним, что неравенство обработки данных устанавливает, что для марковских процессов $X \rightarrow Y \rightarrow Z$

$$H(X) \geq H(X:Y) \geq H(X:Z), \quad (12.116)$$

причем равенство в первом неравенстве имеет место тогда и только тогда, когда случайная величина X может быть точно восстановлена по Y . Следовательно, неравенство обработки данных обеспечивает необходимые и достаточные теоретико-информационные условия возможности исправления ошибок.

Существует квантовый аналог неравенства обработки данных, который можно применить к квантовому процессу, состоящему из двух стадий, которые можно описать квантовыми преобразованиями \mathcal{E}_1 и \mathcal{E}_2 ,

$$\rho \xrightarrow{\mathcal{E}_1} \rho' \xrightarrow{\mathcal{E}_2} \rho''. \quad (12.117)$$

Мы определяем квантовую *когерентную информацию* следующим образом:

$$I(\rho, \mathcal{E}) \equiv S(\mathcal{E}(\rho)) - S(\rho, \mathcal{E}). \quad (12.118)$$

Предполагается (но точно не известно), что когерентная информация в квантовой теории информации играет роль, аналогичную той, которую играет взаимная информация $H(X:Y)$ в классической теории информации. Это предположение основано в частности на том, что когерентная информация удовлетворяет квантовому неравенству обработки данных, аналогичному классическому неравенству обработки данных.

Теорема 12.10 (квантовое неравенство обработки данных). Пусть ρ — квантовое состояние и \mathcal{E}_1 и \mathcal{E}_2 — сохраняющие след квантовые преобразования. Тогда

$$S(\rho) \geq I(\rho, \mathcal{E}_1) \geq I(\rho, \mathcal{E}_2 \circ \mathcal{E}_1), \quad (12.119)$$

причем равенство в первом неравенстве имеет место тогда и только тогда, когда возможно *идеально обратить* преобразование \mathcal{E}_1 , т. е. существует сохраняющее след квантовое преобразование \mathcal{R} , такое, что $F(\rho, \mathcal{R} \circ \mathcal{E}) = 1$.

Сравнение с классическим неравенством обработки данных показывает, что когерентная информация в квантовом неравенстве обработки данных играет роль, идентичную той роли, которую играет взаимная информация в классическом неравенстве обработки данных. Конечно, эвристический аргумент такого рода нельзя рассматривать в качестве точного доказательства того, что когерентная информация является точным квантовым аналогом классической взаимной информации. Чтобы это доказать, должно быть получено соотношение между когерентной информацией и пропускной способностью квантового канала, подобное соотношению между классической взаимной информацией и классической пропускной способностью канала, однако, такое соотношение пока не установлено. (См. ссылки на некоторые работы в этом направлении в разд. «История и дополнительная литература» в конце главы.)

Как понятие идеальной обратимости, определенное в теореме 12.10, связано с более привычными понятиями, такими, которые используются, например, в контексте исправления квантовых ошибок? По определению, сохраняющее след квантовое преобразование \mathcal{E} является *идеально обратимым* по входному состоянию ρ , если существует такое сохраняющее след квантовое преобразование \mathcal{R} , что

$$F(\rho, \mathcal{R} \circ \mathcal{E}) = 1. \quad (12.120)$$

Однако, из пункта (4) [уравнения (9.143), (9.144)] следует, что квантовое преобразование идеально обратимо тогда и только тогда, когда для каждого состояния $|\psi\rangle$ из носителя ρ

$$(\mathcal{R} \circ \mathcal{E})(|\psi\rangle\langle\psi|) = |\psi\rangle\langle\psi|. \quad (12.121)$$

Это наблюдение связывает понятие идеальной обратимости с кодами, исправляющими квантовые ошибки. Напомним, что код, исправляющий квантовые ошибки, является подпространством некоторого большего гильбертова пространства, порожденным кодовыми словами. Для обеспечения устойчивости к шуму, вносимому квантовым преобразованием \mathcal{E} , необходимо, чтобы квантовое преобразование \mathcal{E} можно было обратить с помощью сохраняющего след обратного преобразования \mathcal{R} , т. е. для всех состояний $|\psi\rangle$ в данном коде должно выполняться равенство $(\mathcal{R} \circ \mathcal{E})(|\psi\rangle\langle\psi|) = |\psi\rangle\langle\psi|$. Это условие эквивалентно критерию идеальной обратимости из теоремы 12.10, т. е. $F(\rho, \mathcal{R} \circ \mathcal{E}) = 1$ для ρ , носителем которого является кодовое пространство.

Доказательство.

Квантовое неравенство обработки данных можно доказать, используя конструкцию из четырех систем: R и Q вводятся как и раньше, тогда как системы E_1 и E_2 находятся изначально в чистых состояниях, выбранных таким образом, что унитарное взаимодействие Q и E_1 определяет динамику \mathcal{E}_1 , а унитарное взаимодействие Q и E_2 — динамику \mathcal{E}_2 . Доказательство первой части квантового неравенства обработки данных основано на применении неравенства субаддитивности $S(R', E'_1) \leq S(R') + S(E'_1)$, что дает

$$I(\rho, \mathcal{E}_1) = S(\mathcal{E}_1(\rho)) - S(\rho, \mathcal{E}_1) \quad (12.122)$$

$$= S(Q') - S(E'_1) \quad (12.123)$$

$$= S(R', E'_1) - S(E'_1) \quad (12.124)$$

$$\leq S(R') + S(E'_1) - S(E'_1) = S(R') \quad (12.125)$$

$$= S(R) = S(Q) = S(\rho). \quad (12.126)$$

Доказательство второй части квантового неравенства обработки данных основано на применении неравенства сильной субаддитивности,

$$S(R'', E''_1, E''_2) + S(E''_1) \leq S(R'', E''_1) + S(E''_1, E''_2). \quad (12.127)$$

Поскольку состояние системы $R''Q''E''_1E''_2$ чистое, можно записать

$$S(R'', E''_1, E''_2) = S(Q''). \quad (12.128)$$

Ни одна из систем R и E_1 не включена во вторую стадию динамического процесса, в котором Q и E_2 взаимодействуют унитарно. Следовательно, их состояния не меняются в течение всей этой стадии: $\rho^{R''E''_1} = \rho^{R'E'_1}$. Однако, поскольку после выполнения первой стадии динамического процесса состояние системы RQE_1 чистое, имеем

$$S(R'', E''_1) = S(R', E'_1) = S(Q'). \quad (12.129)$$

Два других члена в неравенстве сильной субаддитивности (12.127) представляют обменные энтропии

$$S(E''_1) = S(E'_1) = S(\rho, \mathcal{E}_1); \quad S(E''_1, E''_2) = S(\rho, \mathcal{E}_2 \circ \mathcal{E}_1). \quad (12.130)$$

Подставляя эти выражения в (12.127), получаем неравенство

$$S(Q'') + S(\rho, \mathcal{E}_1) \leq S(Q') + S(\rho, \mathcal{E}_2 \circ \mathcal{E}_1), \quad (12.131)$$

которое можно переписать как вторую часть неравенства обработки данных, $I(\rho, \mathcal{E}_1) \leq I(\rho, \mathcal{E}_2 \circ \mathcal{E}_1)$.

Чтобы завершить доказательство, нужно показать, что \mathcal{E} идеально обратимо по входному состоянию ρ тогда и только тогда, когда первое неравенство в квантовом неравенстве обработки данных является равенством

$$S(\rho) = I(\rho, \mathcal{E}) = S(\rho') - S(\rho, \mathcal{E}). \quad (12.132)$$

Чтобы доказать необходимость этого условия обратимости, предположим, что \mathcal{E} можно идеально обратить по входному состоянию ρ с помощью обратного преобразования \mathcal{R} . Из второй части квантового неравенства обработки данных видно, что

$$S(\rho') - S(\rho, \mathcal{E}) \geq S(\rho'') - S(\rho, \mathcal{R} \circ \mathcal{E}). \quad (12.133)$$

Из условия обратимости следует, что $\rho'' = \rho$. Более того, из квантового неравенства Фано (12.112) и условия идеальной обратимости $F(\rho, \mathcal{R} \circ \mathcal{E}) = 1$ следует, что $S(\rho, \mathcal{R} \circ \mathcal{E}) = 0$. Поэтому вторую часть квантового неравенства обработки данных для $\rho \rightarrow \mathcal{E}(\rho) \rightarrow (\mathcal{R} \circ \mathcal{E})(\rho)$ можно переписать в виде

$$S(\rho') - S(\rho, \mathcal{E}) \geq S(\rho). \quad (12.134)$$

Используя первую часть квантового неравенства обработки данных, $S(\rho) \geq S(\rho') - S(\rho, \mathcal{E})$, получаем

$$S(\rho') - S(\rho, \mathcal{E}) \geq S(\rho) \quad (12.135)$$

для любого \mathcal{E} , которое идеально обратимо по входному состоянию ρ .

Теперь приведем конструктивное доказательство того, что выполнение условия

$$S(\rho) = S(\rho') - S(\rho, \mathcal{E}) \quad (12.136)$$

достаточно для того, чтобы квантовое преобразование \mathcal{E} было обратимо по входному состоянию ρ . Заметив, что $S(\rho) = S(Q) = S(R) = S(R')$, $S(\rho') = S(Q') = S(R', E')$ и $S(\rho, \mathcal{E}) = S(E')$, мы убеждаемся, что $S(R') + S(E') = S(R', E')$; как показано в подразд. 11.3.4, последнее равенство эквивалентно условию $\rho^{R'E'} = \rho^{R'} \otimes \rho^{E'}$. Предположим, что начальное состояние системы Q имеет вид $\rho = \sum_j p_j |i\rangle\langle i|$ и что мы расширяем это состояние до чистого состояния $|RQ\rangle = \sum_j \sqrt{p_j} |i\rangle|i\rangle$, где R — первая система, а Q — вторая система.

Заметим, что $\rho^{R'} = \rho^R = \sum_j p_j |i\rangle\langle i|$. Кроме того, предположим, что $\rho^{E'} = \sum_j q_j |j\rangle\langle j|$ для некоторого ортонормированного базиса $|j\rangle$, так что

$$\rho^{R'E'} = \sum_{ij} p_i q_j |i\rangle\langle i| \otimes |j\rangle\langle j|. \quad (12.137)$$

Эта матрица имеет собственные векторы $|i\rangle|j\rangle$ и поэтому при помощи разложения Шмидта можно записать состояние системы $R'Q'E'$ после применения квантового преобразования \mathcal{E} в виде

$$|R'Q'E'\rangle = \sum_{ij} \sqrt{p_i q_j} |i\rangle|i,j\rangle|j\rangle, \quad (12.138)$$

где $|i,j\rangle$ — некоторый ортонормированный набор состояний для системы Q . Определим проекторы P_j при помощи тождества $P_j \equiv \sum_i |i,j\rangle\langle i,j|$. Процедура восстановления состоит в том, что сначала нужно произвести измерение, описанное проекторами P_j , которое дает состояние $|j\rangle$ среды, а затем выполнить унитарную операцию U_j , зависящую от j , которая возвращает состояние $|i,j\rangle$ в состояние $|i\rangle$: $U_j|i,j\rangle \equiv |i\rangle$. Таким образом, j — результат измерения (синдром) и U_j — соответствующая операция восстановления. Полная процедура восстановления может быть описана следующим образом

$$\mathcal{R} \equiv \sum_j U_j P_j \sigma P_j U_j^\dagger. \quad (12.139)$$

Проекторы P_j ортогональны, что следует из ортогональности состояний $|i,j\rangle$, однако их набор может быть не полным. Чтобы квантовое преобразование \mathcal{R} сохраняло след, необходимо в заданный набор проекторов добавить дополнительный проектор $\tilde{P} \equiv I - \sum_j P_j$.

Конечное состояние системы RQE после применения обратного преобразования имеет вид

$$\begin{aligned} \sum_j U_j P_j |R'Q'E'\rangle\langle R'Q'E'| P_j U_j^\dagger \\ = \sum_j \sum_{i_1 i_2} \sqrt{p_{i_1} p_{i_2}} q_j |i_1\rangle\langle i_2| \otimes (U_j |i_1, j\rangle\langle i_2, j| U_j^\dagger) \otimes |j\rangle\langle j| \end{aligned} \quad (12.140)$$

$$= \sum_{i_1 i_2} \sqrt{p_{i_1} p_{i_2}} |i_1\rangle\langle i_2| \otimes |i_1\rangle\langle i_2| \otimes \rho^{E'}, \quad (12.141)$$

откуда видно, что $\rho^{R''Q''} = \rho^{RQ}$, и, следовательно, $F(\rho, \mathcal{R} \circ \mathcal{E}) = 1$, т. е. преобразование \mathcal{E} идеально обратимо по входному состоянию ρ , что и требовалось доказать. ■

Это завершает доказательство теоретико-информационных условий обратимости для квантовых преобразований, сохраняющих след. Интуитивно можно понять этот результат, предположив, что Q — элемент памяти в квантовом компьютере, R — остальная часть квантового компьютера и E — среда, взаимодействие которой с Q порождает шум. Более элегантно теоретико-информационное

условие обратимости можно представить как утверждение, что состояние среды E' после воздействия шума не должно быть коррелированным с состоянием остальной части квантового компьютера R' . В более понятных терминах это означает, что ошибку можно исправить тогда, когда среда ничего «не узнает» об остальной части квантового компьютера через взаимодействие с Q' !

Более конкретно, предположим, что Q — система из n кубитов и C — квантовый $[n, k]$ -код, исправляющий ошибки, в этой системе с ортонормированными кодовыми словами $|x\rangle$ и проектором P на пространство кода. Рассмотрим матрицу плотности $P/2^k$, которая может быть «расширена» до чистого состояния RQ :

$$\frac{1}{\sqrt{2^k}} \sum_x |x\rangle|x\rangle. \quad (12.142)$$

Предположим, что этот код может исправлять произвольные ошибки на некотором подмножестве Q_1 кубитов. Этот код, в частности, способен исправить ошибку, которая приводит к замене этих кубитов на кубиты в некотором стандартном состоянии. Теоретико-информационное условие обратимости, а именно $\rho^{R'E'} = \rho^R \otimes \rho^{E'}$, в этом случае можно представить как $\rho^{RQ_1} = \rho^R \otimes \rho^{Q_1}$. Таким образом, система R и подсистема Q_1 , ошибки в которой могут быть исправлены, должны быть изначально некоррелированы, чтобы было возможно исправление ошибок!

Упражнение 12.14. Покажите, что условие $\rho^{RQ_1} = \rho^R \otimes \rho^{Q_1}$ также является достаточным для того, чтобы можно было исправлять ошибки в подсистеме Q_1 .

Аргументы, использованные в доказательстве квантового неравенства обработки данных, можно применить для доказательства множества других неравенств. Например, пусть мы имеем квантовую систему Q в состоянии ρ , которое подвергается квантовому преобразованию \mathcal{E} . Первая часть неравенства обработки данных получается, если применить неравенство субаддитивности для энтропии к системам R' и E' . Если вместо этого неравенство субаддитивности применить к системам Q' и E' , то получим

$$S(\rho) = S(R) = S(R') = S(Q', E') \leq S(Q') + S(E') = S(\mathcal{E}(\rho)) + S(\rho, \mathcal{E}). \quad (12.143)$$

Следовательно,

$$\Delta S + S(\rho, \mathcal{E}) \geq 0, \quad (12.144)$$

где $\Delta S \equiv S(\mathcal{E}(\rho)) - S(\rho)$ — изменение энтропии, вызванное преобразованием \mathcal{E} . Грубо говоря, это неравенство устанавливает, что сумма изменения энтропии системы и изменения энтропии среды должна быть неотрицательна. Это соответствует второму началу термодинамики и будет использовано в подразд. 12.4.4 при проведении термодинамического анализа исправления квантовых ошибок!

Упражнение 12.15. Используя все возможные комбинации свойств субаддитивности и сильной субаддитивности, получите другие неравенства для второй стадии квантового процесса $\rho \rightarrow \rho' = \mathcal{E}_1(\rho) \rightarrow \rho'' = (\mathcal{E}_2 \circ \mathcal{E}_1)(\rho)$, и выразите

результаты, когда это возможно, в терминах обменной энтропии и энтропий $S(\rho), S(\rho'), S(\rho'')$. Если в этих терминах невозможно выразить величину, появляющуюся в одном из таких неравенств, представьте ее, используя только ρ и элементы преобразования $\{E_j\}$ для \mathcal{E}_1 и $\{F_k\}$ для \mathcal{E}_2 .

12.4.3 Квантовая граница Синглтона

Теоретико-информационный подход к исправлению квантовых ошибок может быть использован для доказательства замечательной границы для способности квантовых кодов исправлять ошибки, а именно *квантовой границы Синглтона*. Напомним, что $[n, k, d]$ -код использует n кубитов, чтобы закодировать k кубитов, и способен исправить ошибки (упр. 10.45) в $d - 1$ кубитах. Квантовая граница Синглтона выражается неравенством $n - k \geq 2(d - 1)$ в противоположность классической границе Синглтона (упр. 10.21), которая для классического $[n, k, d]$ -кода имеет вид $n - k \geq d - 1$. Поскольку квантовый код для исправления ошибок в t кубитах должен иметь кодовое расстояние, по меньшей мере, $2t + 1$, то $n - k \geq 4t$. Поэтому, например код для $k = 1$ кубита, способный исправлять ошибки в одном ($t = 1$) из кодирующих кубитов, должен удовлетворять условию $n - 1 \geq 4$, т. е. n должно быть, по меньшей мере, равно 5, так что пятикубитовый код, описанный в гл. 10, является наименьшим возможным кодом для решения этой задачи.

Доказательство квантовой границы Синглтона основывается на теоретико-информационных методах, которые мы использовали для анализа исправления квантовых ошибок. Предположим, что код — это 2^k -мерное подпространство, связанное с системой Q , с ортонормированным базисом, обозначенным через $|x\rangle$. Введем 2^k -мерную вспомогательную систему R также с 2^k ортонормированными базисными векторами, обозначенными через $|x\rangle$, и рассмотрим запутанное состояние системы RQ

$$|RQ\rangle = \frac{1}{\sqrt{2^k}} \sum_x |x\rangle|x\rangle. \quad (12.145)$$

Мы делим n кубитов системы Q на три отдельных блока, первый и второй из которых, Q_1 и Q_2 , состоят из $d - 1$ кубитов каждый, а третий Q_3 содержит остальные $n - 2(d - 1)$ кубитов. Поскольку код имеет кодовое расстояние d , любое множество из $d - 1$ ошибок можно исправить, и, следовательно, можно исправить ошибки либо в Q_1 , либо в Q_2 . Отсюда следует, что R и Q_1 должны быть некоррелированы, как R и Q_2 . Учитывая это наблюдение и субаддитивность энтропии, а также то, что состояние системы $RQ_1Q_2Q_3$ чистое, получаем

$$S(R) + S(Q_1) = S(R, Q_1) = S(Q_2, Q_3) \leq S(Q_2) + S(Q_3), \quad (12.146)$$

$$S(R) + S(Q_2) = S(R, Q_2) = S(Q_1, Q_3) \leq S(Q_1) + S(Q_3). \quad (12.147)$$

Сложение этих двух неравенств дает

$$2S(R) + S(Q_1) + S(Q_2) \leq S(Q_1) + S(Q_2) + 2S(Q_3). \quad (12.148)$$

Сокращая одинаковые слагаемые и подставляя $S(R) = k$, получаем $k \leq S(Q_3)$. Однако, Q_3 имеет размер $n - 2(d - 1)$ кубитов, так что $S(Q_3) \leq n - 2(d - 1)$, следовательно, $k \leq n - 2(d - 1)$, откуда $2(d - 1) \leq n - k$. Это и есть квантовая граница Синглтона.

В качестве примера использования границы Синглтона рассмотрим деполяризующий канал $\mathcal{E}(\rho) = (1 - p)\rho + p/3(X\rho X + Y\rho Y + Z\rho Z)$. Предположим, что деполяризующий канал действует независимо на большое число n кубитов. Если $p > \frac{1}{4}$, то больше четверти этих кубитов будут ошибочны, так что любой код, способный восстанавливать кубиты, должен иметь $t > n/4$. Однако, из квантовой границы Синглтона видно, что $n - k \geq 4t > n$ и поэтому k должно быть отрицательным, т.е. в этом случае невозможно закодировать никакие кубиты. Таким образом, квантовая граница Синглтона позволяет сделать вывод, что при $p > \frac{1}{4}$ пропускная способность деполяризующего канала для квантовой информации равна нулю!

12.4.4 Исправление квантовых ошибок, охлаждение и демон Максвелла

Исправление квантовых ошибок можно рассматривать как процесс охлаждения, способный поддерживать энтропию квантовой системы постоянной, несмотря на влияние шумовых процессов, которые стремятся ее изменить. Действительно, с этой точки зрения исправление квантовых ошибок может показаться странным, поскольку оно позволяет уменьшать энтропию квантовой системы, что, очевидно, противоречит второму началу термодинамики! Чтобы понять, что второе начало термодинамики при этом все-таки не нарушается, мы анализируем исправление квантовых ошибок подобно тому, как проводили анализ демона Максвелла во вставке 3.5. Исправление квантовых ошибок по существу, особый тип демона Максвелла; мы можем представить себе «демона», осуществляющего измерения синдрома, а затем исправляющего ошибки в соответствии с полученным результатом. Так же, как при анализе классического демона Максвелла, запоминание синдрома в памяти демона приводит к рассеянию энергии в соответствии с принципом Ландауэра. Поскольку любая память ограничена, демон должен, в конце концов, начать стирать информацию из своей памяти, чтобы освободить место для новых результатов измерений. Согласно принципу Ландауэра, стирание одного бита информации из памяти увеличивает общую энтропию квантовой системы, демона и среды, по меньшей мере, на один бит.

Можно рассмотреть «цикл» исправления ошибки, состоящий из четырех этапов, как показано на рис. 12.9.

1. Система, находящаяся изначально в состоянии ρ , подвергается воздействию квантового шума, что переводит ее в состояние ρ' . В типичных сценариях исправления ошибки рассматриваются случаи, когда энтропия системы возрастает, $S(\rho') > S(\rho)$, хотя это и не обязательно.
2. Демон осуществляет измерение (синдрома) над состоянием ρ' , которое

описывается при помощи операторов измерения $\{M_m\}$, что дает результат m с вероятностью $p_m = \text{tr}(M_m \rho M_m^\dagger)$ и приводит к состоянию $\rho'_m = M_m \rho M_m^\dagger / p_m$.

3. Демон, используя унитарную операцию V_m (операцию восстановления), создает конечное состояние системы

$$\rho''_m = V_m \rho'_m V_m^\dagger = \frac{V_m M_m \rho' M_m^\dagger V_m^\dagger}{p_m}. \quad (12.149)$$

4. Цикл начинается заново. Чтобы это был действительно цикл и исправление ошибки было успешным, мы должны иметь $\rho''_m = \rho$ для каждого результата измерения m .

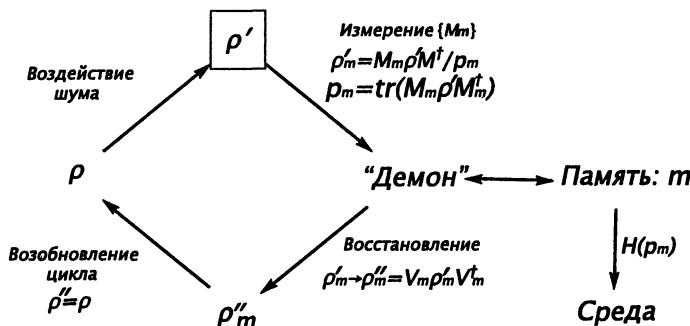


Рис. 12.9. Цикл исправления квантовой ошибки.

Сейчас мы покажем, что любое уменьшение энтропии в течение второго и третьего этапов исправления ошибки сопровождается увеличением энтропии среды, при этом общая энтропия системы и среды может только увеличиваться. После третьего этапа только запись результата измерения m сохраняется в памяти демона. Запуская следующий цикл, демон должен стереть свою запись результата измерения, что приводит к увеличению энтропии среды в соответствии с принципом Ландауэра. Число битов, которые должны быть стерты, определяется представлением, которое демон использует, чтобы сохранить результат измерения m . Согласно теореме Шеннона о кодировании для канала без шума, в среднем требуется, по меньшей мере, $H(p_m)$ битов, чтобы запомнить результат измерения, и, следовательно, один цикл исправления ошибки приводит к увеличению энтропии среды, в среднем, на $H(p_m)$ битов, когда стирается запись измерения.

До исправления ошибки квантовая система находилась в состоянии ρ' . После исправления ошибки квантовая система находится в состоянии ρ , так что полное изменение энтропии системы из-за исправления ошибки $\Delta S = S(\rho) - S(\rho')$. Прирост энтропии $H(p_m)$ (в среднем) связан со стиранием записи измерения, так что полное изменение энтропии равно $\Delta(S) + H(p_m)$. Наша задача —

оценить эти термодинамические потери и продемонстрировать, что второе начало термодинамики никогда не нарушается. Чтобы сделать это, полезно ввести два понятия. Пусть \mathcal{E} представляет шум, который имеет место во время первого этапа цикла исправления ошибки, $\rho \rightarrow \rho' = \mathcal{E}(\rho)$, и \mathcal{R} — квантовое преобразование исправления ошибки,

$$\mathcal{R}(\sigma) \equiv \sum_m V_m M_m \sigma M_m^\dagger V_m^\dagger. \quad (12.150)$$

Для входного состояния ρ' w -матрица этого процесса имеет элементы $W_{mn} = \text{tr}(V_m M_m \rho' M_n^\dagger V_n^\dagger)$, и, следовательно, каждый диагональный элемент $W_{mm} = \text{tr}(V_m M_m \rho' M_m^\dagger V_m^\dagger) = \text{tr}(M_m \rho M_m^\dagger)$ является вероятностью p_m , с которой демон получает результат m при измерении синдрома ошибки. Согласно теореме 11.9, энтропия диагональных элементов W , по меньшей мере, так же велика как энтропия W , так что

$$H(p_m) \geq S(W) = S(\rho', \mathcal{R}). \quad (12.151)$$

Равенство имеет место тогда и только тогда, когда операторы $V_m M_m$ представляют каноническое разложение \mathcal{R} по отношению к ρ' , так что недиагональные элементы в W исключаются. Из равенства (12.144) следует

$$\Delta S + S(\rho', \mathcal{R}) = S(\rho) - S(\rho') + S(\rho', \mathcal{R}) \geq 0. \quad (12.152)$$

Используя этот результат и формулу (12.151), получаем $\Delta S + H(p_m) \geq 0$. Но $\Delta S + H(p_m)$ представляет собой полное изменение энтропии, вызванное процедурой исправления ошибки. Мы делаем вывод, что исправление ошибки может привести лишь к *увеличению* общей энтропии, причем любое уменьшение энтропии системы из-за исправлении ошибки компенсируется увеличением энтропии, когда синдром ошибки стирается.

Упражнение 12.16. Покажите, что в случае, когда \mathcal{R} идеально исправляет \mathcal{E} для данного входного ρ , неравенство

$$S(\rho) - S(\rho') + S(\rho', \mathcal{R}) \geq 0 \quad (12.153)$$

должно превратиться в равенство.

12.5 Запутанность как физический ресурс

До сих пор мы рассматривали квантовую информацию, уделяя особое внимание ресурсам, которые мало отличаются от ресурсов классической теории информации. Для удобства на рис. 12.10 дана сводная таблица многих квантовых и классических результатов. Одной из замечательных особенностей квантовых вычислений и квантовой информации является то, что квантовая механика содержит принципиально новые типы ресурсов, которые значительно отличаются от понятия информации в классической теории. По-видимому, из этих ресурсов лучше всего исследована квантовая запутанность, к рассмотрению которой мы сейчас и перейдем.

Теория информации	
Классическая	Квантовая
Энтропия Шеннона	Энтропия фон Неймана
$H(X) = -\sum_x p(x) \log p(x)$	$S(\rho) = \text{tr}(\rho \log \rho)$
Различимость и доступная информация	
Буквы всегда различимы	Граница Холево
$N = X $	$H(X:Y) \leq S(\rho) - \sum_x p_x S(\rho_x)$
	$\rho = \sum_x p_x \rho_x$
Кодирование для канала без шума	
Теорема Шеннона	Теорема Шумахера
$n_{\text{биты}} = H(X)$	$n_{\text{кубиты}} = S\left(\sum_x p_x \rho_x\right)$
Пропускная способность каналов с шумом для классической информации	
Теорема Шеннона о кодировании для канала с шумом	Теорема Холево–Шумахера–Вестморланда
$C(N) = \max_{p(x)} H(X:Y)$	$C^{(1)}(\mathcal{E}) = \max_{\{\rho(x), \rho'(x)\}} \left[S(\rho') - \sum_x p_x S(\rho'_x) \right]$ $\rho_x = \mathcal{E}(\rho_x), \quad \rho' = \sum_x p_x \rho_x$
Теоретико-информационные соотношения	
Неравенство Фано	Квантовое неравенство Фано
$H(p_e) + p_e \log(X - 1) \geq H(X Y)$	$H(F(\rho, \mathcal{E})) + (1 - F(\rho, \mathcal{E})) \log(d^2 - 1) \geq S(\rho, \mathcal{E})$
Взаимная информация $H(X:Y) = H(Y) - H(Y X)$	Когерентная информация $I(\rho, \mathcal{E}) = S(\mathcal{E}(\rho)) - S(\rho, \mathcal{E})$
Неравенство обработки данных $X \rightarrow Y \rightarrow Z$	Квантовое неравенство обработки данных $\rho \rightarrow \mathcal{E}_1(\rho) \rightarrow (\mathcal{E}_2 \circ \mathcal{E}_1)(\rho)$
$H(X) \geq H(X:Y) \geq H(X:Z)$	$S(\rho) \geq I(\rho, \mathcal{E}_1) \geq I(\rho, \mathcal{E}_2 \circ \mathcal{E}_1)$

Рис. 12.10. Некоторые важные классические информационные соотношения и их квантовые аналоги.

Мы говорим «лучше всего исследована», но этим не все сказано! Еще очень далеко до создания общей теории квантовой запутанности. Тем не менее, на пути к созданию общей теории уже достигнуты определенные успехи, раскрывающие загадочную структуру запутанных состояний и некоторые важные связи между свойствами квантовых каналов с шумом и различными типами преобразований запутанности. Мы сделаем только краткий обзор того, что уже известно, уделяя особое внимание свойствам преобразования запутанности, разделенной между двумя системами, Алисой и Бобом. Конечно, очень интересно разработать общую теорию запутанности для многокомпонентных систем, но как это сделать — не очень понятно.

12.5.1 Преобразование запутанности чистого состояния системы из двух компонент

Отправной точкой нашего исследования является следующий простой вопрос. В какие запутанные состояния $|\varphi\rangle$ Алиса и Боб могут преобразовать запутанное чистое состояние $|\psi\rangle$, которое они разделяют, при условии, что каждый из них может выполнять произвольные операции над своими локальными системами, включая измерение, и использовать только классическую связь? Квантовая коммуникация между Алисой и Бобом не разрешена, что ограничивает класс преобразований, которые они могут выполнить.

В качестве примера предположим, что Алиса и Боб разделяют запутанную пару кубитов в состоянии Белла $(|00\rangle + |11\rangle)/\sqrt{2}$. Алиса выполняет измерение с двумя возможными результатами, которое описывается операторами M_1 и M_2 :

$$M_1 = \begin{bmatrix} \cos \theta & 0 \\ 0 & \sin \theta \end{bmatrix}; \quad M_2 = \begin{bmatrix} \sin \theta & 0 \\ 0 & \cos \theta \end{bmatrix}. \quad (12.154)$$

После измерения состояние представляет собой либо $\cos \theta |00\rangle + \sin \theta |11\rangle$, либо $\cos \theta |11\rangle + \sin \theta |00\rangle$ в зависимости от результата измерения 1 или 2. В последнем из этих двух случаев Алиса применяет элемент NOT после измерения и в результате получает состояние $\cos \theta |01\rangle + \sin \theta |10\rangle$. Затем она посылает результат измерения (1 или 2) Бобу, который ничего не делает со своим кубитом, если результат измерения равен 1, и применяет элемент NOT, если результат равен 2. Конечным состоянием совместной системы будет $\cos \theta |11\rangle + \sin \theta |00\rangle$, независимо от результата измерения, который получила Алиса. Таким образом, Алиса и Боб преобразовали свой начальный запутанный ресурс $(|00\rangle + |11\rangle)/\sqrt{2}$ в состояние $\cos \theta |00\rangle + \sin \theta |11\rangle$, выполняя только локальные операции над своими индивидуальными системами и используя классическую связь.

Не совсем очевидно значение проблемы преобразования запутанности. Класс преобразований, которые мы разрешили — локальные операции и классическая коммуникация (ЛОКК) — вызывает определенный интерес. Оказалось, что обобщения проблемы преобразования запутанности обнаруживают глубокие и неожиданные связи с исправлением квантовых ошибок. Более того, методы, применяемые при решении этой проблемы, представляют большой интерес

и дают возможность глубже понять свойства запутанности. В частности, мы обнаружим тесную связь между запутанностью и теорией *мажоризации*.

Прежде чем приступить к изучению преобразований запутанности, познакомимся с некоторыми существенными фактами, касающимися мажоризации. Мажорирование — это отношение порядка для d -мерных действительнозначных векторов, предназначенное для формального описания того, что один вектор более или менее хаотичен по сравнению с другим. Более точно, предположим, что $x = (x_1, \dots, x_d)$ и $y = (y_1, \dots, y_d)$ — два d -мерных вектора. Мы используем обозначение x^\downarrow для вектора, который состоит из компонент вектора x , расположенных в порядке невозрастания, так что, например, x_1^\downarrow — наибольшая компонента x . Мы говорим, что y мажорирует x , записывая $x \prec y$, если $\sum_{j=1}^k x_j^\downarrow \leq \sum_{j=1}^k y_j^\downarrow$ для $k = 1, \dots, d$, причем неравенство переходит в равенство при $k = d$. Как это связано с понятием беспорядка, скоро станет ясно!

Связь между мажоризацией и преобразованием запутанности формулируется легко, но довольно неожиданно. Предположим, что $|\psi\rangle$ и $|\varphi\rangle$ — состояния совместной системы Алиса–Боб. Определим $\rho_\psi \equiv \text{tr}_B(|\psi\rangle\langle\psi|)$, $\rho_\varphi \equiv \text{tr}_B(|\varphi\rangle\langle\varphi|)$ как соответствующие приведенные матрицы плотности системы Алисы, и пусть λ_ψ и λ_φ — векторы, компоненты которых являются собственными значениями ρ_ψ и ρ_φ . Мы покажем, что $|\psi\rangle$ можно преобразовать в $|\varphi\rangle$ при помощи ЛОКК тогда и только тогда, когда $\lambda_\psi \prec \lambda_\varphi$! Чтобы продемонстрировать это, приведем некоторые простые сведения о мажоризации.

Упражнение 12.17. Покажите, что $x \prec y$ тогда и только тогда, когда для всех действительных t : $\sum_{j=1}^d \max(x_j - t, 0) \leq \sum_{j=1}^d \max(y_j - t, 0)$ и $\sum_{j=1}^d x_j = \sum_{j=1}^d y_j$.

Упражнение 12.18. Используя результат предыдущего упражнения, покажите, что множество x таких, что $x \prec y$, выпуклое.

Приведенное ниже утверждение позволяет глубже вникнуть в понятие мажорирования, показывая, что $x \prec y$ тогда и только тогда, когда x можно представить в виде выпуклой комбинации перестановок y . На неформальном языке $x \prec y$, если x — более хаотичен, чем y в том смысле, что x можно получить путем перестановки элементов y и смешивания полученных векторов. Это утверждение — один из наиболее полезных результатов в теории мажоризации.

Утверждение 12.11. $x \prec y$ тогда и только тогда, когда $x = \sum_j p_j P_j y$ для некоторого распределения вероятностей p_j и перестановочных матриц P_j .

Доказательство.

Предположим, что $x \prec y$. Без потери общности можно предположить, что $x = x^\downarrow$ и $y = y^\downarrow$. Докажем, что $x = \sum_j p_j P_j y$, индукцией по размерности d . Для $d = 1$ результат ясен. Предположим, что x и y представляют собой $d + 1$ -мерные векторы, такие, что $x \prec y$. Тогда $x_1 \leq y_1$. Выберем j таким, что $y_j \leq x_1 \leq y_{j-1}$ и зададим t в пределах $[0, 1]$ так, что $x_1 = ty_1 + (1-t)y_j$. Определим выпуклую комбинацию перестановок как $D \equiv tI + (1-t)T$, где T — перестановочная матрица, которая переставляет первый и j -й элементы вектора. Тогда

$$Dy = (x_1, y_2, \dots, y_{j-1}, (1-t)y_1 + ty_j, y_{j+1}, \dots, y_{d+1}). \quad (12.155)$$

Пусть $x' \equiv (x_2, \dots, x_{d+1})$ и $y' \equiv (y_2, \dots, y_{j-1}, (1-t)y_1 + ty_j, y_{j+1}, \dots, y_{d+1})$. В упр. 12.19 предлагается показать, что $x' \prec y'$. Из предположения индукции $x' = \sum_j p'_j P'_j y'$ для вероятностей p_j и перестановочных матриц P'_j , откуда $x = (\sum_j p'_j P'_j) Dy$, где P'_j расширены до размерности $d+1$ (они действуют три-вально на первый элемент). Поскольку $D = (tI + (1-t)T)$ и произведение перестановочных матриц есть перестановочная матрица, получаем искомый результат.

Упражнение 12.19. Проверьте, что $x' \prec y'$.

Наоборот, предположим, что $x = \sum_j p_j P_j y$. Ясно, что $P_j y \prec y$, и из упр. 12.18 следует, что $x = \sum_j p_j P_j y \prec y$. ■

Матрицы, которые являются выпуклыми комбинациями перестановочных матриц, обладают многими интересными свойствами. Заметим, например, что элементы такой матрицы должны быть неотрицательными, а каждая строка и каждый столбец матрицы должны в сумме давать единицу. Матрица с такими свойствами называется *дважды стохастической* матрицей. Согласно *теореме Биркгофа*, дважды стохастические матрицы в точности соответствуют матрицам, которые можно представить как выпуклые комбинации перестановочных матриц. Мы не будем здесь доказывать теорему Биркгофа (см. разд. «История и дополнительная литература» в конце главы), ограничимся лишь ее формулировкой.

Теорема 12.12 (теорема Биркгофа). Матрица D размерности $d \times d$ является дважды стохастической (т. е. имеет неотрицательные элементы и сумма элементов каждой строки и сумма элементов каждого столбца равны 1) тогда и только тогда, когда D можно представить в виде выпуклой комбинации перестановочных матриц $D = \sum_j p_j P_j$.

Из теоремы Биркгофа и утверждения 12.11 следует, что $x \prec y$ тогда и только тогда, когда $x = Dy$ для некоторой дважды стохастической матрицы D . Этот результат позволяет доказать замечательное и полезное операторное обобщение утверждения 12.11. Пусть H и K — два эрмитовых оператора. Мы говорим, что $H \prec K$, если $\lambda(H) \prec \lambda(K)$, где $\lambda(H)$ — вектор собственных значений эрмитова оператора H .

Теорема 12.13. Пусть H и K — эрмитовы операторы. $H \prec K$ тогда и только тогда, когда существует распределение вероятностей p_j и унитарные матрицы U_j такие, что

$$H = \sum_j p_j U_j K U_j^\dagger. \quad (12.156)$$

Доказательство.

Пусть $H \prec K$. Тогда из утверждения 12.11 следует, что $\lambda(H) = \sum_j p_j P_j \lambda(K)$. Пусть $\Lambda(H)$ обозначает диагональную матрицу, элементы которой являются собственными значениями H . Тогда векторное уравнение $\lambda(H) = \sum_j p_j P_j \lambda(K)$ может быть записано в виде

$$\Lambda(H) = \sum_j p_j P_j \Lambda(K) P_j^\dagger. \quad (12.157)$$

Но $H = V\Lambda(H)V^\dagger$ и $\Lambda(K) = WKW^\dagger$ для некоторых унитарных матриц V и W , так что $H = \sum_j p_j P_j U_j K U_j^\dagger$, где $U_j \equiv VP_j W$ — унитарная матрица.

Наоборот, предположим, что $H = \sum_j p_j U_j K U_j^\dagger$. Так же как и раньше, это эквивалентно $\Lambda(H) = \sum_j p_j V_j \Lambda(K) V_j^\dagger$ для некоторых унитарных матриц V_j . Записывая элементы матриц V_j в виде $V_{j,kl}$, имеем

$$\lambda(H)_k = \sum_{jl} p_j V_{j,kl} \lambda(K)_l V_{j,lk}^\dagger = \sum_{jl} p_j |V_{j,kl}|^2 \lambda(K)_l. \quad (12.158)$$

Введем матрицу D с элементами $D_{kl} \equiv \sum_j p_j |V_{j,kl}|^2$, так что $\lambda(H) = D\lambda(K)$. Элементы матрицы D неотрицательны по определению, и сумма элементов каждой строки и сумма элементов каждого столбца равна единице, поскольку строки и столбцы унитарной матрицы являются единичными векторами, т. е. D — дважды стохастическая матрица и, следовательно, $\lambda(H) \prec \lambda(K)$. ■

Теперь мы располагаем всеми фактами, касающимися мажоризации, которые необходимы при изучении ЛОКК-преобразований запутанности чистого состояния системы из двух компонент. Прежде всего сведем проблему изучения общих протоколов с двусторонней классической связью к протоколам с односторонней классической связью.

Утверждение 12.14. Пусть $|\psi\rangle$ может быть преобразовано в $|\varphi\rangle$ посредством ЛОКК. Тогда это преобразование можно выполнить по протоколу, который включает только следующие этапы: Алиса проводит единственное измерение, которое описывается операторами измерения M_j , посыпает полученный результат j Бобу, который применяет унитарный оператор U_j к своей системе.

Доказательство.

Без потери общности мы можем предложить протокол, который включает следующие этапы: Алиса проводит измерение, посыпает полученный результат Бобу. Выполнив измерение (которое может зависеть от информации, полученной от Алисы), Боб отправляет полученный результат Алисе, которая проводит измерение... и т. д. Идея доказательства — показать, что эффект любого измерения, которое выполняет Боб, может воспроизвести Алиса (с одним небольшим уточнением), так что все действия Боба могут быть на самом деле заменены действиями Алисы! Чтобы убедиться в этом, допустим, что Боб выполняет измерение, описываемое операторами M_j , над чистым состоянием $|\psi\rangle$. Предположим, что это чистое состояние имеет разложение Шмидта $|\psi\rangle = \sum_l \sqrt{\lambda_l} |l_A\rangle |l_B\rangle$. Введем операторы N_j , действующие на систему Алисы, которые имеют такие же матричные элементы в базисе $\{|l_A\rangle\}$, что и операторы Боба M_j в базисе $\{|l_B\rangle\}$, т. е., если $M_j = \sum_{kl} M_{j,kl} |k_B\rangle \langle l_B|$, то

$$N_j \equiv \sum_{kl} M_{j,kl} |k_A\rangle \langle l_A|. \quad (12.159)$$

Предположим, что Боб выполняет измерение, описываемое операторами измерения M_j . Тогда состояние после измерения $|\psi_j\rangle \sim M_j |\psi\rangle =$

$\sum_{kl} M_{j,kl} \sqrt{\lambda_l} |l_A\rangle |k_B\rangle$ с вероятностью $\sum_{kl} \lambda_l |M_{j,kl}|^2$. С другой стороны, если Алиса делает измерение, описываемое операторами N_j , то состояние после измерения $|\varphi_j\rangle \sim N_j |\psi\rangle = \sum_{kl} M_{j,kl} \sqrt{\lambda_l} |k_A\rangle |l_B\rangle$ с вероятностью $\sum_{kl} \lambda_l |M_{j,kl}|^2$. Отметим, что состояния $|\psi_j\rangle$ и $|\varphi_j\rangle$ переходят друг в друга при отображении $|k_A\rangle \leftrightarrow |k_B\rangle$, и, следовательно, должны иметь одни и те же компоненты Шмидта. Из упр. 2.80 следует, что существуют унитарный оператор U_j , действующий на систему Алисы, и оператор V_j , действующий на систему Боба, такие, что $|\psi_j\rangle = (U_j \otimes V_j) |\varphi_j\rangle$. Следовательно, измерение, описываемое операторами M_j , которое выполняет Боб, эквивалентно измерению Алисы, описываемому операторами $U_j N_j$, с последующим выполнением Бобом унитарного преобразования V_j . Таким образом, измерение Боба над известным чистым состоянием может быть промоделировано с помощью измерения, выполняемого Алисой, и унитарного преобразования, которое производит Боб.

Пусть Алиса и Боб выполняют протокол из нескольких циклов, преобразующий $|\varphi\rangle$ в $|\psi\rangle$. Без потери общности можно предположить, что первый цикл протокола состоит в выполнении Алисой измерения и посылке полученного результата Бобу. Второй цикл включает выполнение Бобом измерения (возможно, зависящего от результата измерения Алисы) и посылку полученного результата Алисе. Вместо этого, однако, мы можем предположить, что это измерение моделируется посредством измерения, которое выполняет Алиса, и унитарного преобразования, производимого Бобом. Действительно, мы можем заменить все измерения, производимые Бобом, и передачу информации от Боба к Алисе измерениями, выполняемыми Алисой, и унитарными преобразованиями, которые должен произвести Боб в зависимости от результатов измерений Алисы. Наконец, все измерения, выполненные Алисой, могут быть объединены в одно измерение (упр. 2.57), результат которого определяет унитарное преобразование, выполняемое Бобом. Этот протокол обеспечивает точно такой же результат, как и исходный протокол с двусторонней связью. ■

Теорема 12.15. Чистое состояние $|\psi\rangle$ системы из двух компонент может быть преобразовано в другое чистое состояние $|\varphi\rangle$ при помощи ЛОКК тогда и только тогда, когда $\lambda_\psi \prec \lambda_\varphi$.

Доказательство.

Предположим, что $|\psi\rangle$ может быть преобразовано в другое чистое состояние $|\varphi\rangle$ при помощи ЛОКК. Согласно утверждению 12.14, можно предположить, что это преобразование осуществляется посредством выполняемого Алисой измерения, описываемого с операторами M_j , с последующей передачей полученного результата Бобу, который выполняет унитарное преобразование U_j . Алиса начинает с состояния ρ_ψ и заканчивает состоянием ρ_φ независимо от результатов измерения, так что, мы должны иметь

$$M_j \rho_\psi M_j^\dagger = p_j \rho_\varphi, \quad (12.160)$$

где p_j — вероятность результата j . Из полярного разложения $M_j \sqrt{\rho_\psi}$ следует, что существует такое унитарное преобразование V_j , что

$$M_j \sqrt{\rho_\psi} = \sqrt{M_j \rho_\psi M_j^\dagger} V_j = \sqrt{p_j \rho_\varphi} V_j. \quad (12.161)$$

Умножение этого уравнения на сопряженное ему дает

$$\sqrt{\rho_\psi} M_j^\dagger M_j \sqrt{\rho_\psi} = p_j V_j^\dagger \rho_\varphi V_j. \quad (12.162)$$

Суммируя по j и используя соотношение полноты $\sum_j M_j^\dagger M_j = I$, получаем

$$\rho_\psi = \sum_j p_j V_j^\dagger \rho_\varphi V_j, \quad (12.163)$$

откуда $\lambda_\psi \prec \lambda_\varphi$ согласно теореме 12.13.

Доказательство обратного утверждения теоремы 12.15 получается путем рассуждений в обратном порядке. Пусть $\lambda_\psi \prec \lambda_\varphi$, так что $\rho_\psi \prec \rho_\varphi$ и, согласно теореме 12.13, существуют вероятности p_j и такие унитарные операторы U_j , что $\rho_\psi = \sum_j p_j U_j \rho_\varphi U_j^\dagger$. Теперь предположим, что ρ_ψ обратимо (от этого предположения легко отказаться; см. упр. 12.20) и зададим операторы M_j для системы Алисы следующим образом:

$$M_j \sqrt{\rho_\psi} \equiv \sqrt{p_j \rho_\varphi} U_j^\dagger. \quad (12.164)$$

Чтобы убедиться, что эти операторы описывают измерение, нужно проверить соотношение полноты. Мы имеем $M_j = \sqrt{p_j \rho_\varphi} U_j^\dagger \rho_\psi^{-1/2}$ и, следовательно,

$$\sum_j M_j^\dagger M_j = \rho_\psi^{-1/2} \left(\sum_j p_j U_j \rho_\varphi U_j^\dagger \right) \rho_\psi^{-1/2} = \rho_\psi^{-1/2} \rho_\varphi \rho_\psi^{-1/2} = I, \quad (12.165)$$

что является соотношением полноты. Предположим, что Алиса выполняет измерение, описываемое операторами M_j , получает при этом результат j и соответствующее состояние $|\psi_j\rangle \sim M_j |\psi\rangle$. Пусть ρ_j — приведенная матрица плотности, соответствующая состоянию $|\psi_j\rangle$, так что, используя (12.164), получаем

$$\rho_j \sim M_j \rho_\psi M_j^\dagger = p_j \rho_\varphi \quad (12.166)$$

и, таким образом, $\rho_j = \rho_\varphi$. Из упр. 2.81 следует, что Боб может преобразовать $|\psi_j\rangle$ в $|\varphi\rangle$, применяя подходящее унитарное преобразование V_j . ■

Упражнение 12.20. Покажите, что в доказательстве обратного утверждения теоремы 12.15 можно отказаться от предположения о том, что матрица ρ_ψ обратима.

Упражнение 12.21 (катализ запутанности). Предположим, что Алиса и Боб разделяют пару четырехуровневых систем в состоянии $|\psi\rangle = \sqrt{0,4}|00\rangle + \sqrt{0,4}|11\rangle + \sqrt{0,1}|22\rangle + \sqrt{0,1}|33\rangle$. Покажите, что Алиса и Боб, применяя ЛОКК, не могут преобразовать это состояние в состояние $|\varphi\rangle = \sqrt{0,5}|00\rangle + \sqrt{0,25}|11\rangle + \sqrt{0,25}|22\rangle$. Однако предположим, что сочувствующий банк хочет предложить им взаймы *катализатор*, запутанную пару кубитов в состоянии $|c\rangle = \sqrt{0,6}|00\rangle + \sqrt{0,4}|11\rangle$. Покажите, что Алиса и Боб могут преобразовать состояние $|\psi\rangle|c\rangle$ в

состояние $|\varphi\rangle|c\rangle$, применяя локальные операции и классическую коммуникацию; после завершения преобразования Алиса и Боб вернут катализатор $|c\rangle$ в банк.

Упражнение 12.22 (преобразование запутанности без классической связи). Предположим, что Алиса и Боб пытаются преобразовать чистое состояние $|\psi\rangle$ в чистое состояние $|\varphi\rangle$, используя только локальные операции (без классической коммуникации). Покажите, что это возможно тогда и только тогда, когда $\lambda_\psi \cong \lambda_\varphi \otimes x$, где x — некоторый действительный вектор с неотрицательными компонентами, в сумме дающими 1, а знак « \cong » означает, что векторы слева и справа от него имеют одинаковые ненулевые компоненты.

12.5.2 Очищение и разбавление запутанности

Предположим, что вместо одного состояния $|\psi\rangle$ Алиса и Боб имеют большое количество копий этого состояния. Какие типы преобразования запутанности Алиса и Боб могут выполнить со всеми этими копиями? Мы уделим особое внимание двум специальным типам преобразования запутанности: *очищению запутанности* и *разбавлению запутанности*. Идея очищения запутанности состоит в том, что Алиса и Боб должны преобразовать некоторое большое число копий какого-либо известного чистого состояния $|\psi\rangle$ в как можно большее количество копий состояния Белла $(|00\rangle + |11\rangle)/\sqrt{2}$, используя локальные операции и классическую коммуникацию. При этом требуется, чтобы они это сделали с большой степенью совпадения. Разбавление запутанности представляет собой обратный процесс, т. е. преобразование большого количества копий состояния Белла $(|00\rangle + |11\rangle)/\sqrt{2}$ в копии состояния $|\psi\rangle$ с использованием ЛОКК.

Что является причиной изучения очищения и разбавления запутанности? Предположим, что мы рассматриваем запутанность как физический ресурс. Тогда можно количественно определить запутанность подобно тому, как мы это делаем с другими физическими ресурсами, такими как энергия или энтропия. Пусть мы выбрали состояние Белла $(|00\rangle + |11\rangle)/\sqrt{2}$ в качестве *стандартной единицы* запутанности — основной меры, такой, как стандартный килограмм или стандартный метр. Мы можем связать меру запутанности с квантовым состоянием $|\psi\rangle$ так же, как мы связываем массу с предметом. Предположим, например, что мы берем 15 шоколадных печений определенного сорта, вес² которых равен стандартному килограмму; мы утверждаем, что одно шоколадное печенье весит $1/15$ килограмма. Строго говоря, если одно шоколадное печенье весит $1/14,8$ килограмма, мы были бы в некотором затруднении, поскольку нет такого целого числа шоколадных печений, которыми можно было бы уравновесить стандартный килограмм, и совсем не очевидно, как определить нецелое число шоколадных печений. К счастью, мы замечаем, что 148 шоколадных печений точно уравновешивают 10 стандартных килограммов, так что вес одного шоколадного печенья равен $10/148$ килограмма. Но что, если реальный

²Далее речь идет, на самом деле, о массе печенья, хотя используется более распространенное в быту слово «вес» — Прим. ред

вес равен не $1/14,8$ килограмма, а более экзотической величине, как, например, $1/14,7982\dots$ килограмма? Тогда мы просто приближаемся к пределу, при котором большое количество m шоколадного печенья уравновешивает другое большое количество n стандартных килограммов, и утверждаем, что масса одного шоколадного печенья должна быть предельным отношением n/m , когда и m , и n становятся очень большими.

Аналогично, возможный подход к определению количества запутанности в чистом состоянии $|\psi\rangle$ состоит в следующем: задано большое число n состояний Белла $(|00\rangle + |11\rangle)/\sqrt{2}$ и нам предложено сделать как можно больше копий (с большой степенью совпадения), $|\psi\rangle$, используя локальные операции и классическую коммуникацию. Если число копий $|\psi\rangle$, которое можно произвести, равно m , то мы определяем предельное отношение n/m как *запутанность приготовления* состояния $|\psi\rangle$. Предположив, что процесс при использовании ЛОКК протекает в противоположном направлении — от m копий $|\psi\rangle$ к n копиям состояния Белла $(|00\rangle + |11\rangle)/\sqrt{2}$, мы определим предельное отношение n/m как *очищаемая запутанность* состояния $|\psi\rangle$. Совсем не очевидно, что эти два определения дают одно и то же число для количества запутанности; тем не менее, мы увидим, что для чистых состояний $|\psi\rangle$ запутанность приготовления и очищаемая запутанность — это фактически одно и то же!

Рассмотрим простые протоколы для разбавления и очищения запутанности. Пусть запутанное состояние $|\psi\rangle$ имеет разложение Шмидта

$$|\psi\rangle = \sum_x \sqrt{p(x)} |x_A\rangle |x_B\rangle. \quad (12.167)$$

Мы обозначили возвещенные в квадрат коэффициенты Шмидта через $p(x)$, поскольку они имеют свойства распределений вероятностей (неотрицательны и сумма равна единице) и понятия теории вероятностей оказываются полезными для понимания очищения и разбавления запутанности. Можно записать m -кратное тензорное произведение $|\psi\rangle^{\otimes m}$ в виде

$$|\psi\rangle^{\otimes m} = \sum_{x_1, x_2, \dots, x_m} \sqrt{p(x_1)p(x_2)\dots p(x_m)} |x_1 x_2 \dots x_m A\rangle |x_1 x_2 \dots x_m B\rangle. \quad (12.168)$$

Предположим, что мы определили новое квантовое состояние $|\varphi_m\rangle$, пренебрегая всеми членами x_1, \dots, x_m , которые не являются ϵ -типовыми в том смысле, как определено в подразд. 12.2.1:

$$|\varphi_m\rangle \equiv \sum_{x\text{-типовная}} \sqrt{p(x_1)p(x_2)\dots p(x_m)} |x_1 x_2 \dots x_m A\rangle |x_1 x_2 \dots x_m B\rangle. \quad (12.169)$$

Состояние $|\varphi_m\rangle$ не является нормированным квантовым состоянием. Чтобы его нормировать, определим $|\varphi'_m\rangle \equiv |\varphi_m\rangle / \sqrt{\langle \varphi_m | \varphi_m \rangle}$. Из части 1 теоремы о типичных последовательностях степень совпадения $F(|\psi\rangle^{\otimes m}, |\varphi_m\rangle) \rightarrow 1$ при $m \rightarrow \infty$. Более того, из части 2 теоремы о типичных последовательностях количество членов в сумме (12.169) не превышает $2^{m(H(p(x))+\epsilon)} = 2^{m(S(\rho\psi)+\epsilon)}$, где ρ_ψ — результат фиксирования Бобом его части состояния $|\psi\rangle$.

Теперь предположим, что Алиса и Боб разделяют $n = m(S(\rho_\psi) + \varepsilon)$ состояний Белла. Алиса локально приготавливает «обе части» $|\varphi'_m\rangle$, а затем использует состояния Белла, которые она разделяет с Бобом, для телепортации Бобу принадлежащей ему половины состояния $|\varphi'_m\rangle$. Таким образом, Алиса и Боб могут разбавить свои n состояний Белла, чтобы получить $|\varphi'_m\rangle$, которое является очень хорошей аппроксимацией $|\psi\rangle^{\otimes m}$. Эта процедура разбавления запутанности дает $n = m(S(\rho_\psi) + \varepsilon)$, так что отношение n/m стремится к $S(\rho_\psi) + \varepsilon$. Мы можем выбрать ε сколь угодно малым, поэтому делаем вывод, что запутанность приготовления состояния $|\psi\rangle$ не больше, чем $S(\rho_\psi)$, поскольку мы только что показали, что $S(\rho_\psi)$ состояний Белла могут быть (асимптотически) преобразованы в одну копию $|\psi\rangle$.

Протокол очищения запутанности для преобразования копий $|\psi\rangle$ в состояния Белла строится аналогичным образом. Предположим, что Алиса и Боб разделяют m копий $|\psi\rangle$. Производя измерение, проектирующее на ε -типичное подпространство для ρ_ψ , Алиса может с большой степенью совпадения преобразовать состояние $|\psi\rangle^{\otimes m}$ в состояние $|\varphi'_m\rangle$. Наибольший коэффициент Шмидта в $|\varphi'_m\rangle$, не превышает $2^{-m(S(\rho_\psi)-\varepsilon)}$, в соответствии с определением типичных последовательностей. В нормированном состоянии $|\varphi'_m\rangle$ коэффициенты Шмидта больше (но не более, чем в $1/\sqrt{1-\delta}$ раз), поскольку, согласно теореме о типичных последовательностях, величина $1-\delta$ является нижней границей вероятности того, что последовательность ε -типичная, и может быть сколь угодно близка к 1 для достаточно больших m . Таким образом, наибольшее собственное значение матрицы состояния $\rho_{\varphi'_m}$ не превышает $2^{-m(S(\rho_\psi)-\varepsilon)/(1-\delta)}$. Пусть мы выбираем любое n такое, что

$$\frac{2^{-m(S(\rho_\psi)-\varepsilon)}}{1-\delta} \leq 2^{-n}. \quad (12.170)$$

Вектор собственных значений $\rho_{\varphi'_m}$ мажоризуется вектором $(2^{-n}, 2^{-n}, \dots, 2^{-n})$ и, следовательно, согласно теореме 12.5, состояние $|\varphi'_m\rangle$ может быть преобразовано в n состояний Белла путем использования локальных операций и классической коммуникации. Из формулы (12.170) видно, что это возможно при условии $n \approx mS(\rho_\psi)$, и, следовательно, запутанность очищения не меньше $S(\rho_\psi)$.

Мы представили стратегию очищения $|\psi\rangle$ в $S(\rho_\psi)$ состояний Белла и разбавления $S(\rho_\psi)$ состояний Белла в копию $|\psi\rangle$. В самом деле, нетрудно увидеть, что описанные нами процедуры действительно позволяют оптимально осуществить разбавление и очищение запутанности! Предположим, например, что существует более эффективный протокол разбавления запутанности, позволяющий разбавить $|\psi\rangle$ в $S > S(\rho_\psi)$ состояний Белла. Начиная с $S(\rho_\psi)$ состояний Белла, Алиса и Боб могли бы сделать копию $|\psi\rangle$ с помощью уже описанного протокола, а затем использовать гипотетический протокол для приготовления S состояний Белла. Таким образом, используя локальные операции и классическую коммуникацию, Алиса и Боб могли бы преобразовать $S(\rho_\psi)$ состояний Белла в $S > S(\rho_\psi)$ состояний Белла! Нетрудно убедиться (см. упр. 12.24), что, используя локальные операции и классическую коммуникацию, невозможно

увеличить число состояний Белла, и такой гипотетический протокол разбавления существовать не может. Аналогично можно показать, что описанная процедура очищения запутанности является оптимальной. Таким образом, запутанность приготовления и запутанность очищения для состояния $|\psi\rangle$ одинаковы и равны $S(\rho_\psi)$!

Упражнение 12.23. Докажите, что описанная нами процедура очищения запутанности является оптимальной.

Упражнение 12.24. Напомним, что число Шмидта чистого состояния системы из двух компонент — это число ненулевых коэффициентов Шмидта. Докажите, что число Шмидта чистого квантового состояния нельзя увеличить посредством локальных операций и классической коммуникации. Используйте полученный результат для доказательства того, что число состояний Белла, разделенных между Алисой и Бобом, не может быть увеличено посредством локальных операций и классической коммуникации.

Мы показали, как оптимально можно преобразовать состояния Белла квантовой системы из двух компонент в копии запутанного состояния $|\psi\rangle$ и обратно, что дает основание определить количество запутанности в этом квантовом состоянии как число состояний Белла, в которые можно преобразовать копии $|\psi\rangle$ и наоборот, т. е. $S(\rho_\psi)$. Что мы можем почерпнуть из данного определения? Ниже мы увидим, что, обобщая понятие очищаемой запутанности, можно получить интересные возможности исправления квантовых ошибок. Однако, следует отметить, что пока изучение запутанности только начинается, и не совсем ясно, насколько улучшится наше понимание квантовых вычислений и квантовой информации в результате изучения количественных мер запутанности. Мы сносно понимаем свойства чистых состояний квантовых систем из двух компонент, но очень плохо разбираемся в системах, состоящих из трех и более компонент, а также в смешанных состояниях для двухкомпонентных систем. Улучшение понимания запутанности и распространение полученных результатов на квантовые алгоритмы, исправление квантовых ошибок и квантовую связь являются основными вопросами в области квантовых вычислений и квантовой информации!

12.5.3 Очищение запутанности и исправление квантовых ошибок

Мы определили очищение запутанности для чистых состояний, но это определение можно распространить и на смешанные состояния. Пусть ρ — состояние квантовой системы из двух компонент, принадлежащей Алисе и Бобу. Они разделяют большое количество m копий этого состояния; используя локальные операции и классическую коммуникацию, Алиса и Боб пытаются преобразовать эти копии в максимально возможное число n состояний Белла с большой степенью совпадения. Очищаемая запутанность $D(\rho)$ является предельным значением отношения n/m для наилучшего протокола очищения. Мы уже показали, что $D(|\psi\rangle) = S(\rho_\psi)$ для чистых состояний $|\psi\rangle$, однако пока не знаем, как вычислить $D(\rho)$ для смешанного состояния.

Разработано много методов очищения запутанности, которые дают нижние границы $D(\rho)$ для определенных классов состояний ρ . В нашей книге эти методы не будут рассматриваться (см. разд. «История и дополнительная литература» в конце главы). Мы лишь опишем замечательную связь между очищаемой запутанностью и исправлением квантовых ошибок.

Представим себе, что Алиса пытается послать Бобу квантовую информацию по квантовому каналу с шумом \mathcal{E} . Мы предполагаем, что канал является кубитовым, как, например, деполяризующий канал, хотя те же самые основные идеи легко применить и для некубитовых каналов. Один из методов передачи квантовой информации по кубитовому каналу состоит в следующем. Алиса приготавливает большое число m состояний Белла и посыпает половину каждой пары Белла по каналу. Предположим, что в результате применения \mathcal{E} к половине пары Белла получается состояние ρ , так что Алиса и Боб разделяют m копий ρ . Теперь Алиса и Боб осуществляют очищение запутанности и получают $mD(\rho)$ пар Белла. Алиса может подготовить состояние из $mD(\rho)$ кубитов и телепортировать его Бобу, используя $mD(\rho)$ пар Белла, которые они разделяют.

Таким образом, протоколы очищения запутанности могут быть использованы в качестве модели исправления ошибок для квантовых каналов связи между Алисой и Бобом. Это позволяет Алисе надежно передать $mD(\rho)$ кубитов информации Бобу, где $D(\rho)$ — очищаемая запутанность для состояния ρ , которое появляется в результате посылки одной половины пары Белла по каналу с шумом \mathcal{E} , соединяющему Алису и Боба.

В самом деле, замечательно, что этот способ коммуникации с использованием очищения запутанности может иногда работать, даже когда не работают традиционные методы исправления квантовых ошибок. Например, из подразд. 12.4.3 мы знаем, что квантовая информация не может быть передана по деполяризующему каналу с $p = 3/4$. Однако, известны протоколы очищения запутанности, которые могут обеспечить ненулевую скорость передачи $D(\rho)$ даже для этого канала! Это возможно, поскольку в протоколах очищения запутанности осуществляется классическая связь между Алисой и Бобом, тогда как в традиционных методах исправления ошибок классическая связь не используется.

Этот пример позволяет объяснить утверждение, которое мы сделали еще в гл. 1 и проиллюстрировали на рис. 12.11, о том, что существуют каналы с нулевой пропускной способностью для квантовой информации, которые могут быть использованы для передачи квантовой информации, когда один такой канал соединяет Алису с Бобом, а другой — Боба с Алисой! Этот очень простой способ передачи информации основан на очищении запутанности. Чтобы очищение запутанности было возможно, нужен классический канал связи между Алисой и Бобом. Половина информации, передаваемой по каналу от Алисы к Бобу, и вся информация, передаваемая по каналу от Боба к Алисе, будет классической. Эти каналы, согласно теореме ХШВ, имеют ненулевую скорость передачи классической информации. Вторая половина информации, передаваемой по каналу от Алисы к Бобу, состоит из половин пар Белла, причем для

выделения «хороших» пар Белла из результирующих состояний используется очищение запутанности. Полученные «хорошие» пары Белла позволят надежно передавать квантовую информацию с помощью телепортации. Все это является наглядной демонстрацией замечательных свойств квантовой информации!

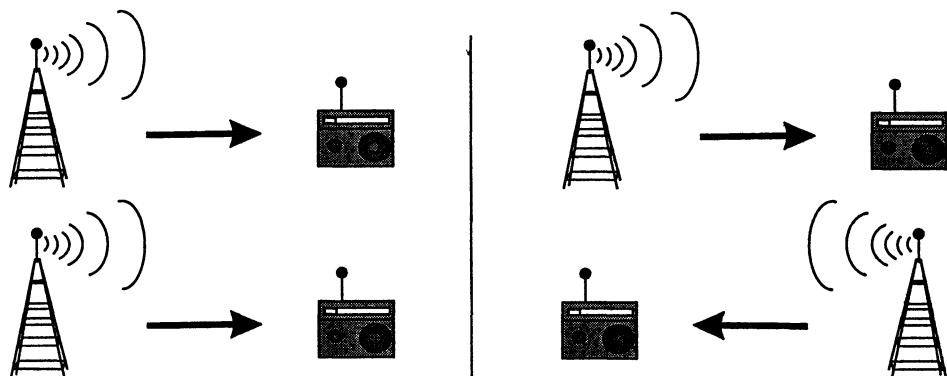


Рис. 12.11. Если у нас есть два классических параллельных канала с сильным шумом с нулевой пропускной способностью, то объединенный канал также имеет нулевую пропускную способность. Не удивительно, что если изменить направление одного из каналов на обратное, то пропускная способность также будет нулевой Но в квантовой механике изменение направления одного из каналов с нулевой пропускной способностью на обратное действительно может позволить передавать информацию!

12.6 Квантовая криптография

Подходящим завершением этой главы является одно из замечательных применений квантовой теории информации. Как мы видели в гл. 5, квантовые компьютеры могут быть использованы для взломывания некоторых из самых лучших криптосистем с открытым ключом. Однако, квантовая механика, отнимая одной рукой, к счастью, возвращает другой: процедура, известная как *квантовая криптография*, или *квантовое распределение ключей*, использует принципы квантовой механики, чтобы сделать безопасной передачу секретной информации. Здесь мы опишем эту процедуру и обсудим ее безопасность. Начнем с объяснения основных идей классического подхода, *криптографии с закрытым ключом* (подразд. 12.6.1). Криптография с закрытым ключом — гораздо более старый вид криптографии по сравнению с криптосистемами с открытым ключом (упомянутыми в гл. 5), но принципы криптографии с закрытым ключом используются в квантовых криптосистемах. Два других важных классических метода, усиление конфиденциальности и согласование информации, которые также используются в квантовых системах, мы опишем в подразд. 12.6.2. Три различных протокола для распределения квантовых ключей представлены в подразд. 12.6.3. Насколько надежны эти протоколы? Оказывается, как мы уви-

дим в подразд. 12.6.4, *когерентная информация*, мера квантовой информации, которая нам встретилась впервые в подразд. 12.4.1, задает нижнюю границу возможности использования в принципе квантового канала связи для передачи секретной информации! Это означает, что понятие квантовой информации может быть использовано для доказательства надежности квантовых протоколов распределения ключей. В подразд. 12.6.5, завершающем эту главу, мы дадим набросок для доказательства безопасности квантовой криптографии на основе теории исправления квантовых ошибок.

12.6.1 Криптография с закрытым ключом

До изобретения в 70-х гг. XX в. криптографии с открытым ключом работа всех криптосистем основывалась на другом принципе, известном как *криптография с закрытым ключом*. В криптосистеме с закрытым ключом у Алисы должен быть *кодирующий ключ*, который позволяет ей зашифровать сообщение, которое она хочет послать Бобу, а у Боба должен быть соответствующий *декодирующий ключ*, с помощью которого Боб расшифровывает зашифрованное сообщение. Простой, но эффективной криптосистемой с закрытым ключом является *шифр Вернама*, который иногда называют *одноразовым блокнотом*. Вначале у Алисы и Боба есть одинаковые n -битовые строки секретного ключа. Алиса кодирует свое n -битовое сообщение, прибавляя ключ к сообщению, а Боб декодирует, вычитая ключ, как показано на рис. 12.12.

Важнейшей особенностью этой системы является то, что пока строки ключа действительно секретны, система гарантированно безопасна. Иначе говоря, если протокол, который используют Алиса и Боб, успешно работает, то связь абсолютно безопасна (подслушивающая Ева всегда может блокировать канал связи, но Алиса и Боб могут обнаружить это и объявить сбой). Для любой стратегии подслушивания, которую использует Ева, Алиса и Боб могут гарантировать, что взаимная информация Евы с их незакодированным сообщением может быть сделана сколь угодно малой. Напротив, безопасность криптографии с открытым ключом (приложение 5) основана на недоказанных математических гипотезах о трудности решения определенных задач, таких, как разложение на множители (с классическими компьютерами!), но несмотря на это, такие криптосистемы более удобны и широко используются.

Основной трудностью при использовании криптосистем с закрытым ключом является безопасное распределение битов ключа. В частности, шифр Вернама надежен, только пока число битов ключа не меньше размера кодируемого сообщения, причем биты ключа нельзя использовать повторно! Большое количество битов ключа делает такие схемы непрактичными для широкого применения. Кроме того, биты ключа должны быть доставлены заранее, тщательно защищены до использования, а потом уничтожены; в противном случае классическая информация такого рода может быть в принципе скопирована, что подвергает опасности надежность всего протокола. Несмотря на эти недостатки, криптосистемы с закрытым ключом, такие как шифр Вернама, продолжают использовать благодаря их гарантированной безопасности с ключами,

доставленными при тайном свидании, доверенным курьером или при помощи надежных личных связей.



Рис. 12.12. Шифр Вернама Алиса кодирует, прибавляя к посыпалому сообщению случайные биты ключа (или как в нашем примере, буквы алфавита). Боб декодирует, вычитая биты ключа, чтобы восстановить сообщение

Упражнение 12.25. Рассмотрите систему с n пользователями, любая пара которых хотела бы общаться лично. Сколько требуется ключей при использовании криптографии с открытым ключом? Сколько требуется ключей при использовании криптографии с закрытым ключом?

12.6.2 Усиление конфиденциальности и согласование информации

Первый шаг в криптографии с закрытым ключом — распределение строки ключа. Что, если Алиса и Боб начнут с дефектных ключей? Предположим, в частности, что Алиса и Боб разделяют коррелированные случайные классические битовые строки X и Y , и существует верхняя граница для взаимной информации Евы с X и Y . Как они могут получить из этих дефектных ключей достаточно хороший ключ для выполнения безопасного криптографического протокола? Мы покажем, что, выполнив *согласование информации*, а затем *усиление конфиденциальности*, Алиса и Боб могут систематически увеличивать корреляцию между своими строками ключа, одновременно уменьшая вза-

имную информацию с подслушивающей Евой до некоторого желаемого уровня безопасности. Эти классические процедуры будут использованы в квантовом протоколе распределения ключей, описанном в следующем разделе.

Согласование информации — не что иное, как исправление ошибок, выполняемое в открытом канале, которое устраняет расхождения между X и Y , что позволяет получить совместную битовую строку W и насколько возможно уменьшить утечку информации к Еве. Предположим, что после этой процедуры Ева получила случайную величину Z , которая частично коррелирована с W . Тогда Алиса и Боб используют усиление конфиденциальности для выделения из W меньшего набора битов S , корреляция которого с Z ниже желаемого порога. Поскольку этот последний шаг концептуально нов, рассмотрим его в первую очередь.

Детальное доказательство того, почему достигается усиление конфиденциальности, выходит за рамки этой книги, но мы опишем основной метод и приведем главную теорему. Один из способов усиления конфиденциальности состоит в использовании класса универсальных хеш-функций \mathcal{G} , которые отображают набор n -битовых строк \mathcal{A} в набор m -битовых строк \mathcal{B} . При этом для любых различных $a_1, a_2 \in \mathcal{A}$ и g , случайно выбранного из \mathcal{G} , вероятность того, что $g(a_1) = g(a_2)$, не более, чем $1/|\mathcal{B}|$.

Коллизионная энтропия случайной величины X с распределением вероятностей $p(x)$ определяется как

$$H_c(X) = -\log \left[\sum_x p(x)^2 \right]. \quad (12.171)$$

(Иногда ее называют энтропией Ренни второго порядка.) Используя выпуклость логарифмической функции, нетрудно показать, что энтропия Шеннона ограничивает эту величину сверху: $H(X) \geq H_c(X)$. Коллизионная энтропия используется в следующей теореме об универсальных хеш-функциях:

Теорема 12.16. Пусть X — случайная величина из алфавита X с распределением вероятностей $p(x)$ и коллизионной энтропией $H_c(X)$ и пусть G — случайная величина, соответствующая равновероятному случайному выбору хеш-функций из универсального класса хеш-функций, отображающих \mathcal{X} в $\{0, 1\}^m$. Тогда

$$H(G(X)|G) \geq H_c(G(X)|G) \geq m - 2^{m-H_c(X)}. \quad (12.172)$$

Теорему 12.16 можно использовать для усиления конфиденциальности следующим образом. Алиса и Боб открыто выбирают $g \in \mathcal{G}$ и каждый применяет g к W , получая новую битовую строку S в качестве своего секретного ключа. Если неопределенность Евы относительно W при заданном ее знании $Z = z$ (о конкретном значении W), выраженная через коллизионную энтропию, ограничена снизу некоторым числом $H_c(W|Z = z) > d$, то из теоремы 12.16 следует, что

$$H_c(S|G, Z = z) \geq m - 2^{m-d}. \quad (12.173)$$

Другими словами, m может быть выбрано настолько малым, чтобы $H_c(S|G, Z = z)$ приблизительно равнялась m . Это приводит к максимально возможной неопределенности Евы относительно ключа S , обеспечивая секретность ключа.

Согласование информации также уменьшает число битов ключа, которые Алиса и Боб могут получить, однако, это уменьшение может быть ограничено следующим образом. Проводя проверки на четность по нескольким подмножествам своих битов X , Алиса может составить (классическое) сообщение u , содержащее описания этих подмножеств и их четности. Получив это сообщение, Боб исправляет ошибки в своей строке Y , после чего и Алиса, и Боб имеют одну и ту же строку W . Очевидно, что это потребует посылки $k > H(W|Y)$ битов информации в u . Однако, эта процедура дает Еве дополнительное знание $U = u$, увеличивая таким образом ее коллизионную энтропию до $H_c(W|Z = z, U = u)$. В среднем (по возможным сообщениям согласования u) это увеличение ограничено снизу $H_c(W|Z = z, U = u) \geq H_c(W|Z = z) - H(U)$, где $H(U)$ — обычная энтропия Шеннона для U . Однако это ограничение слишком слабое, поскольку предполагает, что вероятность того, что просочившаяся информация $U = u$ уменьшила H_c на величину, большую $mH(U)$, всего лишь не больше $1/m$. Более сильное ограничение дает следующая теорема:

Теорема 12.17. Пусть X и U — случайные величины из алфавитов \mathcal{X} и \mathcal{U} соответственно, где X имеет распределение вероятностей $p(x)$, а $p(x, u)$ — совместное распределение U с X . Пусть также $s > 0$ — произвольный параметр. Тогда с вероятностью, по меньшей мере, $1 - 2^{-s}$, U принимает значение u , для которого

$$H_c(X|U = u) \geq H_c(X) - 2 \log |\mathcal{U}| - 2s. \quad (12.174)$$

Входящее в это выражение s называется *параметром секретности*. Применение теоремы к протоколу согласования позволяет сделать вывод, что Алиса и Боб могут выбрать такое s , что коллизионная энтропия Евы будет ограничена снизу как $H_c(W|Z = z, U = u) \geq d - 2(k + s)$ с вероятностью, большей, чем $1 - 2^{-s}$. Затем, усиление конфиденциальности дает им возможность очистить m битов секретного ключа S , для которого полная информация Евы меньше, чем $2^{m-d+2(k+s)}$ битов.

Усиление конфиденциальности и согласование информации с помощью CSS кода

Как отмечалось выше, согласование информации — это не что иное, как исправление ошибок. Оказывается, что усиление конфиденциальности также тесно связано с исправлением ошибок, и обе задачи можно решить, используя классические коды. Такая точка зрения будет полезна при доказательстве безопасности квантового распределения ключей в подразд. 12.6.5, поскольку у нас есть хорошо разработанная теория квантовых кодов, исправляющих ошибки. Ввиду этого полезно привести следующие соображения.

Декодирование из случайно выбранного CSS кода (см. подразд. 10.4.2) можно рассматривать как согласование информации и усиление конфиденциаль-

ности. Хотя CSS коды обычно используются для кодирования квантовой информации, для наших целей мы можем ограничиться их классическими свойствами. Рассмотрим два классических линейных кода C_1 и C_2 , которые удовлетворяют условиям для CSS $[n, m]$ -кода, исправляющего t ошибок: $C_2 \subset C_1$, C_1 и C_2^\perp исправляют t ошибок. Алиса выбирает случайную n -битовую строку X и передает ее Бобу, который получает Y .

Допустим, что в канале связи между Алисой и Бобом ожидаемое число ошибок на кодовый блок, вызванное всеми источниками шума, *включая подслушивание*, меньше, чем t ; на практике это может быть установлено случайнym тестированием канала. Предположим также, что Ева ничего не знает о кодах C_1 и C_2 ; это можно гарантировать, если Алиса случайным образом выбирает код. Наконец, предположим, что существует известная Алисе и Бобу верхняя граница для взаимной информации данных Z Евы с их собственными данными X и Y .

Боб получает $Y = X + \varepsilon$, где ε — некоторая ошибка. Поскольку известно, что ошибок меньше, чем t , если Алиса и Боб исправляют свои состояния до ближайшего кодового слова в C_1 , то их результаты $X', Y' \in C_1$ идентичны, и $W = X' = Y'$. Этот шаг — не что иное, как согласование информации. Конечно, взаимная информация Евы с W может оставаться недопустимо большой. Чтобы ее уменьшить, Алиса и Боб устанавливают, к какому из 2^m классов смежности C_2 в C_1 принадлежит их состояние W , т. е. они вычисляют класс смежности $W + C_2$ в C_1 . В результате Алиса и Боб получают m -битовую строку ключа S . Благодаря тому, что Ева не знает C_2 , эта процедура может уменьшить взаимную информацию Евы с S до приемлемого уровня, усилив конфиденциальность.

12.6.3 Квантовое распределение ключей

Квантовое распределение ключей (КРК) является протоколом, который *гарантирует* надежен, и посредством которого биты закрытого ключа могут быть созданы в процессе коммуникации двух сторон по *открытым* каналу. Эти биты ключа могут быть использованы для реализации классической криптосистемы с закрытым ключом, что обеспечивает безопасную связь. Единственное требование для протокола КРК состоит в том, что при передаче кубитов по открытому каналу частота появления ошибок должна быть меньше определенного порога. Безопасность получающегося в результате ключа гарантируется свойствами квантовой информации и, следовательно, обусловлена только фундаментальными законами физики.

Квантовое распределение ключей основано на том, что Ева не может извлечь никакой информации из кубитов, передаваемых от Алисы к Бобу, не нарушив их состояние. Во-первых, согласно теореме о невозможности копирования (вставка 12.1), Ева не может копировать кубит Алисы. Во-вторых, у нас есть следующее утверждение.

Утверждение 12.18 (получение информации приводит к возмущению сигнала). При любой попытке различить два неортогональных квантовых состояния извлечение информации сопровождается возмущением сигнала.

Доказательство.

Пусть $|\psi\rangle$ и $|\varphi\rangle$ — неортогональные квантовые состояния, о которых Ева пытается получить информацию. Исходя из результатов разд. 8.2, без потери общности можно допустить, что процесс, который Ева использует для получения информации, представляет собой унитарное взаимодействие состояния ($|\psi\rangle$ или $|\varphi\rangle$) с вспомогательной системой, приготовленной в стандартном состоянии $|u\rangle$. Допуская, что этот процесс не нарушает ни одно из этих состояний, получаем

$$|\psi\rangle|u\rangle \rightarrow |\psi\rangle|v\rangle, \quad (12.175)$$

$$|\varphi\rangle|u\rangle \rightarrow |\varphi\rangle|v'\rangle. \quad (12.176)$$

Для Евы желательно, чтобы $|v\rangle$ и $|v'\rangle$ были различными, с тем, чтобы она могла получить информацию о состоянии. Однако, поскольку скалярные произведения сохраняются при унитарных преобразованиях, должны выполняться следующие равенства:

$$\langle v|v'\rangle\langle\psi|\varphi\rangle = \langle u|u\rangle\langle\psi|\varphi\rangle, \quad (12.177)$$

$$\langle v|v'\rangle = \langle u|u\rangle = 1, \quad (12.178)$$

откуда следует, что $|v\rangle$ и $|v'\rangle$ должны совпадать. Таким образом, установление различия между $|\psi\rangle$ и $|\varphi\rangle$ должно неизбежно нарушить, по меньшей мере, одно из этих состояний. ■

Мы воспользуемся этой идеей передачи неортогональных кубитовых состояний между Алисой и Бобом. Проверяя переданные состояния на предмет нарушения, Алиса и Боб получают верхнюю оценку любого шума и подслушивания, которые имеют место в их канале связи. Эти «контрольные» кубиты случайным образом вставляются между кубитами данных (из которых позднее извлекаются биты ключа), так что верхнее ограничение также применяется к кубитам данных. Затем Алиса и Боб выполняют согласование информации и усиление конфиденциальности для выделения общей строки секретного ключа. Таким образом, максимальное значение приемлемой скорости возникновения ошибок определяется эффективностью лучших протоколов согласования информации и усиления конфиденциальности. Ниже представлены три различных протокола КРК, которые работают таким образом.

Протокол BB84

Алиса начинает с двух строк a и b , каждая из которых содержит $(4 + \delta)n$ случайных классических битов. Затем она кодирует эти строки блоком $(4 + \delta)n$ кубитов,

$$|\psi\rangle = \bigotimes_{k=1}^{(4+\delta)n} |\psi_{a_k b_k}\rangle, \quad (12.179)$$

где a_k — k -й бит a (и так же для b), а состояния $|\psi_{a_k b_k}\rangle$ задаются как

$$|\psi_{00}\rangle = |0\rangle, \quad (12.180)$$

$$|\psi_{10}\rangle = |1\rangle, \quad (12.181)$$

$$|\psi_{01}\rangle = |+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}, \quad (12.182)$$

$$|\psi_{11}\rangle = |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}. \quad (12.183)$$

При этом a кодируется в базисе X или Z в зависимости от b . Отметим, что не все четыре состояния взаимно ортогональны, и поэтому никакое измерение не может позволить с уверенностью различить их (все). Затем Алиса посыпает $|\psi\rangle$ Бобу по открытому квантовому каналу связи.

Боб получает $\mathcal{E}(|\psi\rangle\langle\psi|)$, где \mathcal{E} — квантовое преобразование, описывающее общее действие канала и Евы, и публично объявляет об этом. Теперь у Алисы, Боба и Евы есть свои собственные состояния, описываемые различными матрицами плотности. Отметим, что поскольку Алиса не раскрыла b , Ева не знает, в каком базисе ей нужно провести измерения, чтобы подслушать сообщение Алисы, посланное Бобу. В лучшем случае она может только гадать, и если ее догадка неверна, то она нарушит состояние, полученное Бобом. Более того, поскольку шум \mathcal{E} может частично возникать в результате воздействия среды (плохой канал), а не только потому, что Ева подслушивает, Ева не может полностью контролировать \mathcal{E} .

Конечно, Боб также не может извлечь никакой информации из $\mathcal{E}(|\psi\rangle\langle\psi|)$, поскольку ничего не знает о b . Тем не менее, он измеряет каждый кубит в базисе X или Z в соответствии со строкой b' случайных $(4 + \delta)n$ битов, которую он создает самостоятельно. Пусть результатом измерения Боба будет a' . После этого Алиса публично объявляет b . Ведя обсуждение по открытому каналу, Боб и Алиса отбрасывают все биты из $\{a', a\}$, кроме тех, для которых соответствующие биты b' и b одинаковы. Оставшиеся биты удовлетворяют равенству $a' = a$, поскольку для этих битов Боб проводил измерения в том же базисе, в котором Алиса их приготовливала. Отметим, что b не несет никакой информации ни об a , ни о битах a' , полученных в результате измерения Боба, но важно, что Алиса не объявляет b до тех пор, пока Боб не объявит о том, что он получил кубиты Алисы. Чтобы упростить нижеизложенное объяснение, предположим, что Алиса и Боб сохраняют только $2n$ битов полученного ими результата; величину δ можно выбрать достаточно большой, чтобы это можно было сделать с экспоненциально малой вероятностью ошибки.

Теперь Алиса и Боб выполняют тесты, чтобы определить величину шума или подслушивания во время их связи. Алиса случайным образом выбирает n битов (из оставшихся $2n$ битов) и открыто объявляет о своем выборе. Затем Боб и Алиса объявляют и сравнивают значения этих контрольных битов.

Если больше, чем t битов не совпадает, то они прерывают выполнение протокола и начинают все с начала. Величину t Алиса и Боб выбирают так, что если тест завершается успешно, они могут использовать алгоритмы согласования информации и усиления конфиденциальности для получения t вполне секретных совместных битов ключа из оставшихся n битов.

Протокол BB84

1. Алиса выбирает $(4 + \delta)n$ случайных битов данных.
2. Алиса выбирает случайную $(4 + \delta)n$ -битовую строку b и кодирует каждый бит данных как $\{|0\rangle, |1\rangle\}$, если соответствующий бит b равен 0, или $\{|+\rangle, |-\rangle\}$, если бит равен 1.
3. Алиса посыпает Бобу полученное состояние.
4. Боб получает $(4 + \delta)n$ кубитов, объявляет об этом событии и измеряет каждый кубит в базисе X или Z случайнм образом.
5. Алиса объявляет b .
6. Алиса и Боб отбрасывают все биты, которые Боб измерил в базисе, отличном от того, в котором их подготовила Алиса. С большой вероятностью остается, по меньшей мере, $2n$ битов (в противном случае выполнение протокола прекращается).
7. Алиса выбирает n битов, чтобы использовать их для проверки вмешательства Евы, и сообщает Бобу, какие биты выбраны.
8. Алиса и Боб объявляют и сравнивают значения n контрольных битов. Если количество не совпадающих битов больше допустимого числа, Алиса и Боб прекращают выполнение протокола.
9. Алиса и Боб выполняют согласование информации и усиление конфиденциальности по оставшимся n битам для получения t совместных битов ключа.

Рис. 12.13. Протокол BB84 квантового распределения ключей, использующий четыре состояния.

Этот протокол, называемый BB84 в честь его создателей (см. разд. «История и дополнительная литература» в конце этой главы), приведен на рис. 12.13, а его экспериментальная реализация описана во вставке 12.6. Некоторые варианты этого протокола, например с использованием меньшего числа контрольных битов, называются так же.

Упражнение 12.26. Пусть a'_k — результат измерения Бобом кубита $|\psi_{a_k b_k}\rangle$ в предположении, что канал без шума и нет подслушивания. Покажите, что при $b'_k \neq b_k$ результат a'_k является случайнм и полностью не коррелирован с a_k , но $a'_k = a_k$ при $b'_k = b_k$.

Упражнение 12.27 (тесты случайной выборки). Проверка n случайно выбранных из $2n$ контрольных битов позволяет Алисе и Бобу с большой вероятностью оценить сверху количество ошибок в своих непроверенных битах. В частности, для любого $\delta > 0$ вероятность получить меньше, чем δn ошибок в контрольных битах и более, чем $(\delta + \varepsilon)n$ ошибок в остальных n битах, асимптотически меньше, чем $\exp[-O(\varepsilon^2 n)]$ для больших n . Мы докажем здесь это утверждение.

1. Без потери общности можно предположить, что число ошибок в $2n$ битах равно μn , где $0 \leq \mu \leq 2$. Если в контрольных битах произошло δn ошибок, а в остальных битах $(\delta + \varepsilon)n$ ошибок, то $\delta = (\mu - \varepsilon)/2$. Эти два утверждения означают следующее:

$< \delta n$ ошибок в контрольных битах

$$\Rightarrow < \delta n \text{ ошибок в контрольных битах}, \quad (12.184)$$

$> (\delta + \varepsilon)n$ ошибок в остальных битах

$$\Rightarrow > (\mu - \varepsilon)n \text{ ошибок в остальных битах}, \quad (12.185)$$

и, в сущности, утверждение вверху справа включает в себя утверждение внизу справа. Используя этот факт, покажите, что вероятность p , которую мы хотели бы оценить, удовлетворяет неравенству

$$p < \binom{2n}{n}^{-1} \binom{\mu n}{\delta n} \binom{(2-\mu)n}{(1-\delta)n} \delta n. \quad (12.186)$$

2. Покажите, что для больших n справедливо неравенство

$$\frac{1}{an+1} 2^{anH(b/a)} \leq \binom{an}{bn} \leq 2^{anH(b/a)}, \quad (12.187)$$

где $H(\cdot)$ — функция двоичной энтропии (11.8). Примените это неравенство к оценке для p , приведенной ранее.

3. Используйте неравенство $H(x) < 1 - 2(x - \frac{1}{2})^2$, чтобы получить окончательный результат, $p < \exp[-O(\varepsilon^2 n)]$. Вы можете заменить μ константой, которая соответствует наихудшему возможному случаю.
4. Сравните полученный результат с неравенством Чернова (вставка 3.4). Можете ли вы по-другому получить верхнюю оценку для p ?

Протокол B92

Протокол BB84 можно обобщить на случай использования других состояний и базисов и при этом получить аналогичные результаты. В самом деле, существует очень простой протокол для случая только двух состояний. В целях

упрощения достаточно рассмотреть, что происходит при передаче по каналу одного бита; этот случай легко обобщается на блоки кубитов, как в BB84.

Предположим, что Алиса приготавливает один произвольный классический бит a и посыпает Бобу

$$|\psi\rangle = \begin{cases} |0\rangle & \text{при } a = 0, \\ \frac{|0\rangle + |1\rangle}{\sqrt{2}} & \text{при } a = 1. \end{cases} \quad (12.188)$$

В зависимости от выбранного случайно классического бита a' Боб измеряет полученный им от Алисы кубит либо в Z -базисе $|0\rangle, |1\rangle$ (если $a' = 0$), либо в X -базисе $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ (если $a' = 1$). Из своего измерения Боб получает результат b , равный 0 или 1 в соответствии с собственными значениями X или Z (-1 и $+1$). Затем Боб открыто сообщает b (но утаивает a'), и Алиса и Боб проводят публичное обсуждение, оставляя в тайне только те пары $\{a, a'\}$, для которых $b = 1$. Отметим, что при $a = a'$ всегда $b = 0$. Только при $a = 1 - a'$ Боб получит $b = 1$ с вероятностью $\frac{1}{2}$. Окончательным ключом для Алисы будет a , а ключом для Боба будет $1 - a'$.

Этот протокол, известный как B92 (см. разд. «История и дополнительная литература» в конце главы), показывает, что невозможность достоверного различия неортогональных состояний лежит в основе квантовой криптографии.

Поскольку никаким подслушивающим устройствам невозможно различить состояния Алисы без нарушения корреляции между битами, которые Алиса и Боб получили в результате, этот протокол, как и BB84, позволяет Алисе и Бобу создать совместные биты ключа и определить верхнюю границу для шума и подслушивания во время их связи. Затем они могут выполнить согласование информации и усиление конфиденциальности, чтобы извлечь секретные биты из своих коррелированных случайных битовых строк.

Упражнение 12.28. Покажите, что при $b = 1$ биты a и a' полностью коррелированы.

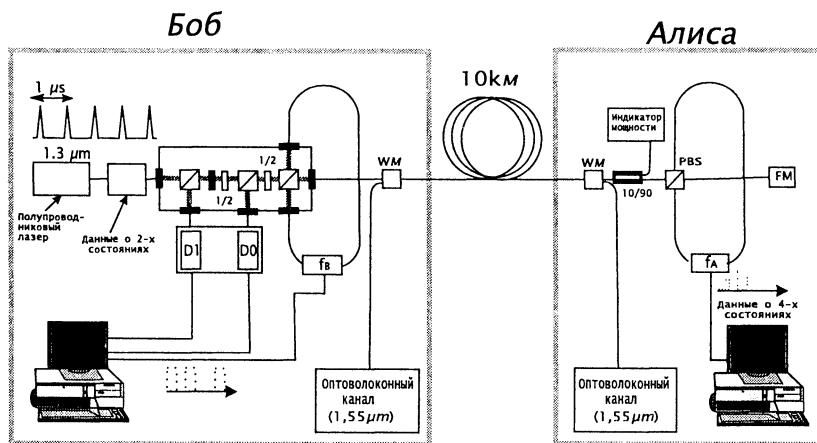
Упражнение 12.29. Составьте протокол, использующий шесть собственных значений X , Y и Z , и докажите, что он надежен. Обсудите чувствительность этого протокола к шуму и подслушиванию по сравнению с протоколами BB84 и B92.

Протокол ЭПР

Биты ключа в протоколах BB84 и B92 создаются Алисой. Однако, оказывается, что ключ может быть получен из фундаментально случайного процесса, основанного на свойствах запутанности. Это проиллюстрировано следующим протоколом.

Вставка 12.6. Экспериментальная квантовая криптография

Квантовое распределение ключей особенно интересно, поскольку легко осуществляется экспериментально. Здесь приведена разработанная IBM схема одной системы, в которой используются промышленные волоконно-оптические компоненты для доставки битов ключа на расстояние 10 километров:



Вначале Боб создает когерентные состояния $|\alpha\rangle$, используя полупроводниковый лазер, испускающий излучение с длиной волны $1,3 \mu\text{м}$, и передает их Алисе, которая ослабляет их, чтобы получить единственный фотон (приблизительно). Она также поляризует фотон в одном из четырех состояний протокола BB84, используя как $|0\rangle$ и $|1\rangle$ состояния горизонтальной и вертикальной поляризации. Затем Алиса возвращает фотон Бобу, который измеряет его с помощью анализатора поляризации в случайном базисе. Используя специальную конфигурацию, в которой фотон проходит один и тот же путь дважды, можно сделать прибор, который автоматически компенсирует несовершенства волоконной линии (такие как, медленно флюктуирующая длина пути и поляризационные сдвиги). Затем Алиса и Боб выбирают подмножество результатов, для получения которых они использовали один и тот же базис, соглашаются свою информацию и выполняют усиление конфиденциальности, связываясь по открытому каналу (по той же волоконной линии) при помощи фотонов длины волны $1,55 \mu\text{м}$. Биты ключа могут создаваться со скоростью несколько сотен в секунду. В конечном счете усовершенствование источника света и детектора должны позволить увеличить скорость на несколько порядков. Продемонстрировано квантовое распределение ключей на расстоянии, превышающем 40 километров, а также в телекоммуникационной линии, смонтированной под Женевским озером.

Предположим, что Алиса и Боб разделяют n запутанных пар кубитов в состоянии

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}. \quad (12.189)$$

Эти состояния, называемые ЭПР парами, можно получить множеством различных способов. Например, Алиса может приготовить эти пары и затем послать их половины Бобу или наоборот. Приготовить пары могла бы третья сторона и послать их половины Алисе и Бобу, или Алиса и Боб, встретившись много лет назад, могли бы поделить их и сохранить до настоящего времени. Алиса и Боб выбирают произвольное подмножество ЭПР пар и проверяют, нарушают ли они неравенство Белла (формула (2.225) в разд. 2.6), или проводят другой подходящий тест для степени совпадения. Прохождение теста гарантирует, что Алиса и Боб продолжают поддерживать достаточно чистые запутанные квантовые состояния, устанавливая нижнюю границу для степени совпадения остальных ЭПР пар (и, следовательно, для любого шума или подслушивания). Измеряя эти состояния в совместно определенных случайных базисах, Алиса и Боб получают коррелированные классические битовые строки, из битов которых они могут создать секретный ключ, как в протоколах BB92 и BB84. Используя рассуждение, основанное на границе Холево, из оценки степени совпадения ЭПР пар Алисы и Боба можно получить верхнюю оценку доступной Еве информации о битах ключа.

Откуда появились биты ключа в этом ЭПР протоколе? Из симметрии (Алиса и Боб осуществляют идентичные действия на своих кубитах, возможно даже одновременно), нельзя утверждать, что либо Алиса, либо Боб создает ключ. Напротив, ключ действительно случаен. В самом деле, тот же подход применяется и в протоколе BB84, поскольку он может быть сведен к обобщенной версии ЭПР протокола. Предположим, что Алиса приготавливает произвольный классический бит b и в соответствии с ним измеряет свою половину ЭПР пары либо в базисе $|0\rangle, |1\rangle$, либо в базисе $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$, получая a . Пусть Боб делает то же самое, измеряя в своем (выбранном случайно) базисе b' и получая a' . Затем они обмениваются b и b' по открытому классическому каналу и сохраняют в качестве своего ключа только те $\{a, a'\}$, для которых $b = b'$. Отметим, что этот ключ не определен до тех пор, пока Алиса и Боб не проведут измерения на своих половинах ЭПР пар. Аналогичное рассмотрение возможно и для протокола BB92. Квантовая криптография иногда рассматривается не как обмен или передача секретных ключей, а скорее, как их генерация, поскольку принципиально ни Алиса, ни Боб не может предопределить ключ, на котором они остановятся по завершении протокола.

12.6.4 Секретность и когерентная информация

Итак, мы описали основной протокол КРК и доказали, что он надежен, но не установили количественные ограничения. Оказывается, существует интересная фундаментальная связь между основными количественными мерами квантовой информации, описанными в этой главе, и мерами достижимой в принципе безопасности квантовой криптографии, которые мы опишем ниже.

Квантовая когерентная информация $I(\rho, \mathcal{E})$ задает нижнюю границу способности квантового канала передавать секретную информацию. В наиболее общем случае Алиса приготавливает состояния ρ_k^A , где $k = 0, 1, \dots$ — номера различных возможных состояний, которые она может послать с некоторой вероятностью p_k . Боб получает состояния $\rho_k^B = \mathcal{E}(\rho_k^A)$, которые могут быть отличны от ρ_k^A из-за шума канала или подслушивания Евы. Взаимная информация результата любого измерения, которое может произвести Боб, и выбранного Алисой значения k , $H_{\text{Боб:Алиса}}$, ограничена сверху энтропией Холево (12.6),

$$H_{\text{Боб:Алиса}} \leq \chi^B = S(\rho^B) - \sum_k p_k S(\rho_k^B), \quad (12.190)$$

где $\rho^B = \sum_k p_k \rho_k^B$. Аналогично, взаимная информация Евы с Алисой ограничена сверху,

$$H_{\text{Ева:Алиса}} \leq \chi^E = S(\rho^E) - \sum_k p_k S(\rho_k^E). \quad (12.191)$$

Поскольку любая дополнительная информация, которой обладает Боб по сравнению с Евой (по крайней мере, выше определенного порога), в принципе, может использоваться Бобом и Алисой для очищения общего секретного ключа, например с помощью усиления конфиденциальности, имеет смысл определить величину

$$\mathcal{P} = \sup [H_{\text{Боб:Алиса}} - H_{\text{Ева:Алиса}}], \quad (12.192)$$

как гарантированную секретность канала, где супремум берется по всем стратегиям, которые Алиса и Боб могут применить при использовании этого канала. Это и есть максимум дополнительной классической информации о квантовом сигнале Алисы, которую Боб может получить по сравнению с Евой. Согласно теореме ХШВ, Алиса и Боб могут применить такую стратегию, что $H_{\text{Боб:Алиса}} = \chi^B$, тогда как для любой стратегии Евы $H_{\text{Ева:Алиса}} \leq \chi^E$. Следовательно, $\mathcal{P} \geq \chi^B - \chi^E$ при подходящем выборе стратегии.

Из упр. 12.11 следует, что нижнюю оценку секретности \mathcal{P} можно получить из предположения, что все состояния сигнала Алисы $\rho_k^A = |\psi_k^A\rangle\langle\psi_k^A|$ являются чистыми состояниями, изначально не запутанными с Евой, которая начинает действовать в некотором состоянии $|0^E\rangle$ (без потери общности можно предположить, что оно должно быть чистым). В общем случае в канале от Алисы к Бобу существуют взаимодействия с некоторым окружением, отличным от Евы, но чтобы предоставить Еве наибольшее возможное преимущество, все эти взаимодействия могут быть приписаны ей, так что окончательное совместное состояние, полученное Евой и Бобом после передачи, таково

$$|\psi^{EB}\rangle = U|\psi_k^A\rangle|0^E\rangle. \quad (12.193)$$

Поскольку это чистое состояние, приведенные матрицы плотности ρ_k^E и ρ_k^B будут иметь одни и те же ненулевые собственные значения, и, следовательно, одинаковые энтропии $S(\rho_k^E) = S(\rho_k^B)$. Поэтому

$$\mathcal{P} \geq \chi^B - \chi^E \quad (12.194)$$

$$= S(\rho^B) - \sum_k p_k S(\rho_k^B) - S(\rho^E) + \sum_k p_k S(\rho_k^E) \quad (12.195)$$

$$= S(\rho^B) - S(\rho^E) \quad (12.196)$$

$$= I(\rho, \mathcal{E}). \quad (12.197)$$

Таким образом, нижняя оценка гарантированной секретности канала \mathcal{E} задается квантовой когерентной информацией $I(\rho, \mathcal{E})$, определенной в (12.118). Отметим, что этот результат не обеспечивается ни одним протоколом (которые могут иметь свои недостатки в обеспечении надежности). Протокол должен также проводить тесты (которые не учитываются в этом вычислении), чтобы определить свойства канала \mathcal{E} , для которого эту оценку можно применить. Итак, хотя теоретико-информационная оценка, к которой мы пришли здесь, достаточно хороша, нам еще нужно многое сделать, чтобы иметь возможность количественно определить надежность КРК!

12.6.5 Безопасность квантового распределения ключей

Насколько безопасно квантовое распределение ключей? Поскольку неизбежно нарушение передаваемого состояния при перехвате информации, у нас есть веская причина верить в безопасность КРК. Однако, чтобы дать заключение, что протокол действительно безопасен, необходимо *количественное* определение безопасности, которое явным образом ограничивает информированность Евы об окончательном ключе при фиксированной мере усилий Алисы и Боба. Используем следующий критерий:

Протокол КРК является *надежным*, если для любых параметров $s > 0$ и $l > 0$, выбранных Алисой и Бобом, и для любой стратегии подслушивания выполнение протокола либо прекращается, либо успешно завершается с вероятностью, по меньшей мере, $1 - O(2^{-s})$, и гарантирует, что взаимная информация Евы с окончательным ключом меньше, чем 2^{-l} . Стока ключа должна быть существенно случайной.

В этом разделе мы приведем основные элементы доказательства надежности протокола BB84. Это доказательство будет подходящим завершением данной главы, поскольку в нем элегантно сочетаются многие идеи квантовой теории информации, обеспечивая проведение достаточно простого и ясного рассуждения. Основой этого доказательства является весьма неожиданное наблюдение, что с учетом выполнения согласования информации и усиления конфиденциальности скорость передачи ключа, которую, в конечном счете, мы можем получить, совпадает с достижимой скоростью передачи кубита для CSS кодов (подразд. 10.4.2) по каналам связи с шумом!

Ниже в общих чертах изложена основная идея. Относительно просто установить, что протоколы BB84, B92 и ЭПР надежны, если Ева может одновременно «атаковать» не более одного передаваемого кубита. Трудность возника-

ет, если существует возможность коллективных атак, когда Ева манипулирует большими блоками передаваемых кубитов и, возможно, хранит их. Для рассмотрения этого случая необходимо более общее рассуждение. Предположим, что мы как-нибудь узнали, что Ева никогда не вносит больше t ошибочных кубитов на блок. Тогда Алиса могла бы закодировать свои кубиты исправляющим t ошибок квантовым кодом, так что любое вмешательство Евы могло бы быть устранено Бобом при декодировании. Чтобы осуществить этот план, нужно прояснить два обстоятельства. Во-первых, каким образом можно получить верхнюю границу для t ? Это возможно с помощью подходящего выбора контрольных кубитов, что обеспечивает надежность протокола (даже при коллективных атаках!). К сожалению, для выполнения этого протокола, как правило, требуется устойчивый к ошибкам квантовый компьютер, чтобы надежно кодировать и декодировать кубиты. Поэтому вторая проблема заключается в выборе квантового кода, такого, чтобы полная последовательность кодирования, декодирования и измерения могла осуществляться с использованием не квантовых вычислений и запоминания, а только с помощью приготовления и измерения отдельных кубитов. Использование CSS кодов (после некоторых упрощений) сводится к протоколу BB84. Ниже мы начнем с очевидно надежного протокола ЭПР, а затем решим две указанные проблемы, упростив протокол до BB84.

Требования для надежного протокола KPK

Предположим, что у Алисы есть n пар запутанных кубитов, каждая в состоянии

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \quad (12.198)$$

Обозначим это состояние как $|\beta_{00}\rangle^{\otimes n}$. Алиса передает половину каждой пары Бобу; из-за шума и подслушивания в канале результирующее состояние может не быть чистым и его можно описать матрицей плотности ρ . Затем Алиса и Боб осуществляют локальные измерения, чтобы получить ключ, как описано ранее. Приведенную ниже лемму можно использовать, чтобы показать, что степень совпадения ρ с $|\beta_{00}\rangle^{\otimes n}$ устанавливает верхнюю границу для взаимной информации Евы с ключом.

Лемма 12.19 (высокая точность воспроизведения подразумевает малую энтропию). Если $F(\rho, |\beta_{00}\rangle^{\otimes n}) > 1 - 2^{-s}$, то $S(\rho) < (2n + s + 1 / \ln 2)2^{-s} + O(2^{-2s})$.

Доказательство.

Если $F(\rho, |\beta_{00}\rangle^{\otimes n})^2 = {}^{\otimes n}\langle\beta_{00}|\rho|\beta_{00}\rangle^{\otimes n} > 1 - 2^{-s}$, то наибольшее собственное значение ρ должно быть больше, чем $1 - 2^{-s}$. Следовательно, энтропия ρ ограничена сверху энтропией диагональной матрицы плотности ρ_{\max} с диагональными элементами $1 - 2^{-s}, 2^{-s}/(2^{2n}-1), 2^{-s}/(2^{2n}-1), \dots, 2^{-s}/(2^{2n}-1)$, т. е. ρ_{\max} имеет наибольший элемент $1 - 2^{-s}$ и оставшаяся вероятность распределена в равной степени между остальными $2^{2n}-1$ диагональными элементами.

Из выражения

$$S(\rho_{\max}) = -(1 - 2^{-s}) \log(1 - 2^{-s}) - 2^{-s} \log \frac{2^{-s}}{2^{2n} - 1} \quad (12.199)$$

следует желаемый результат. ■

В соответствии с формулой (12.6), $S(\rho)$ является верхней границей для доступной Еве информации о результатах измерений ρ Алисы и Боба. Это означает, что, если протокол КРК может обеспечить Алису и Боба ЭПР парами со степенью совпадения, по меньшей мере, $1 - 2^{-s}$ (с большой вероятностью), то он надежен.

Упражнение 12.30. Упростите (12.199), чтобы получить выражение для $S(\rho)$, приведенное в утверждении леммы.

Упражнение 12.31. Может быть неясно, почему $S(\rho)$ ограничивает взаимную информацию Евы с результатами измерений Алисы и Боба. Покажите, что это следует из наихудшего допущения, состоящего в том, что Ева имеет полный контроль над каналом.

Случайная выборка может ограничить подслушивание сверху

Как может протокол обеспечить нижнюю границу степени совпадения ЭПР пар Алисы и Боба? Главная идея — классический прием, основанный на случайной выборке, с которым мы столкнулись в описании протокола BB84 (упр. 12.27). Однако, аргументы, основанные на классической вероятности, не применимы при рассмотрении данных, полученных в результате квантовых измерений. Это наглядно демонстрируется неравенством Белла (разд. 2.6). С другой стороны, квантовые эксперименты *все же допускают* классическую интерпретацию всякий раз, когда рассматриваются измерения наблюдаемых, относящихся к одному базису. К счастью, оказывается, что для оценки степени совпадения ЭПР пар требуется, чтобы Алиса и Боб произвели измерения только в одном базисе.

В соответствии с (10.14), с кубитом, который передается по квантовому каналу с шумом, может произойти одно из четырех событий: состояние кубита не изменится (I), классическая ошибка (изменение бита) (X), переворачивание фазы (Z), или комбинация классической ошибки и переворачивания фазы (Y). Напомним, что базис Белла определяется четырьмя состояниями

$$\begin{aligned} |\beta_{00}\rangle &= \frac{|00\rangle + |11\rangle}{\sqrt{2}}, & |\beta_{10}\rangle &= \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \\ |\beta_{01}\rangle &= \frac{|01\rangle + |10\rangle}{\sqrt{2}}, & |\beta_{11}\rangle &= \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \end{aligned} \quad (12.200)$$

Пусть Алиса посылает Бобу второй кубит из каждой пары. Если в этом кубите происходит классическая ошибка, то $|\beta_{00}\rangle$ преобразуется в $|\beta_{01}\rangle$. Аналогично, переворачивание фазы дает $|\beta_{10}\rangle$, а комбинация двух ошибок дает $|\beta_{11}\rangle$.

(с точностью до несущественного общего фазового множителя). Обычное измерение, которое обнаруживает классическую ошибку, описывается проекторами $\Pi_{bf} = |\beta_{01}\rangle\langle\beta_{01}| + |\beta_{11}\rangle\langle\beta_{11}|$ и $I - \Pi_{bf}$, и аналогично измерение, которое описывается проекторами $\Pi_{pf} = |\beta_{10}\rangle\langle\beta_{10}| + |\beta_{11}\rangle\langle\beta_{11}|$ и $I - \Pi_{pf}$, обнаруживает переворачивание фазы. Поскольку оба эти измерения не изменяют базис Белла, данные, полученные в результате этих измерений, можно описывать в терминах классической теории вероятностей. В самом деле, любые измерения, которые не изменяют базис Белла, можно также описывать классически.

Более точно, Алиса и Боб могут ограничить степень совпадения своих ЭПР пар посредством случайной выборки подмножества таких пар. Предположим, что Алиса посыпает Бобу половины $2n$ ЭПР пар. Потом они случайно выбирают из них n пар кубитов и проверяют их, измеряя Π_{bf} или Π_{pf} (также случайно выбранные). Из классических рассуждений, которые были использованы в тестах случайной выборки в протоколе BB84 (упр. 12.27), следует, что если обнаружено b классических ошибок или переворачиваний фазы, то остальные n ЭПР пар с экспоненциальной вероятностью будут содержать такое же количество ошибок при измерении в базисе Белла.

Состояния Белла нелокальны, и, как правило, измерения в базисе Белла требуют нелокальных операций, которые могут быть трудно реализуемы. Однако, к счастью, без них можно обойтись в данной процедуре, поскольку $\Pi_{bf} = (I \otimes I - Z \otimes Z)/2$ и $\Pi_{pf} = (I \otimes I - X \otimes X)/2$. Таким образом, Алиса и Боб могут провести необходимые проверки с локальными измерениями операторов Паули, измеряя либо Z , либо X .

Упражнение 12.32. Отметим, что локальные измерения, которые производят Алиса и Боб, как, например, $I \otimes X$ и $X \otimes I$, не коммутируют с базисом Белла. Покажите, что, несмотря на это, статистика, которую Алиса и Боб получают из своих измерений, такая же, какую они могли бы получить, измеряя Π_{bf} и Π_{pf} .

Модифицированный протокол Ло–Чу

Случайная выборка в базисе Белла обеспечивает Алису и Боба ЭПР парами ρ с степенью совпадения с идеальным состоянием $|\beta_{00}\rangle^{\otimes n}$, и, как отмечалось ранее, это ограничивает взаимную информацию Евы с результатами любых измерений над состоянием ρ . Однако, чтобы ρ можно было использовать для генерации ключа, Алиса и Боб должны уменьшать взаимную информацию Евы с их состояниями до экспоненциально малой величины. Это может быть достигнуто путем применения классического усиления конфиденциальности к результатам измерения Алисы и Боба или, что эквивалентно, Алиса и Боб могут сначала осуществить очищение запутанности, как это делалось в подразд. 12.5.2, чтобы получить ρ' , очень близкое к $|\beta_{00}\rangle^{\otimes m}$ для некоторого $m < n$, а затем измерить конечное состояние. Этот вид «квантового усиления конфиденциальности» будет нам полезен.

Приблизительная аргументация такова. Очищение запутанности можно осуществить, выполнив исправление квантовых ошибок. Поскольку ρ с большой

вероятностью должно иметь δn ошибок, кодирование этих кубитов квантовым кодом, исправляющим δn ошибок, позволяет исправить эти ошибки. Как мы убедились в подразделах 10.5.5 и 10.5.8, если используется стабилизирующий $[n, m]$ -код, то кодирование, измерение синдрома и исправление ошибок можно осуществить, измерив операторы Паули, определенные строками проверочной матрицы для данного кода. Алиса и Боб просто выполняют одинаковые измерения и операции восстановления на своих n кубитах — половинах ρ , получая состояние с исправленной ошибкой, степень совпадения с $|\beta_{00}\rangle^{\otimes m}$ порядка «единица минус вероятность того, что происходит больше, чем δn ошибок». При этом оказывается, что измерения синдрома не изменяют базис Белла, так как Алиса и Боб выполняют одинаковые действия.

Сочетание случайной выборки и очищения запутанности дает модифицированный протокол Ло–Чу, представленный на рис. 12.14. Сделаем несколько замечаний по поводу этого протокола. Благодаря случайным преобразованиям Адамара, которые выполняются на этапах 3 и 7 протокола, не имеет значения, в каком базисе, X или Z , Ева измеряет каждый доступный ей кубит (что приводит к ошибкам X или Z). Эти преобразования определяют, какой из проекторов P_{bf} или P_{pf} нужно измерять на контрольных кубитах. Процедура этапа 9 может быть выполнена для любого стабилизирующего кода, как в упр. 12.34. Граница Варшамова–Гильберта для CSS кодов (10.74) показывает, что существуют хорошие квантовые коды для блоков большой длины, так что если выбрать n достаточно большим, то для квантового $[n, m]$ -кода, исправляющего δn ошибок, критерии надежности будут выполнены.

Упражнение 12.33. Пусть $\{M_1, M_2, \dots, M_n\}$ — множество наблюдаемых, которые принимают значения X_i при измерении над состоянием ρ . Докажите, что случайные величины X_i можно описывать в терминах классической теории вероятностей, если $[M_i, M_j] = 0$, т. е. если они попарно коммутируют.

Упражнение 12.34 (очищение запутанности посредством исправления ошибок). В подразд. 10.5.8 мы показали, что кодовые слова стабилизирующего $[n, m]$ -кода можно получить, измеряя его образующие g_1, \dots, g_{n-m} над произвольным n -кубитовым квантовым состоянием и применяя затем операторы Паули, чтобы получить собственное состояние всех образующих с собственным значением +1. Используя эту идею, покажите, что, если мы начинаем с n ЭПР пар в состоянии $|\beta_{00}\rangle^{\otimes n}$ и выполняем измерения одинаковых образующих на двух n -кубитовых половинах этих пар, а затем применяем операторы Паули для исправления разницы в результатах этих измерений, то получаем закодированное состояние $|\beta_{00}\rangle^{\otimes m}$. Покажите также, что если стабилизирующий код исправляет до δn ошибок, то даже когда в n -кубитовой половине допускается δn ошибок, мы получим $|\beta_{00}\rangle^{\otimes m}$.

Квантовый протокол исправления ошибок

В модифицированном протоколе Ло–Чу используется исправление квантовых ошибок для выполнения очищения запутанности; этот протокол, по существу,

Модифицированный протокол Ло–Чу

1. Алиса создает $2n$ ЭПР пар в состоянии $|\beta_{00}\rangle^{\otimes 2n}$.
2. Алиса случайным образом выбирает n из $2n$ ЭПР пар, чтобы использовать их в качестве контрольных для проверки вмешательства Евы. Пока Алиса ничего не делает с ними.
3. Алиса выбирает произвольную $2n$ -битовую строку b и применяет преобразование Адамара к второму кубиту каждой пары, для которой $b = 1$.
4. Алиса посылает Бобу второй кубит каждой пары.
5. Боб получает кубиты и публично объявляет об этом.
6. Алиса объявляет b и те n кубитов, которые являются контрольными.
7. Боб применяет преобразования Адамара к кубитам, для которых $b = 1$.
8. Алиса и Боб измеряют n своих контрольных кубитов в базисе $|0\rangle, |1\rangle$, и каждый открыто оповещает о результатах. Если больше, чем t из n битов не совпадают, они прекращают выполнение протокола.
9. Алиса и Боб измеряют n своих остальных кубитов в соответствии с проверочной матрицей для заранее определенного квантового $[n, m]$ -кода, исправляющего до t ошибок. Они обмениваются результатами, вычисляют синдромы ошибок и затем исправляют свои состояния, получая m почти идеальных ЭПР пар.
10. Алиса и Боб измеряют m ЭПР пар в базисе $|0\rangle, |1\rangle$, чтобы получить общий секретный ключ.

Рис. 12.14. Протокол КРК, являющийся надежным благодаря использованию совершенных квантовых компьютеров, исправлению ошибок и случайному тестированию ЭПР пар

основан на ЭПР протоколе. Запутанность является хрупким ресурсом, и для исправления квантовых ошибок, как правило, требуются эффективные квантовые компьютеры, которые еще необходимо построить. К счастью, однако, этот протокол можно упростить, не нарушая надежности всей процедуры. Начнем с устранения необходимости распределения ЭПР пар.

Отметим, что измерения, которые производит Алиса на своих кубитах в конце модифицированного протокола Ло–Чу, могут быть выполнены в самом начале без изменения состояний всех остальных кубитов. Измерения Алисой ее половин контрольных ЭПР пар на этапе 8 разрушают пары, превращая их в n одиночных кубитов, так что вместо запутанных состояний Алиса может просто посыпать одиночные кубиты. Это приводит к изменению этапов протокола

- 1'. Алиса приготавливает n случайных контрольных битов и n ЭПР пар в состоянии $|\beta_{00}\rangle^{\otimes n}$. Она также приготавливает n кубитов в состоянии $|0\rangle$ или $|1\rangle$ в соответствии с контрольными битами.
- 2'. Алиса случайным образом выбирает n позиций (из $2n$) и помещает контрольные кубиты в эти позиции, а половину каждой ЭПР пары — в остальные позиции.
- 3'. Боб измеряет n контрольных кубитов в базисе $|0\rangle$, $|1\rangle$ и публично сообщает результат Алисе. Если больше t битов не совпадают, Алиса и Боб прекращают выполнение протокола.

Аналогично, измерения Алисы на этапах 9 и 10 разрушают ЭПР пары, превращая их в *случайные* кубиты, *закодированные случайным квантовым кодом*. Это можно показать следующим образом. Особенно удобным кодом является CSS $[n, m]$ -код C_1 по C_2 , $\text{CSS}(C_1, C_2)$, который кодирует m кубитов в n кубитов и исправляет до t ошибок; этот код мы используем в остальной части этого раздела. Напомним из подразд. 10.4.2, что для этого кода H_1 и H_2^\perp являются проверочными матрицами, соответствующими классическим кодам C_1 и C_2^\perp и каждое кодовое состояние можно представить как

$$\frac{1}{|C_2|} \sum_{w \in C_2} |v_k + w\rangle, \quad (12.201)$$

где v_k принадлежит одному из 2^m классов смежности C_2 в C_1 (индекс k указывает, что вектор v_k принадлежит классу смежности k -го кодового слова). Напомним также, что существует семейство кодов, эквивалентных этому, $\text{CSS}_{z,x}(C_1, C_2)$, с кодовыми состояниями

$$|\xi_{v_k, z, x}\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{w \in C_2} (-1)^{z \cdot w} |v_k + w + x\rangle. \quad (12.202)$$

Эти состояния образуют ортонормированный базис для 2^n -мерного гильбертова пространства (см. упр. 12.35), и, следовательно, можно записать состояние n ЭПР пар Алисы как

$$|\beta_{00}\rangle^{\otimes n} = \sum_{j=0}^{2^n} |j\rangle |j\rangle = \sum_{v_k, z, x} |\xi_{v_k, z, x}\rangle |\xi_{v_k, z, x}\rangle. \quad (12.203)$$

Отметим, что в этом выражении мы использовали два кет-вектора, где первый обозначает кубиты, которые хранит Алиса, а второй — кубиты, которые она посыпает Бобу. Когда Алиса измеряет образующие стабилизатора, соответствующие H_1 и H_2^\perp , на своих кубитах на этапе 9, она получает *случайные* значения для x и z , и аналогично, ее измерение на шаге 10 дает ей *случайное* v_k . Остальные n кубитов будут в состоянии $|\xi_{v_k, z, x}\rangle$, которое соответствует

кодовому слову для v_k в $\text{CSS}_{z,x}(C_1, C_2)$. Это всего лишь закодированная форма 2^m -кубитового состояния $|k\rangle$. Следовательно, как сказано выше, измерения Алисы создают случайные кубиты, закодированные случайным кодом.

Итак, вместо того, чтобы отправить половины ЭПР пар Алиса может случайно выбрать x, z и k , затем закодировать $|k\rangle$ кодом $\text{CSS}_{z,x}(C_1, C_2)$ и отослать Бобу закодированные n кубитов. Таким образом получаются модифицированные этапы протокола

- 1''. Алиса приготавливает n случайных контрольных битов, случайный m -битовый ключ k и две произвольные n -битовые строки x и z . Она кодирует $|k\rangle$ кодом $\text{CSS}_{z,x}(C_1, C_2)$ и также приготавливает n кубитов в состоянии $|0\rangle$ или $|1\rangle$ в соответствии с контрольными битами.
- 2''. Алиса случайным образом выбирает n позиций (из $2n$), помещает контрольные кубиты в эти позиции и закодированные кубиты в остальные позиции.
- 6''. Алиса объявляет b, x, z и позиции n контрольных кубитов.
- 9''. Боб декодирует остальные n кубитов из $\text{CSS}_{z,x}(C_1, C_2)$.
- 10''. Боб измеряет свои кубиты, чтобы получить общий секретный ключ k .

Полученный в результате так называемый протокол CSS кодов приведен на рис. 12.15.

Упражнение 12.35. Покажите, что состояния $|\xi_{v_k,z,x}\rangle$, определенные в (12.202), образуют ортонормированный базис для 2^n -мерного гильбертова пространства, т. е.

$$\sum_{v_k, z, x} |\xi_{v_k,z,x}\rangle \langle \xi_{v_k,z,x}| = I. \quad (12.204)$$

Указание: для $[n, k_1]$ -кода C_1 , $[n, k_2]$ -кода C_2 и $m = k_1 - k_2$ существует 2^m различных значений v_k , 2^{n-k_1} различных x и 2^{k_2} различных z .

Упражнение 12.36. Проверьте равенство (12.203).

Упражнение 12.37. Существует другой способ понять, почему измерения Алисы на этапах 9 и 10 разрушают ЭПР пары, превращая их в случайные кубиты, закодированные случайным квантовым кодом. Предположим, что у Алисы есть ЭПР пара $(|00\rangle + |11\rangle)/\sqrt{2}$. Покажите, что если Алиса измеряет первый кубит в базисе X , то разрушается второй кубит, переходя в собственное состояние X , определенное результатом измерения. Аналогично, покажите, что если Алиса измеряет в базисе Z , то второй кубит остается в собственном состоянии Z , определенном результатом измерения. Используя это наблюдение и результаты подразд. 10.5.8, покажите, что измерения H_1 , H_2^\perp и \tilde{Z} , выполненные Алисой над ее половинами ЭПР пар, дают случайное кодовое слово $\text{CSS}_{z,x}(C_1, C_2)$, которое тоже определено результатами измерений Алисы.

Протокол CSS кодов

- 1''. Алиса создает n случайных контрольных битов, случайный t -битовый ключ k и две случайные n -битовые строки x и z . Она кодирует $|k\rangle$ кодом $\text{CSS}_{z,x}(C_1, C_2)$ и приготавливает n кубитов в состоянии $|0\rangle$ или $|1\rangle$ в соответствии с контрольными битами.
- 2''. Алиса случайным образом выбирает n позиций (из $2n$), помещает контрольные кубиты в эти позиции, а закодированные кубиты в оставшиеся позиции.
3. Алиса выбирает случайную $2n$ -битовую строку b и применяет преобразование Адамара к каждому кубиту, для которого $b = 1$.
4. Алиса посыпает Бобу полученные в результате кубиты.
5. Боб получает кубиты и публично объявляет об этом.
- 6'. Алиса объявляет b, x, z и позиции n контрольных кубитов.
7. Боб применяет преобразования Адамара к кубитам, для которых $b = 1$.
- 8'. Боб измеряет n контрольных кубитов в базисе $|0\rangle, |1\rangle$ и открыто сообщает результаты Алисе. Если больше, чем t из n битов не совпадают, Алиса и Боб прекращают выполнение протокола.
- 9'. Боб декодирует остальные n кубитов из $\text{CSS}_{z,x}(C_1, C_2)$.
- 10'. Боб измеряет свои кубиты, чтобы получить общий секретный ключ k .

Рис. 12.15. Надежный протокол CSS кодов, полученный упрощением модифицированного протокола Ло–Чу.

Протокол CSS кодов надежен, поскольку получен непосредственно из модифицированного протокола Ло–Чу и при этом гораздо проще, так как не использует ЭПР пары явным образом. К сожалению, этого все-таки недостаточно, поскольку для реализации протокола требуются надежные квантовые вычисления, чтобы осуществить кодирование и декодирование (вместо приготовления и измерения одиночных кубитов), и Бобу необходимо временно сохранить кубиты в квантовой памяти в ожидании сообщения от Алисы. Однако, эти два требования можно исключить, поскольку CSS коды отделяют исправление перевернутой фазы от исправления классических ошибок.

Сведение к протоколу BB84

Во-первых, отметим, что Боб измеряет свои кубиты в базисе Z непосредственно после декодирования, поэтому информация об исправлении фазы, которую

посыпает Алиса в качестве z , не нужна. Следовательно, поскольку C_1 и C_2 — классические коды, вместо декодирования и измерения Боб может провести непосредственные измерения, получая $v_k + w + x + \varepsilon$ (где ε обозначает некоторую возможную ошибку, обусловленную шумом в канале и действиями Евы), а затем декодировать *классически*: Боб вычитает объявленное Алисой значение x , исправляет результат так, чтобы он совпал с кодовым словом в C_1 , которое есть в точности $v_k + w$, если кодовое расстояние не превышено. Окончательный ключ k является классом смежности $v_k + w + C_2$ в C_1 (см. Приложение 2, где дано определение классов смежности и приведены обозначения). Таким образом, имеем

9''. Боб измеряет остальные кубиты, получая $v_k + w + x + \varepsilon$, вычитает x из результата, исправляет ошибки при помощи кода C_1 , что дает $v_k + w$.

10''. Боб вычисляет класс смежности $v_k + w + C_2$ в C_1 , чтобы получить ключ k .

Во-вторых, поскольку Алисе не нужно объявлять z , состояние, которое она посыпает, является смешанным, усредненным по произвольным значениям z ,

$$\rho_{v_k, x} = \frac{1}{2^n} \sum_z |\xi_{v_k, z, x}\rangle \langle \xi_{v_k, z, x}| \quad (12.205)$$

$$= \frac{1}{2^n |C_2|} \sum_{w_1, w_2 \in C_2} (-1)^{z(w_1 + w_2)} |v_k + w + x\rangle \langle v_k + w + x| \quad (12.206)$$

$$= \frac{1}{|C_2|} \sum_{w \in C_2} |v_k + w + x\rangle \langle v_k + w + x|. \quad (12.207)$$

Это состояние создать просто: Алисе нужно только *классическим способом* случайно выбрать $w \in C_2$ и приготовить $|v_k + w + x\rangle$, используя свои случайно определенные x и k . Таким образом, мы имеем

1'''. Алиса создает n случайных контрольных битов, случайную n -битовую строку x , случайное $v_k \in C_1/C_2$ и случайное $w \in C_2$. Она приготавливает n кубитов в состоянии $|0\rangle$ или $|1\rangle$ в соответствии с $v_k + w + x$, и, аналогично, n кубитов в соответствии с контрольными битами.

Этапы 1''' и 9'' можно и дальше упростить, слегка изменив этап 6'. Теперь Алиса посыпает состояние $|v_k + w + x\rangle$, Боб его получает и измеряет, что дает $v_k + w + x + \varepsilon$; затем Алиса посыпает x , которое Боб вычитает, получая $v_k + w + \varepsilon$. Но если Алиса выбирает $v_k \in C_1$ (вместо C_1/C_2), то в w нет необходимости. Более того, тогда $v_k + x$ является полностью случайной n -битовой строкой, и поэтому вместо указанных выше действий Алиса может произвольно выбрать x и послать $|x\rangle$. Боб получит и измерит его, что даст $x + \varepsilon$, затем Алиса пошлет $x - v_k$, которое Боб вычтет, получая $v_k + \varepsilon$. Теперь нет никакой разницы между случайными контрольными битами и битами кода! Это дает нам

1''''. Алиса выбирает случайное $v_k \in C_1$ и приготавливает $2n$ кубитов в состоянии $|0\rangle$ или $|1\rangle$ в соответствии с $2n$ случайными битами.

- 2''. Алиса случайным образом выбирает n позиций (из $2n$) для контрольных кубитов, а остальную часть обозначает как $|x\rangle$.
- 6''. Алиса объявляет b , $x - v_k$ и позиции n контрольных кубитов.
- 9''. Боб измеряет остальные кубиты, получая $x + \epsilon$, вычитает $x - v_k$ из полученного результата, исправляет ошибки при помощи кода C_1 , что дает v_k .
- 10''. Алиса и Боб вычисляют класс смежности $v_k + C_2$ в C_1 , чтобы получить ключ k .

Заметим далее, что Алисе нет необходимости выполнять операции Адамара (хотя на практике операции с одиночными кубитами не так трудны в случае представления их фотонами). Алиса может вместо этого подготовить свои кубиты или в базисе $|0\rangle, |1\rangle(Z)$, или в базисе $|+\rangle, |-\rangle(X)$ в зависимости от битов b :

- 1''''. Алиса создает $(4 + \delta)n$ случайных битов. Для каждого бита она приготавливает кубит либо в базисе $|0\rangle, |1\rangle$, либо в базисе $|+\rangle, |-\rangle$ в зависимости от произвольной битовой строки b .

Таким образом, кодирование и декодирование теперь выполняются классически. Осталась одна проблема — устранить необходимость квантовой памяти. Чтобы решить ее, предположим, что Боб делает измерения сразу после получения кубитов от Алисы, в случайно выбранном базисе — X или Z . Когда Алиса впоследствии объявляет b , они могут сохранить только те биты, для которых их базисы оказываются одними и теми же. Это позволяет Бобу полностью отказаться от своего квантового запоминающего устройства. Заметим, что с большой вероятностью Алиса и Боб теряют половину своих битов, поэтому для того, чтобы получить то же самое число битов ключа, что было раньше, они должны начать с несколько большего (на δ), чем двойное количество случайных первоначальных битов. Конечно, теперь Алиса должна отложить выбор, контрольных битов до тех пор, пока не закончится этап согласования. Это дает нам окончательный протокол (рис. 12.16), такой же, что и BB84, только с незначительными внешними отличиями. Отметим, что при помощи классического кода C_1 осуществляется согласование информации, а вычисление класса смежности $v_k + C_2$ в C_1 усиливает конфиденциальность (см. подразд. 12.6.2).

Итак, мы последовательно доказали надежность протокола BB84 квантового распределения ключей, начав с очевидно надежной процедуры, требующей безошибочного квантового вычисления и квантовой памяти, а затем постепенно свели ее к протоколу BB84. Поскольку проведенные модификации сохраняют неизменным квантовое состояние Евы (с учетом раскрытой классической информации), мы делаем вывод, что протокол BB84 надежен. Однако, приведенное доказательство применимо лишь для ситуации, когда посылаются идеально приготовленные состояния. На практике источники кубитов несовершены; например, таким источником часто является лазерное излучение, ослабленное приблизительно до отдельных фотонов, представляющих кубиты

(как описано в подразд. 7.4.1). Кроме того, в приведенном доказательстве не рассматриваются трудности, которые Алиса и Боб должны преодолеть при декодировании; для реального распределения ключей код C_1 должен быть эффективно декодируемым. Это доказательство также не устанавливает верхнюю границу для приемлемого подслушивания; оно использует CSS коды, которые не оптимальны. Существует оценка, что приемлемое количество классических фазовых ошибок при использовании протокола, подобного BB84, порядка 11%, но и при кодировании и декодировании с помощью квантовых компьютеров допустимо и большее количество ошибок. Предельные возможности квантовой криптографии представляют собой интересный, пока еще не решенный вопрос, и мы ожидаем, что подобные фундаментальные вопросы о физических пределах для вычислений и связи будут увлекать исследователей и в будущем.

Надежный протокол BB84

1. Алиса выбирает $(4 + \delta)n$ случайных битов.
2. Для каждого бита Алиса приготавливает кубит либо в базисе Z , либо в базисе X в соответствии с произвольной битовой строкой b .
3. Алиса посыпает Бобу полученные в результате кубиты.
4. Алиса выбирает случайным образом $v_k \in C_1$.
5. Боб получает кубиты, публично объявляет об этом и измеряет каждый кубит, выбрав случайным образом базис Z или X .
6. Алиса объявляет b .
7. Алиса и Боб отбрасывают те биты, которые Боб измерил в базисе, отличном от b . С большой вероятностью остается, по меньшей мере, $2n$ битов; в противном случае выполнение протокола прекращается. Алиса произвольно выбирает n контрольных битов из множества оставшихся $2n$ и объявляет о своем выборе.
8. Алиса и Боб публично сравнивают значения своих контрольных битов. Если количество не совпадающих битов больше допустимого числа t , Алиса и Боб прекращают выполнение протокола. У Алисы остается n -битовая строка x , а у Боба $x + \epsilon$.
9. Алиса объявляет $x - v_k$. Боб вычитает это число из своего результата и исправляет ошибку с помощью кода C_1 , получая v_k .
10. Алиса и Боб вычисляют класс смежности $v_k + C_2$ в C_1 , чтобы получить ключ k .

Рис. 12.16. Окончательный протокол КРК, полученный упрощением протокола CSS кодов до протокола BB84 (с незначительными внешними различиями) Для упрощения мы опустили штрихи в нумерации этапов

Упражнение 12.38. Покажите, что, возможность различать неортогональные состояния, нарушает надежность протокола BB84, и более того, всех описанных протоколов КРК.

Задача 12.1. Здесь мы приводим другой способ доказательства границы Холево. Энтропия Холево имеет вид

$$\chi \equiv S(\rho) - \sum_x p_x S(\rho_x). \quad (12.208)$$

- Предположим, что квантовая система состоит из двух частей, A и B . Покажите, что

$$\chi_A \leq \chi_{AB}. \quad (12.209)$$

(*Указание.* Введите дополнительную систему, коррелиированную с AB , и примените сильную субаддитивность.)

- Пусть \mathcal{E} — квантовое преобразование. Используя предыдущий результат, покажите, что

$$\chi' \equiv S(\mathcal{E}(\rho)) - \sum_x p_x S(\mathcal{E}(\rho_x)) \leq \chi \equiv S(\rho) - \sum_x p_x S(\rho_x), \quad (12.210)$$

т. е. энтропия Холево χ не увеличивается под действием квантовых преобразований. Это важный и полезный факт.

- Пусть E_y — множество POVM-элементов. Дополним рассматриваемую квантовую систему «прибором» M с ортонормированным базисом $|y\rangle$. Определим квантовое преобразование как

$$\mathcal{E}(\rho \otimes |0\rangle\langle 0|) \equiv \sum_y \sqrt{E_y} \rho \sqrt{E_y} \otimes |y\rangle\langle y|, \quad (12.211)$$

где $|0\rangle$ — некоторое стандартное чистое состояние «прибора» M . Докажите, что $\chi_M = H(X:Y)$ после действия \mathcal{E} . Используя этот и предыдущие два результата, покажите, что

$$H(X:Y) \leq S(\rho) - \sum_x p_x S(\rho_x), \quad (12.212)$$

это и есть граница Холево.

Задача 12.2. Эта задача представляет собой обобщение предыдущей. Докажите теорему о невозможности копирования, показав, что процесс копирования для неортогональных чистых состояний с необходимостью увеличивает χ .

Задача 12.3. Для фиксированного квантового источника и скорости передачи $R > S(\rho)$ постройте квантовую схему, реализующую сжатие в $1/R$ раз.

Задача 12.4 (линейность запрещает копирование). Предположим, что у нас есть квантовая машина с двумя слотами, A и B . Слот A , *слот данных*, вначале находится в неизвестном квантовом состоянии ρ . Это состояние, которое нужно скопировать. Слот B , *целевой слот*, вначале находится в некотором стандартном квантовом состоянии σ . Будем предполагать, что любая рассматриваемая процедура копирования является *линейной* по начальному состоянию

$$\rho \otimes \sigma \rightarrow \mathcal{E}(\rho \otimes \sigma) = \rho \otimes \rho, \quad (12.213)$$

где \mathcal{E} — некоторая линейная функция. Покажите, что, если $\rho_1 \neq \rho_2$ являются такими операторами, что

$$\mathcal{E}(\rho_1 \otimes \sigma) = \rho_1 \otimes \rho_1, \quad (12.214)$$

$$\mathcal{E}(\rho_2 \otimes \sigma) = \rho_2 \otimes \rho_2, \quad (12.215)$$

то любая смесь ρ_1 и ρ_2 при помощи этой процедуры копируется неправильно.

Задача 12.5 (пропускная способность квантового канала для классической информации — исследование). Является ли пропускная способность для факторизованного состояния (12.71) истинной пропускной способностью квантового канала с шумом для классической информации, т. е. пропускной способностью, когда разрешены запутанные состояния на входе канала?

Задача 12.6 (методы достижения пропускной способности — исследование). Предложите эффективную конструкцию для кодов со скоростью передачи, близкой к пропускной способности для факторизованного состояния (12.71), т. е. к пропускной способности квантового канала с шумом для классической информации.

Задача 12.7 (пропускная способность квантового канала — исследование). Найдите метод оценки пропускной способности заданного квантового канала \mathcal{E} для квантовой информации.

Краткое содержание главы

- **Невозможность копирования.** Невозможно сконструировать квантовое устройство, производящее $|\psi\rangle|\psi\rangle$ при заданном $|\psi\rangle$ для произвольного $|\psi\rangle$.
- **Граница Холево.** Максимум доступной классической информации при попытке различения квантовых состояний ρ_x с распределением вероятностей p есть

$$H(X:Y) \leq \chi \equiv S\left(\sum_x p_x \rho_x\right) - \sum_x p_x S(\rho_x).$$

- **Теорема Шумахера о кодировании для квантового канала без шума.** $S(\rho)$ можно интерпретировать как число кубитов, необходимых для точного представления квантового источника, описываемого матрицей плотности ρ .
- **Теорема Холево–Шумахера–Вестморленда.** Пропускная способность квантового канала с шумом \mathcal{E} для классической информации определяется выражением

$$C(\mathcal{E}) = \max_{\{p_x, |\psi_x\rangle\}} S\left(\sum_x p_x \mathcal{E}(|\psi_x\rangle\langle\psi_x|)\right) - \sum_x p_x S(\mathcal{E}(|\psi_x\rangle\langle\psi_x|)). \quad (12.216)$$

- **Условие мажоризации для преобразования запутанности.** Алиса и Боб могут преобразовать $|\psi\rangle$ в $|\varphi\rangle$ при помощи локальных операций и классической коммуникации тогда и только тогда, когда $\lambda_\psi \prec \lambda_\varphi$, где λ_ψ — вектор собственных значений приведенной матрицы плотности для $|\psi\rangle$ (аналогично для λ_φ).
- **Очищение и разбавление запутанности чистого состояния.** Алиса и Боб могут преобразовать n копий разделенного состояния $|\psi\rangle$ в $nS(\rho)$ пар Белла и обратно с помощью только локальных операций и классической коммуникации при $n \rightarrow \infty$, где ρ — приведенная матрица плотности.
- **Квантовая криптография.** Гарантированно безопасное распределение ключей возможно посредством коммуникации с использованием неортогональных квантовых состояний по протоколу, подобному BB84. Подслушивание в канале вызовет заметное увеличение скорости возникновения ошибок, поскольку получение информации приводит к возмущению квантового состояния.

История и дополнительная литература

Книга Ковера и Томаса [106] является простым введением в классическую теорию информации. Читатель, который хотел бы найти более глубокое, но тем не менее понятное изложение теории информации, может обратиться к книге Цижара и Кернера [88]. Рекомендуем также прочесть оригинальные статьи Шеннона, которые оказали большое влияние на науку двадцатого века. Эти статьи собраны в отдельном томе Шеннона и Уивера [378]. Беннет и Шор [72] и Беннет и Дивинченцо [37] написали превосходные обзорные статьи по квантовой теории информации.

Теорема о невозможности копирования появилась благодаря Диксу [122] и Бутерсу и Зуреку [424]. Очень много работ посвящено развитию их результатов. В большинстве статей описываются различные процедуры копирования, которые представляют интерес, поскольку позволяют оптимизировать некоторую меру точности воспроизведения при копировании или некоторое другое свойство. Мы не будем пытаться сделать здесь полный обзор этих статей, но отметим, что многие из них можно найти в Интернете на странице <http://arXiv.org/> в архиве quant-ph. К работам, представляющим особый интерес, относятся работа Барнума, Кейвса, Йожа и Шумахера [34], в которой теорема о невозможности копирования распространена на смешанные состояния и устройства неунитарного копирования; работа Мора [292] по копированию состояний составных систем; статья Вестморланда и Шумахера [421] о возможной эквивалентности копирования и связи со скоростью, превышающей скорость света, и работа ван Энка [399] с критикой такой эквивалентности.

Гипотезу о границе Холево выдвинул Гордон [164] в 1964 г., а доказал Холево [190] в 1973. Простое доказательство, которое мы привели, основано на трудном для доказательства неравенстве сильной субаддитивности, однако Холево использовал более прямой подход, который был упрощен Фухсом и Кейвсом [146]. Метод с применением сильной субаддитивности впервые использовали Юен и Озава [428]; см. также работу Шумахера, Вестморланда и Бутерса [382].

Теорема о кодировании для классического канала без шума принадлежит Шеннону [353, 378]. Теорема о кодировании для квантового канала без шума описана в новаторской статье Шумахера [350], в которой введены многие фундаментальные понятия квантовой теории информации, включая источники, меры точности воспроизведения и квантовое состояние как ресурс, который можно рассматривать в теоретико-информационных терминах. В этой работе появился широко используемый теперь термин *кубит*, который возник в дискуссии Шумахера с Буттерсом. В статье Йожа и Шумахера [206] описан упрощенный вариант подхода Шумахера. Эти работы основаны на *усредненной по ансамблю* степени совпадения (см. упр. 12.8) в отличие от приведенного в данной книге доказательства Нильсена [303], в котором используется точность воспроизведения запутанности. Небольшой пробел в оригинальных работах Шумахера, а также Шумахера и Йожа, восполнен работой Барнума, Фухса, Йожа и Шумахера [52]. Впоследствии М. Городецкий [193] предложил более сильное доказательство того же результата, что открыло путь к теории квантового сжатия данных, представленных ансамблями смешанных состояний. Описанная во вставке 12.4 процедура сжатия, которая является квантовым аналогом метода кодирования перечислением Ковера [106], приписывается Шумахеру [350], а квантовые схемы для нее приведены в работе Клива и Дивинченцо [79]. Обобщив этот подход, Браунштейн, Фухс, Готтесман и Ло, получили квантовый аналог метода кодирования Хаффмана [51], а Чанг и Мода [94] — арифметического кодирования.

Теорема Холево–Шумахера–Вестморланда (ХШВ) имеет интересную историю. Задача, с которой связана эта теорема, была впервые рассмотрена Холево [191] в 1979 г., который получил некоторые результаты для ее решения. Не по-

дозревая об этой работе, Хаусладен, Йожа, Шумахер, Вестморланд и Вутерс [185] в 1996 г. решили эту задачу для частного случая. Независимо и вскоре после них Холево [192] и Шумахер и Вестморланд [380] доказали теорему ХШВ о пропускной способности квантового канала с шумом для классической информации. Фухс [158] описал некоторые интересные примеры пропускной способности для факторизованного состояния, когда ансамбль состояний, обеспечивающий максимум выражения (12.71), содержит неортогональные члены. Кинг и Рускаи [228] существенно продвинулись в решении задачи, показав, что пропускная способность для факторизованного состояния совпадает с пропускной способностью для состояния общего вида, однако задача в целом осталась нерешенной.

Лин dblад [247] дал определение обменной энтропии, а Шумахер [352] независимо ввел это понятие, доказав квантовое неравенство Фано. Понятие когерентной информации ввели Ллойд [255], Шумахер и Нильсен [365] в контексте пропускной способности квантового канала с шумом; в работе [365] доказано неравенство квантовой обработки данных. Таблицу, которая содержит неравенства, упомянутые в упр. 12.15, можно найти в докторской диссертации Нильсена [303]. Все еще не решенная задача определения пропускной способности квантового канала (задача 12.7) имеет интересную историю. Сначала работа в этом направлении велась, исходя из нескольких различных точек зрения, как можно увидеть из статей Барнума, Нильсена и Шумахера [63], Беннета, Дивинченцо, Смолина и Вутерса [42], Ллойда [255], Шумахера [352], Шумахера и Нильсена [365]. Эквивалентность этих точек зрения была понята благодаря работам Барнума, Нилла и Нильсена [60] и Барнума, Смолина и Терала [73]. Пропускная способность для некоторых каналов (прежде всего для квантового канала стирания) установлена Беннетом, Дивинченцо и Смолиным [41], а нижняя граница для пропускной способности деполяризующего канала с использованием вырожденных квантовых кодов получена Шором и Смолиным [368] и уточнена Дивинченцо, Шором и Смолиным [133]. Зурек [437], Мильбурн [284] и Ллойд [254] анализировали примеры квантовых демонов Максвелла, хотя и не в контексте исправления ошибок. Анализ, проведенный здесь, основан на работе Нильсена, Кейва, Шумахера и Барнума [302]. Этой же точки зрения придерживался и Ведрал [400] при установлении пределов для очищения запутанности. Квантовая граница Синглтона появилась благодаря Ниллу и Лафламу [216]. Приведенным здесь доказательством мы обязаны Прескиллу [329].

Изучение запутанности, превратилось в большую область исследования; по этому вопросу существует настолько большое число статей, что мы не имеем возможности даже их перечислить. Напоминаем, что можно посмотреть архив quant-ph в Интернете <http://arXiv.org/>. Условия для преобразования запутанности, основанные на мажоризации (теорема 12.15), появились благодаря Нильсену [304]. Теорема 12.13 принадлежит Ульману [391, 392, 393]. Утверждение 12.14 возникло благодаря Ло и Попеску [262]. Катализ запутанности открыт Джонатаном и Пленио [205]. Книга Маршалла и Олкина [290] представляет собой всеобъемлющее введение в мажоризацию, включая доказательство теоремы Биркгоффа. Пределы для разбавления и очищения запу-

таннысти установлены Беннетом, Бернштейном, Попеску и Шумахером [31]. Протоколы очищения запутанности для смешанных состояний разработали Беннет, Брассар, Попеску, Шумахер, Смолин и Вутерс [30], а связь с исправлением квантовых ошибок, установленная в работе Беннета, Дивинченцо, Смолина и Вутерса [42], стимулировала множество дальнейших исследований. Пример, проиллюстрированный на рис. 12.11, упомянут в неопубликованной работе Готтесмана и Нильсена. Мы отметим здесь еще несколько представляющих особый интерес статей по запутанности, которые могут послужить отправной точкой при изучении литературы по этому вопросу; к сожалению, множество статей, которые следовало бы упомянуть, в результате оказались пропущены. В серии статей членов семьи Городецких (Михаил, Павел и Ричард Городецкие) тщательно исследованы свойства запутанности; особо следует отметить [178, 179, 180, 181, 182]. Большой интерес также представляют статьи Ведрала и Пленио [406] и Видала [401].

Чтобы составить общее представление о квантовой криптографии на непрофессиональном уровне, обратитесь к статье Беннета, Брассара и Экерта в *Scientific American* [27]. Идеи квантовой криптографии впервые предложены Визнером в конце 60-х гг. XX в. К сожалению, эти идеи не были опубликованы, и о них стало известно только в начале 80-х гг. Визнер предложил использовать (запутанные) квантовые состояния при условии, что их можно долго хранить, для создания денег, которые нельзя подделать [415, 416]. В дальнейшем Беннет разработал еще несколько протоколов, один из которых впервые экспериментально реализовали Беннет, Бессет, Брассар, Сальвайл и Смолин [20], что представляет (в принципе) исторический интерес, поскольку информация в эксперименте передавалась меньше, чем на метр, и, более того, подслушиванию способствовало громкое гудение, которое производил источник питания всякий раз, когда посылали «единицу»! Концепцию усиления конфиденциальности впервые предложили Беннет, Брассар и Робер [32]. По поводу протоколов согласования информации обратитесь к работам [20] и [71]. Беннет, Брассар, Крепо и Морэ [26] сформулировали и доказали в общем виде теорему 12.16 с точки зрения исследования усиления конфиденциальности. Заметим, что информация, раскрытая во время согласования, оказывает большое влияние на порог усиления конфиденциальности, что и отражено в теореме 12.17, доказанной Кошеном и Морэ [93]. Усиление конфиденциальности нашло применение при классической генерации ключа с использованием удаленных коррелированных случайных источников, таких как свет звезды, зарегистрированный спутниками [276]. Протокол четырех состояний, известный как BB84, назван по фамилиям его авторов, Беннета и Брассара [19], и аналогично протокол B92 двух состояний назван по фамилии Беннета [49]. ЭПР протокол разработал Экерт [141]. Доказательством границы случайной выборки в упр. 12.27 мы обязаны Амбайнису. Ограничения, а также безопасность квантовой криптографии подробно обсуждались во многих публикациях. Обратитесь, например, к работам Барнета и Феникса [65], Брассара [69], Экерта, Хатнера, Пальма и Переса [138], а также [322]. Связь между когерентной информацией и конфиденциальностью установили Шумахер и Вестморланд [381]. Опубликовано много

статей по вопросам экспериментальной реализации квантовых криптографических систем. Чтобы получить представление об этом, рекомендуем обратиться к работе Хьюза, Альда, Лютера, Моргана и Шауэра [174]; Мюллер, Збинден и Гизин [300] продемонстрировали квантовую криптографию под Женевским озером. Эксперимент, описанный во вставке 12.7, провели Бетун и Риск [67, 68] из IBM, и мы благодарим их за предоставленную схему экспериментальной установки. Выполнено большое число доказательств надежности различных протоколов распределения квантовых ключей при разных условиях. Следует особо отметить (исчерпывающее, но довольно сложное) доказательство надежности протокола BB84, сделанное Майерсом [278]. Бихам, Бойер, Брассар, ван де Грааф и Мор также обсудили атаки на протокол BB84 [21]. Более простое доказательство с использованием ЭПР состояний в предположении безошибочных квантовых вычислений дано Ло и Чу [237]; это протокол, с которого мы начали подразд. 12.6.5. Ло [259] упростил его, предложив начинать с измерения скорости возникновения ошибок, а затем уже передавать данные о ключе. Еще более простым (и красивым!) доказательством в подразд. 12.6.5 мы обязаны Шору и Прескиллу [366], которые также дали 11% оценку, упомянутую в подразд. 12.6.5. Наше представление этого доказательства также сильно выиграло после обсуждения его с Готтесманом.

Приложение 1

НЕКОТОРЫЕ СВЕДЕНИЯ ИЗ ТЕОРИИ ВЕРОЯТНОСТЕЙ

Приложение содержит небольшое количество элементарных определений и фактов из теории вероятностей. Предполагается, что читатель в какой-то мере знаком с этим материалом. Если же ему не известно ни одно из приводимых ниже утверждений, то следует потратить время на то, чтобы доказать их самостоятельно (следите за встречающимися в тексте упражнениями).

Основное понятие теории вероятностей — *случайная переменная*. Случайная переменная X может принимать значение x из некоторого набора с вероятностью $p(X = x)$. Мы используем прописные буквы для обозначения случайных переменных, а строчные — для значений, которые могут принимать эти переменные. Мы часто используем обозначение $p(x)$ вместо $p(X = x)$, неявно подразумевая выражение « $X = x$ ». В этой книге мы имеем дело только со случайными переменными, которые могут принимать значения из конечного набора. Иногда удобно рассматривать случайные величины, принимающие векторные значения, например из множества $(i, j) : i = 1, \dots, m_1, j = 1, \dots, m_2$.

Условная вероятность того, что $Y = y$, если известно, что $X = x$, задается формулой

$$p(Y = y | X = x) \equiv \frac{p(X = x, Y = y)}{p(X = x)}, \quad (\text{П1.1})$$

где $p(X = x, Y = y)$ — вероятность того, что $X = x$ и $Y = y$. Когда $p(X = x) = 0$, будем считать, что $p(Y = y | X = x) = 0$. Мы часто используем обозначение $p(y|x)$, неявно подразумевая выражения « $Y = y$ » и « $X = x$ ». Случайные переменные X и Y называются *независимыми*, если $p(X = x, Y = y) = p(X = x)p(Y = y)$ для всех x и y . Обратите внимание, что если X и Y — независимые переменные, то $p(y|x) = p(y)$ для любых x и y .

Формула Байеса связывает условные вероятности для X при заданном Y и для Y при заданном X :

$$p(x|y) = p(y|x) \frac{p(x)}{p(y)}. \quad (\text{П1.2})$$

Вероятность $p(y)$ в этом выражении часто переписывают с использованием обсуждающейся ниже формулы полной вероятности.

Упражнение П1.1. Докажите формулу Байеса.

Одним из наиболее важных и часто используемых результатов теории вероятностей является *формула полной вероятности*. Она утверждает, что если X и Y — две случайные переменные, то вероятности для величины Y могут быть записаны в терминах вероятностей для X и условных вероятностей для Y при заданном X :

$$p(y) = \sum_x p(y|x)p(x), \quad (\text{П1.3})$$

где суммирование ведется по всем значениям x , которые может принимать, переменная X .

Упражнение П1.2. Докажите формулу полной вероятности.

Математическое ожидание, или *среднее случайной переменной*, определяется формулой

$$\mathbf{E}(X) \equiv \sum_x p(x)x, \quad (\text{П1.4})$$

где суммирование ведется по всем значениям x , которые может принимать переменная X .

Упражнение П1.3. Докажите, что существует такое значение $x \geq \mathbf{E}(X)$, для которого $p(x) > 0$.

Упражнение П1.4. Докажите, что $\mathbf{E}(X)$ — линейная функция переменной X .

Упражнение П1.5. Докажите, что для независимых случайных переменных X и Y выполняется равенство $\mathbf{E}(XY) = \mathbf{E}(X)\mathbf{E}(Y)$.

Дисперсия случайной переменной X определяется выражением

$$\text{var}(X) \equiv \mathbf{E}[(X - \mathbf{E}(X))^2] = \mathbf{E}(X^2) - \mathbf{E}(X)^2. \quad (\text{П1.5})$$

Квадратичное отклонение $\Delta(X) \equiv \sqrt{\text{var}(X)}$ — это мера разброса случайной переменной относительно своего среднего значения. *Неравенство Чебышёва* описывает более точно, в каком смысле стандартное отклонение является мерой разброса значений случайной переменной, которые она может принимать. Оно утверждает, что для случайной переменной с ненулевой дисперсией и произвольного $\lambda > 0$ выполняется неравенство

$$p(|X - \mathbf{E}(X)| \geq \lambda\Delta(X)) \leq \frac{1}{\lambda^2}. \quad (\text{П1.6})$$

Другими словами, вероятность того, что случайная величина примет значение, отличающееся от среднего более чем на λ стандартных отклонений, уменьшается при стремлении λ к бесконечности.

Упражнение П1.6. Докажите неравенство Чебышёва.

В основном тексте книги использовано много других утверждений из теории вероятностей, включая *неравенство Чернова*, *неравенство Фано* и *закон больших чисел*.

История и дополнительная литература

Существует много превосходных изданий, посвященных теории вероятностей. Следует выделить книгу Гримметта и Штизакера [173], посвященную основным идеям теории вероятностей и стохастических процессов. Более чистая математическая трактовка дана во введении в современную теорию вероятностей Вильямса [418]; особое внимание здесь уделено красивой теории мартингалов. Наконец, глубоким введением в теорию вероятностей является классический двухтомник Феллера [147, 148].

Приложение 2

ТЕОРИЯ ГРУПП

При изучении квантовых вычислений и квантовой информации в ряде случаев полезно использовать теорию групп. Обобщения алгоритмов нахождения порядка элемента, разложения на множители и нахождения периода (гл. 5) основаны на задаче о скрытой подгруппе; формализм стабилизаторов, использованный при описании исправления квантовых ошибок в гл. 10, базируется на некоторых элементарных понятиях теории групп. В теории чисел, рассматриваемой в Приложении 4, использованы свойства группы Z_n^* . Кроме того, квантовые схемы, к которым мы обращаемся на протяжении всей книги, являются примером применения групп Ли. В данном Приложении приводится обзор основных элементарных фактов из теории групп. Мы вводим много фундаментальных понятий и важных определений, но не пытаемся объяснить все сразу, поскольку теория групп — весьма обширная наука.

П2.1 Основные определения

Группой (G, \cdot) называют непустое множество G с бинарной операцией умножения « \cdot », обладающей следующими свойствами: замкнутость ($g_1 \cdot g_2 \in G$ для любых $g_1, g_2 \in G$); ассоциативность $((g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$ для любых $g_1, g_2, g_3 \in G$); существование единицы (есть такой элемент $e \in G$, что для любого $g \in G$ выполняется равенство $g \cdot e = e \cdot g = g$); существование обратного (для любого $g \in G$ имеется такой элемент $g^{-1} \in G$, что $g \cdot g^{-1} = g^{-1} \cdot g = e$). Мы часто опускаем знак « \cdot » и вместо $g_1 \cdot g_2$ пишем просто g_1g_2 , а также говорим о группе G без явного указания на операцию умножения этой группы, но эта операция обязательно должна быть определена.

Группа G называется *конечной*, если число ее элементов конечно. Порядком конечной группы G называется число ее элементов (обозначается $|G|$). Группа G называется *абелевой*, если $g_1g_2 = g_2g_1$ для любых $g_1, g_2 \in G$. Простым примером конечной абелевой группы является аддитивная группа Z_n остатков по модулю n с операцией «умножения», задаваемой обычным сложением по модулю n . Легко проверить, что эта операция удовлетворяет аксиомам замкнутости и ассоциативности; существует «единичный» элемент (0) , так как $x + 0 = x \pmod{n}$ для любого x ; для каждого элемента $x \in G$ существует обратный, равный $n - x$, поскольку $x + (n - x) = 0 \pmod{n}$.

Порядком элемента $g \in G$ называется наименьшее положительное целое число r , для которого g^r (т. е. r раз умноженный сам на себя элемент g) равно единичному элементу e .

Подгруппой H группы G называют подмножество множества G , которое само образует группу с той же самой операцией умножения, которая вводилась в G .

Теорема П2.1 (теорема Лагранжа). Если H — подгруппа конечной группы G , то $|H|$ делит $|G|$.

Упражнение П2.1. Докажите, что для любого элемента g конечной группы существует такое положительное целое число r , что $g^r = e$. Другими словами, для любого элемента такой группы можно определить его порядок.

Упражнение П2.2. Докажите теорему Лагранжа.

Упражнение П2.3. Покажите, что порядок элемента $g \in G$ делит $|G|$.

Элемент g_1 сопряжен с элементом g_2 , если существует такой элемент $h \in G$, что $g_2 = hg_1h^{-1}$ (очевидно, что в этом случае и элемент g_2 сопряжен с элементом g_1). Подгруппа H группы G называется нормальной, если $g^{-1}Hg = H$ для любого $g \in G$. Классом сопряженных элементов G_x элемента x в группе G называется множество $G_x \equiv \{g^{-1}xg \mid g \in G\}$.

Упражнение П2.4. Покажите, что если $y \in G_x$, то $G_y = G_x$.

Упражнение П2.5. Покажите, что если x — элемент абелевой группы G , то $G_x = \{x\}$.

Интересным примером неабелевой группы является группа Паули на n кубитах. Для одного кубита группа Паули будет состоять из матриц Паули, умножаемых на множители вида $\pm 1, \pm i$:

$$G_1 \equiv \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}. \quad (\text{П2.1})$$

Это множество матриц образует группу относительно операции перемножения матриц. Может вызвать удивление тот факт, что множители ± 1 и $\pm i$ не исключены. Причина заключается в том, что только в этом случае множество G_1 будет замкнуто относительно умножения, а следовательно, будет действительно образовывать группу. Общая группа Паули на n кубитах, по определению, состоит из всех n -кратных тензорных произведений матриц Паули, причем по-прежнему следует использовать все множители вида $\pm 1, \pm i$.

П2.1.1 Образующие

Изучение группы часто сильно упрощается за счет использования множества образующих для нее. Говорят, что набор элементов g_1, \dots, g_l группы G порождает эту группу, если любой элемент G может быть представлен в виде произведения (возможно, повторяющихся) элементов из списка g_1, \dots, g_l ; в таком случае используем обозначение $G = \langle g_1, \dots, g_l \rangle$. Например, $G_1 = \langle X, Z, iI \rangle$, поскольку любой элемент группы G может быть представлен в виде произведения матриц X , Z и iI . В то же время $\langle X \rangle = \{I, X\}$ — мы получили подгруппу группы G_1 , не совпадающую со всей группой, поскольку не все элементы из G_1 могут быть представлены в виде степени матрицы X . Обозначение $\langle \dots \rangle$, которое мы используем для образующих групп, в принципе можно спутать с обозначением для наблюдаемых средних значений, введенным в подразд. 2.2.5. Тем не менее на практике из контекста всегда понятно, о каком из двух обозначений идет речь.

Большое преимущество от использования образующих для описания групп заключается в том, что они предоставляют очень компактные средства описания. Пусть группа G имеет мощность $|G|$. Тогда легко показать, что существует множество из $\log(|G|)$ образующих, порождающих группу G . Действительно, предположим, что g_1, \dots, g_l — набор элементов в группе G и g не входит в группу $\langle g_1, \dots, g_l \rangle$. Пусть $f \in \langle g_1, \dots, g_l \rangle$. Тогда $fg \notin \langle g_1, \dots, g_l \rangle$, поскольку в противном случае выполнялось бы условие $g = f^{-1}fg \in \langle g_1, \dots, g_l \rangle$, что противоречит сделанному предположению. Таким образом, для любого элемента $f \in \langle g_1, \dots, g_l \rangle$ существует элемент fg , входящий в группу $\langle g_1, \dots, g_l, g \rangle$, но не содержащийся в $\langle g_1, \dots, g_l \rangle$. Поэтому добавление образующей g к $\langle g_1, \dots, g_l \rangle$, по крайней мере, удваивает размер порождаемой группы, отсюда следует, что группу G можно задать набором образующих, содержащим не более $\log(|G|)$ элементов.

П2.1.2 Циклические группы

Группа G называется *циклической*, если в ней существует такой элемент a , что любой элемент $g \in G$ может быть представлен в виде a^n с некоторым целым n ; при этом элемент a называется образующей группы G и $G = \langle a \rangle$. *Циклической подгруппой* H , порожденной элементом $g \in G$, называется группа $\{e, g, g^2, \dots, g^{r-1}\}$, где r — порядок элемента g . Другими словами, $H = \langle g \rangle$.

Упражнение П2.6. Покажите, что любая группа, порядок которой равен простому числу, является циклической.

Упражнение П2.7. Покажите, что любая подгруппа циклической группы является циклической.

Упражнение П2.8. Покажите, что если элемент $g \in G$ имеет конечный порядок, то $g^m = g^n$ тогда и только тогда, когда $m = n \pmod r$.

П2.1.3 Смежные классы

Для подгруппы H группы G левым смежным классом, определяемым элементом $g \in G$, называется множество $gH \equiv \{gh \mid h \in H\}$. Правый смежный класс вводится аналогичным образом. Зачастую определять, является ли смежный класс «правым» или «левым», приходится из контекста. В случае такой группы, как \mathbf{Z}_n , когда групповой операцией является операция сложения, принято обозначать смежные классы подгруппы H следующим образом: $g + H$ (для $g \in \mathbf{Z}_n$).

Упражнение П2.9. Смежные классы определяют отношение эквивалентности между элементами. Покажите, что элементы $g_1, g_2 \in G$ принадлежат одному и тому же смежному классу подгруппы H в G тогда и только тогда, когда существует такой элемент $h \in H$, что $g_2 = g_1h$.

Упражнение П2.10. Какое количество смежных классов подгруппы H содержится в группе G ?

П2.2 Представления

Пусть M_n — множество комплексных матриц размера $n \times n$. Матричная группа — это множество матриц в M_n , которое удовлетворяет свойствам групп относительно операции перемножения матриц. Обозначим единичный элемент в таких группах через I . *Представление* ρ группы G определяется как функция, которая отображает G в матричную группу, сохраняя операцию умножения в группе. В частности, элемент $g \in G$ так отображается в матрицу $\rho(g) \in M_n$, что из равенства $g_1 g_2 = g_3$ следует, что $\rho(g_1)\rho(g_2) = \rho(g_3)$. Если несколько элементов могут отображаться в один, то такое отображение называют *гомоморфизмом*; если же разные элементы переходят в разные, то такое отображение называется *изоморфизмом*. Представление ρ , отображающее элементы группы во множество матриц M_n , имеет *размерность* $d_\rho = n$. Определенные нами представления также называют *матричными*; существуют представления более общего вида, однако для наших целей они не потребуются. В оставшейся части данного приложения мы будем иметь дело только с группами конечного размера.

П2.2.1 Эквивалентность и приводимость

С представлениями связаны два очень важных понятия: *эквивалентность* и *приводимость*. *Характером* группы матриц $G \in M_n$ называют функцию, определенную на элементах группы следующим образом: $\chi(g) = \text{tr}(g)$ (здесь $g \in G$, а $\text{tr}(\cdot)$ — обычный оператор взятия следа от данной матрицы). Отметим следующие свойства характера: 1) $\chi(I) = n$; 2) $|\chi(g)| \leq n$; 3) если $|\chi(g)| = n$, то $g = e^{i\theta} I$; 4) χ имеет одно и то же значение для всех представителей одного и того же класса сопряженных элементов группы G ; 5) $\chi(g^{-1}) = \chi^*(g)$; 6) $\chi(g)$ является алгебраическим числом. Две группы матриц называются *эквивалентными*, если они изоморфны, а элементы, переходящие друг в друга при изоморфизме, имеют одинаковые характеристики.

Упражнение П2.11 (характеры). Докажите шесть приведенных выше свойств характеров.

Упражнение П2.12 (унитарные группы матриц). Унитарная группа матриц состоит только из унитарных матриц (т. е. матриц, удовлетворяющих условию $U^\dagger U = I$). Покажите, что любая группа матриц эквивалента унитарной группе матриц. Если представление группы состоит только из унитарных матриц, его называют *унитарным*.

Матричную группу G в M_n называют *вполне приводимой*, если она эквивалентна другой матричной группе H , которая имеет блоковую диагональную форму, т. е. все элементы $m \in H$ имеют вид $\text{diag}(m_1, m_2)$ с некоторыми матрицами $m_1 \in M_{n_1}$ и $m_2 \in M_{n_2}$. Если такой эквивалентности не существует, то матричная группа является *неприводимой*. Рассмотрим полезное свойство неприводимых матричных групп.

Лемма П2.2 (лемма Шура). Пусть $G \in M_n$ и $H \in M_k$ — две матричные группы одного порядка, т. е. $|G| = |H|$. Если существует такая матрица S размера $k \times n$, что $Sg_i = h_iS$ для некоторого порядка расположения элементов $g_i \in G$ и $h_i \in H$, то либо S — нулевая матрица, либо $n = k$, а S — квадратная невырожденная матрица.

Упражнение П2.13. Покажите, что любая неприводимая абелева матричная группа является одномерной.

Упражнение П2.14. Докажите, что если ρ — неприводимое представление группы G , то число $|G|/d_\rho$ — целое.

Следующая теорема связывает свойство неприводимости с характерами.

Теорема П2.3. Группа матриц G неприводима тогда и только тогда, когда

$$\frac{1}{|G|} \sum_{g \in G} |\chi(g)|^2 = 1. \quad (\text{П2.2})$$

П2.2.2 Ортогональность

Теорема П2.4 (фундаментальная теорема). Любая группа G имеет ровно r неэквивалентных неприводимых представлений, где r — количество классов сопряженных элементов группы G . Кроме того, если $\rho^p \in M_{d_p}$ и ρ^q — любые два из этих представлений, то элементы матриц удовлетворяют соотношениям ортогональности

$$\sum_{g \in G} [\rho^p(g)]_{ij}^{-1} [\rho^q(g)]_{kl} = \frac{|G|}{d_p} \delta_{il} \delta_{jk} \delta_{pq}, \quad (\text{П2.3})$$

где δ_{pq} равно единице, если $\rho^p = \rho^q$, и нулю — в противном случае.

Упражнение П2.15. Используя фундаментальную теорему, докажите, что характеристики ортогональны, т. е.

$$\sum_{i=1}^r r_i (\chi_i^p)^* \chi_i^q = |G| \delta_{pq} \quad \text{и} \quad \sum_{p=1}^r (\chi_i^p)^* \chi_j^p = \frac{|G|}{r_i} \delta_{ij}, \quad (\text{П2.4})$$

где величины p, q и δ_{pq} имеют тот же смысл, что и в теореме, а χ_i^p — значение, которое принимает характер p -го неприводимого представления на i -м классе сопряженных элементов группы G ; r_i — мощность i -го класса сопряженных элементов.

Упражнение П2.16. Обозначим через S_3 группу всех перестановок трех элементов. Упорядочим их следующим образом: первый элемент отображает 123 в 123, второй — в 231, третий — в 312, четвертый — в 213, пятый — в 132, шестой — в 321. Покажите, что существуют два одномерных неприводимых представления группы S_3 , одно из которых — тривиальное, а второе имеет вид 1, 1, 1, -1, -1, -1 (порядок чисел соответствует приведенному выше порядку элементов группы S_3). Покажите также, что существует двумерное неприводимое представление, состоящее из матриц

$$\begin{aligned} & \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \frac{1}{2} \begin{bmatrix} -1 & -\sqrt{3} \\ \sqrt{3} & -1 \end{bmatrix}, \quad \frac{1}{2} \begin{bmatrix} -1 & \sqrt{3} \\ -\sqrt{3} & -1 \end{bmatrix}, \\ & \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \frac{1}{2} \begin{bmatrix} 1 & \sqrt{3} \\ \sqrt{3} & -1 \end{bmatrix}, \quad \frac{1}{2} \begin{bmatrix} 1 & -\sqrt{3} \\ -\sqrt{3} & -1 \end{bmatrix}. \end{aligned} \quad (\text{П2.5})$$

Проверьте, что указанные выше двумерное и нетривиальное одномерное представления ортогональны.

П2.2.3 Регулярное представление

Число 1 является допустимым одномерным матричным представлением для любой группы, — оно тривиальное. Представление относят к *точным*, если группа матриц представления изоморфна исходной группе. *Регулярным* называют точное представление, построенное по следующим правилам. Пусть $\vec{v} = [g_1, g_2, \dots, g_{|G|}]^T$ — вектор-столбец элементов из группы G . Умножение всех элементов из \vec{v} на элемент $g \in G$ приводит к перестановке этих элементов, которая может быть представлена матрицей размера $|G| \times |G|$, умножаемой на вектор \vec{v} по обычным правилам умножения матрицы на вектор-столбец. Получаемые $|G|$ таких матриц, соответствующие различным перестановкам, образуют точное представление группы G (с операцией умножения матриц).

Упражнение П2.17. Докажите, что регулярное представление действительно является точным.

Упражнение П2.18. Покажите, что характер регулярного представления равен нулю, за исключением представления единичного элемента, для которого $\chi(I) = |G|$.

Разложения произвольных представлений в прямые суммы неприводимых представлений удовлетворяют следующей теореме.

Теорема П2.5. Если ρ — произвольное представление группы G с характером χ , а ρ^p — неэквивалентные неприводимые представления G с характерами χ^p , то $\rho = \bigoplus_p c_p \rho^p$, где знак « \oplus » обозначает прямую сумму, а c_p — числа, определяемые формулой

$$c_p = \frac{1}{|G|} \sum_{i=1}^r r_i (\chi_i^p)^* \chi_i. \quad (\text{П2.6})$$

Упражнение П2.19. Покажите (с использованием теоремы П2.5), что регулярное представление содержит по d_{ρ^p} экземпляров каждого неприводимого представления ρ^p . Другими словами, если R обозначает регулярное представление, а через \hat{G} — множество всех неэквивалентных неприводимых представлений, то

$$\chi_i^R = \sum_{\rho \in \hat{G}} d_{\rho} \chi_i^{\rho}. \quad (\text{П2.7})$$

Упражнение П2.20. Характер регулярного представления равен нулю, кроме того класса сопряженных элементов i , который содержит единичный элемент e группы G . Покажите, что

$$\sum_{\rho \in \hat{G}} d_\rho \chi^\rho(g) = N \delta_{ge}. \quad (\text{П2.8})$$

Упражнение П2.21. Докажите справедливость равенства $\sum_{\rho \in \hat{G}} d_\rho^2 = |G|$.

П2.2.4 Преобразования Фурье

Пусть G — конечная группа порядка N , f — функция, отображающая элементы группы во множество комплексных чисел. Для неприводимого представления ρ группы G (размерность которого равна d_ρ) определим преобразование Фурье \hat{f} функции f следующим образом:

$$\hat{f}(\rho) \equiv \sqrt{\frac{d_\rho}{N}} \sum_{g \in G} f(g) \rho(g). \quad (\text{П2.9})$$

Обратите внимание, что ρ — матричное представление, $\hat{f}(\rho)$ отображает матрицы в матрицы. Пусть \hat{G} — полный набор неэквивалентных неприводимых представлений группы G . Определим обратное преобразование Фурье от \hat{f} следующим равенством:

$$f(g) = \frac{1}{\sqrt{N}} \sum_{\rho \in \hat{G}} \sqrt{d_\rho} \operatorname{tr}(\hat{f}(\rho) \rho(g^{-1})). \quad (\text{П2.10})$$

Поскольку $\sum_\rho d_\rho^2 = N$, обе функции f и \hat{f} могут быть представлены в виде n -мерных векторов над комплексным пространством. Коэффициенты в двух предыдущих уравнениях были выбраны таким образом, что если \hat{G} состоит из унитарных представлений, то преобразования Фурье являются унитарными.

Приведенные выше определения легко понять, если подставить выражение (П2.9) в (П2.10):

$$f(g) = \frac{1}{N} \sum_{\rho \in \hat{G}} \sum_{g' \in G} d_\rho f(g') \operatorname{tr}(\rho(g') \rho(g^{-1})) = \quad (\text{П2.11})$$

$$= \frac{1}{N} \sum_{\rho \in \hat{G}} \sum_{g' \in G} d_\rho f(g') \operatorname{tr}(\rho(g' g^{-1})) = \quad (\text{П2.12})$$

$$= \frac{1}{N} \sum_{g' \in G} f(g') \sum_{\rho \in \hat{G}} d_\rho \chi^\rho(g' g^{-1}). \quad (\text{П2.13})$$

С использованием уравнения (П2.8) можно упростить (П2.13) до следующего вида:

$$f(g) = \sum_{g' \in G} f(g') \delta_{g'g}, \quad (\text{П2.14})$$

что и требовалось.

Упражнение П2.22. Подставьте выражение (П2.10) в (П2.9) и убедитесь, что действительно получается функция $\hat{f}(\rho)$.

Упражнение П2.23. Рассмотрим представления абелевой группы G остатков от деления на N , в которой групповой операцией является сложение по модулю N . По определению, $\rho_h(g) = \exp[-2\pi i gh/N]$ для h -го представления g , $g \in [0, N - 1]$. Это представление является одномерным, поэтому $d_\rho = 1$. Покажите, что уравнения (П2.9), (П2.10) в данном случае выглядят следующим образом:

$$\hat{f}(h) = \frac{1}{\sqrt{N}} \sum_{g=0}^{N-1} f(g) e^{-2\pi i gh/N}, \quad f(h) = \frac{1}{\sqrt{N}} \sum_{g=0}^{N-1} \hat{f}(g) e^{2\pi i gh/N}. \quad (\text{П2.15})$$

Упражнение П2.24. Постройте (с использованием результатов упражнения П2.16) преобразование Фурье на группе S_3 и запишите его в виде унитарных матриц размера 6×6 .

История и дополнительная литература

По теории групп написано много выдающихся книг, и почти все учебники по алгебре содержат раздел, посвященный этой области математики.¹ В данном приложении в значительной мере использованы обозначения из книги Ломонта [260]. Стандартным введением в теорию групп для физиков является учебник Хаммермеша [176]. Преобразования Фурье на произвольных группах не являются широко распространенными. Имеется хорошая статья Диакониса и Рокмора об эффективном выполнении преобразований Фурье на группах [129]; многие их результаты обсуждаются в книге Фэсслера и Стифела [154]. Быстрое преобразование Фурье на группах независимо открыли Бет [50] и Клаузен [90].

¹ На русском языке см., например, Винберг Э. Б. Алгебра М : Фрактал, 1999 — Прим. ред

Приложение 3

ТЕОРЕМА СОЛОВЕЯ–КИТАЕВА

В гл. 4 было показано, что произвольная унитарная операция U может быть реализована на квантовом компьютере с использованием схемы, состоящей из однокубитовых элементов и элементов СНОТ. Такое утверждение об универсальности очень важно, поскольку гарантирует эквивалентность различных моделей квантовых вычислений. Например, это позволяет программисту создавать квантовые схемы с элементами, имеющими четыре входных и выходных кубита, будучи уверенным, что такие схемы могут быть смоделированы с помощью фиксированного числа однокубитовых элементов и элементов СНОТ.

Недостатком универсальности набора из элементов СНОТ и произвольных унитарных элементов на одном кубите является то, что операторы на одном кубите образуют континuum, в то время как описанные в гл. 10 устойчивые к ошибкам методы квантовых вычислений работают только для конечного набора элементов. Однако в гл. 4 мы видели, что любой элемент на одном кубите может быть аппроксимирован с произвольной точностью с использованием конечного набора таких элементов, как СНОТ, элемент Адамара H , фазовый элемент S и $(\pi/8)$ -элемент. Мы также привели эвристическое доказательство того, что для приближенной реализации выбранного элемента на одном кубите с точностью ϵ требуется лишь $\Theta(1/\epsilon)$ элементов, выбранных из конечного множества. Далее, в гл. 10 было показано, что СНОТ, элемент Адамара, фазовый элемент и $(\pi/8)$ -элемент могут быть реализованы устойчивыми к ошибкам.

В данном приложении будет показано, что можно достигнуть более быстрой сходимости, чем $\Theta(1/\epsilon)$. Теорема Соловея–Китаева показывает, что для любого элемента U на одном кубите и $\epsilon > 0$ можно приблизить U с точностью ϵ с использованием $\Theta(\log^c(1/\epsilon))$ элементов из фиксированного конечного набора, где c — малая константа, примерно равная двойке. Наилучшее возможное значение величины c к моменту написания книги неизвестно, поэтому мы приведем доказательство теоремы Соловея–Китаева с величиной c , примерно равной 4, а в задачах, предлагаемых в конце приложения, дадим набросок метода, с помощью которого можно приблизить число c к двойке. Мы также докажем, что c не может быть меньше единицы; определение наилучшего возможного значения c (лежащего, таким образом, между единицей и двойкой) остается нерешенной задачей.

Чтобы оценить важность теоремы Соловея–Китаева, представьте себе, что программист создает алгоритм для квантового компьютера, использующий $f(n)$ элементов. Предположим, что в построенном алгоритме помимо СНОТ, элементов Адамара, фазовых элементов и $(\pi/8)$ -элементов применяется множество других элементов. Какое количество элементов потребуется, чтобы реализовать алгоритм устойчивым к ошибкам образом? Если допустимая ошибка всего алгоритма равна ϵ , то каждый отдельный элемент должен быть ал-

проксимирован с точностью $\varepsilon/f(n)$. Согласно эвристическому доказательству в гл. 4, для реализации устойчивого к ошибкам варианта элемента, используемого в алгоритме, потребуется $\Theta(f(n)/\varepsilon)$ элементов. Таким образом, всего для алгоритма потребуется $\Theta(f^2(n)/\varepsilon)$ элементов, т. е. число элементов для алгоритма растет с полиномиальной скоростью. С учетом теоремы Соловея–Китаева каждый элемент может быть смоделирован с помощью $O(\log^c(f(n)/\varepsilon))$ элементов из устойчивого к ошибкам набора, а полное количество элементов для устойчивого к ошибкам алгоритма должно иметь порядок $O(f(n) \log^c(f(n)/\varepsilon))$, т. е. быть только полилогарифмически большим, чем в исходном алгоритме. Для многих задач такое полилогарифмическое усложнение вполне приемлемо, тогда как полиномиальный рост, присутствующий в эвристическом доказательстве в гл. 4, гораздо менее желателен.

Чтобы сформулировать теорему Соловея–Китаева более точно, следует ввести несколько обозначений. Напомним, что $SU(2)$ — это множество всех действующих на одиночный кубит унитарных матриц с равным единице детерминантам. Мы сфокусируем внимание на $SU(2)$, поскольку все элементы на одном кубите могут быть записаны в виде произведения элемента из $SU(2)$ на несущественный общий фазовый множитель. Пусть \mathcal{G} — конечный набор элементов из $SU(2)$; \mathcal{G} играет роль конечного набора базисных элементов, который использует программист для имитации всех остальных элементов при создании квантового компьютера. Для определенности будем считать, что \mathcal{G} содержит устойчивое к ошибкам множество $\{H, S, T\}$, причем мы провели умножение на подходящую общую фазу, чтобы обеспечить равенство детерминантов единице. Для удобства будем считать, что \mathcal{G} содержит элементы, обратные входящим в него элементам, т. е. если $U \in \mathcal{G}$, то $U^\dagger \in \mathcal{G}$. В случае множества, устойчивого к ошибкам, это означает добавление к множеству элементов $S^\dagger = S^3$ и $T^\dagger = T^7$, которые, по удачному стечению обстоятельств, выражаются через уже входящие в это множество элементы. Словом *длиной* l из \mathcal{G} называется произведение $g_1 g_2 \dots g_l \in SU(2)$, где $g_i \in \mathcal{G}$ для любого i . Множество всех слов длиной не больше l обозначим \mathcal{G}_l , а множество всех слов конечной длины через $\langle \mathcal{G} \rangle$.

Нам понадобится понятие *расстояния* для количественной характеристики того, что мы понимаем под выражением «приближение к унитарной матрице». Конкретный вид метрики не так уж важен. Для наших целей удобно использовать *следовую метрику*, описанную в гл. 9: $D(U, V) \equiv \text{tr}|U - V|$, где $|X| \equiv \sqrt{X^\dagger X}$ — положительный квадратный корень из $X^\dagger X$. На самом деле, данное определение отличается множителем 2 от определения в гл. 9; причина для использования в данном приложении другой нормировки заключается в том, что, как будет показано ниже, это облегчает геометрическую интерпретацию доказательства теоремы Соловея–Китаева (также полезно представлять себе элементы множества $SU(2)$ как точки в пространстве). Подмножество S во множестве $SU(2)$ называется *плотным* в $SU(2)$, если для любого элемента $U \in SU(2)$ и $\varepsilon > 0$ существует такой элемент $s \in S$, что $D(s, U) < \varepsilon$. Предположим, S и W — подмножества в $SU(2)$. Тогда говорят, что S образует ε -сетью в W (где $\varepsilon > 0$), если любая точка из W находится на расстоянии

не больше ε от некоторой точки из S . Нас интересует, насколько быстро \mathcal{G}_l «заполняет» $SU(2)$ при возрастании l . Другими словами, для сколь малого ε множество \mathcal{G}_l образует ε -сеть в $SU(2)$? Теорема Соловея–Китаева гласит, что ε уменьшается с ростом l очень быстро.

Упражнение П3.1. В гл. 4 было введено понятие расстояния $E(U, V) = \max_{|\psi\rangle} \|(U - V)|\psi\rangle\|$, где максимум берется по всем чистым состояниям $|\psi\rangle$. Покажите, что когда U и V являются поворотами кубита, $U = R_m(\theta)$ и $V = R_n(\varphi)$, то выполняется равенство $D(U, V) = 2E(U, V)$, т. е. неважно, используем ли мы в теореме Соловея–Китаева расстояние $E(\cdot, \cdot)$ или следовую метрику.

Теорема П3.1 (Соловея–Китаева). Пусть \mathcal{G} — конечное множество элементов из $SU(2)$, содержащее обратные ко всем своим элементам, а множество $\langle \mathcal{G} \rangle$ плотно в $SU(2)$. Пусть задано число $\varepsilon > 0$. Тогда множество \mathcal{G}_l является ε -сетью в $SU(2)$ при $l = O(\log^c(1/\varepsilon))$, где $c \approx 4$.

Как отмечалось выше, наилучшее возможное значение c немного меньше 4, однако нам удобней привести доказательство для этого частного случая. В задаче П3.1 мы объясним, как можно модифицировать доказательство, чтобы использовать меньшие значения c . Первая часть доказательства состоит в демонстрации того, что точки множества \mathcal{G}_l образуют довольно плотное множество в окрестности единичной матрицы I при увеличении l (это утверждение содержится в следующей лемме). Чтобы сформулировать лемму, обозначим через S_ε множество всех таких точек U в $SU(2)$, что $D(U, I) < \varepsilon$.

Лемма П3.2. Пусть \mathcal{G} — конечное множество элементов из $SU(2)$, содержащее обратные ко всем своим элементам и такое, что множество $\langle \mathcal{G} \rangle$ плотно в $SU(2)$. Тогда существует такая универсальная константа ε_0 , не зависящая от \mathcal{G} , что для любого $\varepsilon \leq \varepsilon_0$ выполняется следующее утверждение: если \mathcal{G}_l — ε^2 -сеть для S_ε , то \mathcal{G}_{5l} является $C\varepsilon^3$ -сетью для $S_{\sqrt{C}\varepsilon^{3/2}}$, где C — константа.

Приведем краткое доказательство леммы П3.2, однако сначала посмотрим, как из нее следует теорема Соловея–Китаева. Доказательство состоит из двух шагов. Первый заключается в итеративном применении леммы П3.2, что позволит показать, что окрестность начала координат быстро заполняется с увеличением длины слова l . Поскольку множество $\langle \mathcal{G} \rangle$ плотно в $SU(2)$, можно найти такое l_0 , что множество \mathcal{G}_{l_0} является ε_0^2 -сетью для $SU(2)$, а следовательно и для S_{ε_0} . Применение леммы П3.2 при $\varepsilon = \varepsilon_0$ и $l = l_0$ демонстрирует, что множество \mathcal{G}_{5l_0} является $C\varepsilon_0^3$ -сетью для $S_{\sqrt{C}\varepsilon_0^{3/2}}$. Повторное применение леммы П3.2 при $\varepsilon = \sqrt{C}\varepsilon_0^{3/2}$ и $l = 5l_0$ показывает, что множество $\mathcal{G}_{5^2l_0}$ есть $C(\sqrt{C}\varepsilon_0^{3/2})^3$ -сеть для $S_{\sqrt{C}(\sqrt{C}\varepsilon_0^{3/2})^{3/2}}$. Повторив процесс k раз, мы обнаружим, что множество $\mathcal{G}_{5^k l_0}$ является $\varepsilon(k)^2$ -сетью для $S_{\varepsilon(k)}$, где

$$\varepsilon(k) = \frac{(C\varepsilon_0)^{(3/2)^k}}{C}. \quad (\text{П3.1})$$

Без ограничения общности можно считать, что число ε_0 было выбрано таким образом, что $C\varepsilon_0 < 1$, а следовательно, $\varepsilon(k)$ очень быстро стремится к нулю при росте k . Также полезно отметить, что если ε_0 выбрано достаточно малым, то $\varepsilon(k)^2 < \varepsilon(k+1)$.

Перейдем ко второму шагу. Выберем произвольный элемент U из $SU(2)$ и, используя идею переноса, проиллюстрированную на рис. ПЗ.1, аппроксимируем U с помощью элементов из \mathcal{G} . Пусть $U_0 \in \mathcal{G}_{l_0}$ есть $\varepsilon(0)^2$ -приближение к U . Теперь определим V таким образом, что $VU_0 = U$, т. е. $V \equiv UU_0^\dagger$. Следовательно, $D(V, I) = \text{tr}|V - I| = \text{tr}|(U - U_0)U_0^\dagger| = \text{tr}|U - U_0| < \varepsilon(0)^2 < \varepsilon(1)$. С помощью обсуждавшегося выше итерационного применения леммы ПЗ.2 можно найти элемент $U_1 \in \mathcal{G}_{5l_0}$, который является $\varepsilon(1)^2$ -приближением к V . Отсюда следует, что U_1U_0 есть $\varepsilon(1)^2$ -приближение к U . Теперь определим V' так, что $V'U_1U_0 = U$, т. е. $V' \equiv UU_0^\dagger U_1^\dagger$. Тогда $D(V', I) = \text{tr}|V' - I| = \text{tr}|(U - U_1U_0)U_0^\dagger U_1^\dagger| = \text{tr}|U - U_1U_0| < \varepsilon(1)^2 < \varepsilon(2)$. Из итерационного применения леммы ПЗ.2 следует, что можно найти такое $U_2 \in \mathcal{G}_{5^2 l_0}$, которое является $\varepsilon(2)^2$ -приближением к V' , а следовательно, $U_2U_1U_0$ – это $\varepsilon(2)^2$ -приближение к U . Продолжая действовать подобным путем, можно построить такой элемент $U_k \in \mathcal{G}_{5^k l_0}$, что $U_kU_{k-1}\dots U_0$ есть $\varepsilon(k)^2$ -приближение к U .

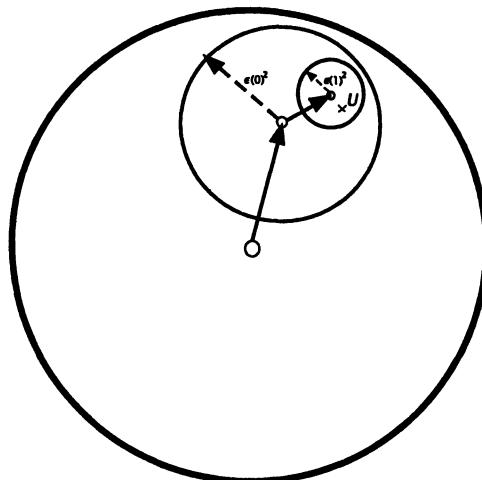


Рис. ПЗ.1. Шаг переноса, применяемый в доказательстве теоремы Соловея–Китаева. Чтобы приблизить произвольный элемент, в начале нужно построить приближение с точностью $\varepsilon(0)^2$ с использованием l_0 элементов из \mathcal{G} . Потом следует улучшить приближение, добавив $5l_0$ дополнительных элементов, чтобы достичь точность лучше $\varepsilon(1)^2$; и затем продолжать дальше этот быстро сходящийся к U процесс

Таким образом, для приближения любого унитарного элемента U с точностью $\varepsilon(k)^2$ можно использовать последовательность из $l_0 + 5l_0 + \dots + 5^k l_0 < \frac{5}{4}5^k l_0$ элементов. Чтобы построить приближение с некоторой требуемой точностью ε , необходимо выбрать такое k , что

$$\varepsilon(k)^2 < \varepsilon. \quad (\text{ПЗ.2})$$

Подставляя сюда формулу (ПЗ.1) можно получить следующее неравенство:

$$\left(\frac{3}{2}\right)^k < \frac{\log(1/C^2\varepsilon)}{2\log(1/C\varepsilon_0)}. \quad (\text{ПЗ.3})$$

Отсюда следует, что для приближения с точностью ε требуется N^* элементов, где

$$N^* < \frac{5}{4} 5^k l_0 = \frac{5}{4} \left(\frac{3}{2}\right)^{kc} l_0 < \frac{5}{4} \left(\frac{\log(1/C^2\varepsilon)}{2\log(1/C\varepsilon_0)}\right)^c l_0; \quad (\text{ПЗ.4})$$

здесь $c = \log 5 / \log(3/2) \approx 4$. Таким образом, для приближения с точностью ε требуется $O(\log^c(1/\varepsilon))$ элементов, т. е. доказательство теоремы Соловея–Китаева завершено.

Для доказательства леммы ПЗ.2 используются несколько элементарных фактов об умножении элементов группы $SU(2)$, которые мы сейчас приведем. Основная идея леммы заключается в работе в окрестности единицы, что сильно упрощает довольно сложные операции умножения в $SU(2)$. Уточним сказанное. Пусть U и V – элементы группы $SU(2)$, определим групповой коммутатор этих элементов с помощью следующей формулы:

$$[U, V]_{\text{gp}} \equiv UVU^\dagger V^\dagger. \quad (\text{ПЗ.5})$$

Предположим, что оба элемента U и V близки к единице, т. е. могут быть записаны в виде $U = e^{-iA}$ и $V = e^{-iB}$, где A и B – такие эрмитовы матрицы, что $\text{tr}|A|, \text{tr}|B| \leq \varepsilon$ для некоторого малого ε . Разложение $e^{\pm iA}$ и $e^{\pm iB}$ в ряд с точностью до квадратичных по A и B членов дает

$$D([U, V]_{\text{gp}}, e^{-[A, B]}) = O(\varepsilon^3), \quad (\text{ПЗ.6})$$

где $[A, B] = AB - BA$ – обычный коммутатор матриц (в действительности коммутатор для алгебры Ли $SU(2)$). Таким образом, в окрестности единицы можно изучать групповой коммутатор, исследуя свойства гораздо более простого коммутатора матриц.

В самом деле, для кубитов коммутатор матриц имеет особенно красивую форму. Произвольный элемент из $SU(2)$ может быть записан в виде $U = u(\vec{a}) \equiv \exp(-i\vec{a} \cdot \vec{\sigma}/2)$ для некоторого вектора \vec{a} с действительными компонентами. Аналогично $V = u(\vec{b}) = \exp(-i\vec{b} \cdot \vec{\sigma}/2)$ для некоторого вектора \vec{b} над полем действительных чисел. Напомним (см. упр. 2.40), что

$$[\vec{a} \cdot \vec{\sigma}, \vec{b} \cdot \vec{\sigma}] = 2i(\vec{a} \times \vec{b}) \cdot \vec{\sigma}, \quad (\text{ПЗ.7})$$

поэтому из (ПЗ.6) можно заключить, что

$$D([U, V]_{\text{gp}}, u(\vec{a} \times \vec{b})) = O(\varepsilon^3). \quad (\text{ПЗ.8})$$

Теперь легко понять основную идею доказательства леммы ПЗ.2. Ниже для полноты картины приводятся детали, связанные в основном с оценками приближений. Сейчас мы объясним только основную идею, которая проиллюстрирована на рис. ПЗ.2. Допустим, мы хотим аппроксимировать элемент $U = u(\vec{x})$ в S_{ε^2} . Из упр. ПЗ.4 можно видеть, что следовые метрики вида $D(U, I)$ равны (с точностью до небольших поправок) евклидову расстоянию $\|\vec{x}\|$, поэтому

для хорошего приближения выполняется неравенство $\|\vec{x}\| \leq \varepsilon^2$. Всегда можно выбрать такие \vec{y} и \vec{z} длиной не более ε , что $\vec{x} = \vec{y} \times \vec{z}$. Выберем \vec{y}_0 и \vec{z}_0 таким образом, что элементы $u(\vec{y}_0)$ и $u(\vec{z}_0)$ принадлежат множествам \mathcal{G}_l , которые соответственно « ε^2 -приближают» $u(\vec{y})$ и $u(\vec{z})$. Применив формулу (П3.6) к коммутатору $[u(\vec{y}_0), \vec{z}_0]_{\text{gp}}$, получим $O(\varepsilon^3)$ -приближение к U . Таким образом, построена $O(\varepsilon^3)$ -сеть для S_{ε^2} ; для завершения доказательства леммы следует применить шаг переноса, аналогичный использованному в основной части доказательства теоремы Соловея–Китаева, что дает $O(\varepsilon^3)$ -приближение к любому элементу из $S_{O(\varepsilon^{3/2})}$ с помощью $5l$ элементов.

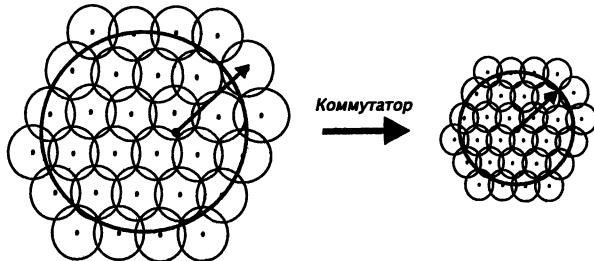


Рис. П3.2. Основная идея доказательства леммы П3.2 За счет взятия групповых коммутаторов элементов U_1 и U_2 в S_ε можно заполнить S_{ε^2} гораздо плотнее. Обратите внимание на то, что плотность кругов, возникающих в правой части рисунка, должна быть гораздо выше, чем это показано, поскольку для каждой пары кругов в левой части рисунка должен появиться один справа; меньшая плотность используется здесь исключительно для удобства восприятия. Доказательство леммы завершается применением шага переноса (который на рисунке не показан) для получения хорошего приближения к произвольному элементу из $S_{\sqrt{3}\varepsilon^{3/2}}$.

Упражнение П3.2. Пусть A и B — такие эрмитовы матрицы, что $\text{tr}|A|$, $\text{tr}|B| \leq \varepsilon$. Докажите, что для любого достаточно малого ε выполняется неравенство

$$D\left([e^{-iA}, e^{-iB}]_{\text{gp}}, e^{-[A, B]}\right) \leq d\varepsilon^3 \quad (\text{П3.9})$$

(здесь d — константа), из которого следует формула (П3.6). (Замечание: для практических целей интересно получить достаточно жесткую оценку величины d .)

Упражнение П3.3. Пусть \vec{x} и \vec{y} — векторы с действительными компонентами. Покажите, что

$$D(u(\vec{x}), u(\vec{y})) = 2\sqrt{2}\sqrt{1 - \cos(x/2)\cos(y/2) - \sin(x/2)\sin(y/2)\hat{x} \cdot \hat{y}}, \quad (\text{П3.10})$$

где $x \equiv \|\vec{x}\|$, $y \equiv \|\vec{y}\|$; \hat{x} и \hat{y} — единичные векторы соответственно в направлении векторов \vec{x} и \vec{y} .

Упражнение П3.4. Покажите, что если $\vec{y} = 0$, то формула для $D(u(\vec{x}), u(\vec{y}))$ упрощается и принимает вид

$$D(u(\vec{x}), I) = 4 \sin \left| \frac{x}{4} \right|. \quad (\text{П3.11})$$

Упражнение П3.5. Покажите, что если $x, y \leq \varepsilon$, то

$$D(u(\vec{x}), u(\vec{y})) = \|\vec{x} - \vec{y}\| + O(\varepsilon^3). \quad (\text{П3.12})$$

Доказательство (леммы П3.2).

Пусть \mathcal{G}_l является ε^2 -сетью в S_ε . Первый шаг доказательства состоит в демонстрации того факта, что $[\mathcal{G}_l, \mathcal{G}_l]_{\text{gp}}$ есть $C\varepsilon^3$ -сеть для множества S_{ε^2} и некоторой константы C .

Пусть $U \in S_{\varepsilon^2}$. Выберем такой вектор \vec{x} , что $U = u(\vec{x})$. Согласно упр. П3.4, $x \leq \varepsilon^2 + O(\varepsilon^6)$. Выберем такую пару векторов \vec{y} и \vec{z} длиной не более $\varepsilon + O(\varepsilon^5)$, что $\vec{x} = \vec{y} \times \vec{z}$. Поскольку \mathcal{G}_l является ε^2 -сетью для S_ε , можно взять такие U_1 и U_2 из $\mathcal{G}_l \cap S_\varepsilon$, что

$$D(U_1, u(\vec{y})) < \varepsilon^2 + O(\varepsilon^5), \quad (\text{П3.13})$$

$$D(U_2, u(\vec{z})) < \varepsilon^2 + O(\varepsilon^5). \quad (\text{П3.14})$$

Выберем такие векторы \vec{y}_0 и \vec{z}_0 , что $U_1 = u(\vec{y}_0)$ и $U_2 = u(\vec{z}_0)$. Из упр. П3.4 следует, что $y_0, z_0 \leq \varepsilon + O(\varepsilon^3)$. Наша задача — показать, что величина $D(U, [U_1, U_2]_{\text{gp}})$ меньше, чем $C\varepsilon^3$. Воспользуемся неравенством треугольника:

$$D(U, [U_1, U_2]_{\text{gp}}) \leq D(U, u(\vec{y}_0 \times \vec{z}_0)) + D(u(\vec{y}_0 \times \vec{z}_0), [U_1, U_2]_{\text{gp}}). \quad (\text{П3.15})$$

Второй член не превышает величины $d'\varepsilon^3$ (см. упр. П3.2), где d' — константа, немного большая d , из-за возможного вклада, связанного с неравенством $y_0, z_0 < \varepsilon + O(\varepsilon^3)$ (вместо $y_0, z_0 < \varepsilon$). Подставив $U = u(\vec{x})$, используя результат упр. П3.5, введя подходящую константу d'' и проводя элементарные алгебраические преобразования, можно увидеть, что

$$D(U, [U_1, U_2]_{\text{gp}}) \leq D(u(\vec{x}), u(\vec{y}_0 \times \vec{z}_0)) + d'\varepsilon^3 \quad (\text{П3.16})$$

$$= \|\vec{x} - \vec{y}_0 \times \vec{z}_0\| + d''\varepsilon^3 \quad (\text{П3.17})$$

$$= \|\vec{y} \times \vec{z} - \vec{y}_0 \times \vec{z}_0\| + d''\varepsilon^3 \quad (\text{П3.18})$$

$$= \|[(\vec{y} - \vec{y}_0) + \vec{y}_0] \times [(\vec{z} - \vec{z}_0) + \vec{z}_0] - \vec{y}_0 \times \vec{z}_0\| + d''\varepsilon^3 \quad (\text{П3.19})$$

$$\leq (d'' + 2)\varepsilon^3 + O(\varepsilon^4) \quad (\text{П3.20})$$

$$\leq C\varepsilon^3, \quad (\text{П3.21})$$

где C — константа, выбранная подходящим образом.

Второй этап доказательства леммы состоит в применении шага переноса, аналогичного использованному в основной части доказательства теоремы Соловея–Китаева. Говоря конкретнее, если задан элемент $U \in S_{\sqrt{C\varepsilon^3}}$, то можно найти такой элемент V из \mathcal{G}_l , что $D(U, V) \leq \varepsilon^2$, а следовательно, $UV^\dagger \in S_{\varepsilon^2}$. После этого можно отыскать W_1 и W_2 из \mathcal{G}_l , так что $D([W_1, W_2]_{\text{gp}}, UV^\dagger) \leq C\varepsilon^3$, а следовательно,

$$D([W_1, W_2]_{\text{gp}}, V, U) \leq C\varepsilon^3, \quad (\text{П3.22})$$

что завершает доказательство. ■

Упражнение ПЗ.6. Зафиксировав множество \mathcal{G} базисных элементов, опишите алгоритм, который по заданному описанию унитарного оператора U на одном кубите и требуемой точности $\varepsilon > 0$ эффективным образом вычисляет последовательность элементов из \mathcal{G} , которая аппроксимирует U с точностью ε .

Анализ в этом приложении является достаточно грубым, можно было бы провести более тонкое исследование. Особый интерес представляет, например, вопрос о наилучшем из возможных показателей степени c в оценке $O(\log^c(1/\varepsilon))$. Несложно убедиться в том, что c не может быть меньше единицы. Чтобы понять это, представьте, что в $SU(2)$ взято N маленьких шаров радиуса ε . Суммарный объем этих шаров имеет порядок ε^d с некоторой (несущественной в данном рассмотрении) константой d . Таким образом, если шары должны покрывать все пространство $SU(2)$, то число N должно быть порядка $\Omega(1/\varepsilon^d)$. Предположим, выбраны все возможные последовательности $U_1 U_2 \dots U_g$, состоящие из g элементов, взятых из \mathcal{G} . Очевидно, что эта последовательность может породить не больше $|\mathcal{G}|^g$ различных унитарных операций. Таким образом, должна выполняться оценка $|\mathcal{G}|^g = \Omega(1/\varepsilon^d)$, отсюда нижняя оценка на количество элементов выглядит как

$$g = \Omega\left(\log\left(\frac{1}{\varepsilon}\right)\right). \quad (\text{ПЗ.23})$$

Задача ПЗ.1. Данная задача описывает усовершенствованную конструкцию, которая дает оценку $O(\log^2(1/\varepsilon) \log^c(\log(1/\varepsilon)))$ на количество элементов для приближения требуемого элемента с точностью ε (при произвольной константе c , большей двойки).

1. Пусть $\mathcal{N} - \delta$ -сеть в S_ε , причем $0 < \delta < \varepsilon \leq \varepsilon_0$, где ε_0 – достаточно малое число. Покажите, что $[\mathcal{N}, \mathcal{N}]_{\text{gp}} - d\delta\varepsilon$ -сеть в S_{ε^2} (где d – некоторая константа).
2. Пусть $\mathcal{G}_l - \delta$ -сеть в S_ε , причем $0 < \delta < \varepsilon \leq \varepsilon_0$. Покажите, что $\mathcal{G}_{4^k l}$ есть $d^k \delta \varepsilon^{2^k-1}$ -сеть в $S_{\varepsilon^{2^k}}$.
3. Определим число k формулой

$$k \equiv \left\lceil \log\left(\frac{\log(1/\varepsilon)}{\log(1/\varepsilon_0)}\right) \right\rceil \quad (\text{ПЗ.24})$$

(здесь квадратные скобки означают взятие целой части действительного числа) и будем считать, что можно найти такое l , что $\mathcal{G}_l - \delta_0$ -сеть в S_{ε_0} , где

$$d^k \delta_0 = \varepsilon_0. \quad (\text{ПЗ.25})$$

Покажите, что $\mathcal{G}_{4^k l} - \varepsilon$ -сеть в $S_{\varepsilon_0^{2^k}}$.

4. С использованием уже доказанной версии теоремы Соловея–Китаева покажите, что $l = O(k^c)$ подходит для предыдущего пункта (здесь $c =$

$\log 5 / \log(3/2)$ — константа, появляющаяся в показателе степени в уже доказанной версии теоремы Соловея–Китаева).

5. Соедините вместе предыдущие утверждения, чтобы доказать, что с помощью $O(\log^2(1/\varepsilon) \log^c(1/\varepsilon))$ элементов можно построить ε -приближение к любому элементу из $SU(2)$.
6. Покажите, что в предыдущем пункте подойдет любая константа $c > 2$.

Задача П3.2 (исследование). Найдите (если она существует) асимптотически более быструю процедуру приближения, чем в предыдущей задаче. В идеале — найдите процедуру, для которой

1. достигается нижняя оценка $\Omega(\log(1/\varepsilon))$ на количество элементов для выполнения приближения;
2. получается эффективный алгоритм для построения таких приближающих последовательностей элементов.

Задача П3.3 (исследование). Зафиксируйте конечное множество \mathcal{G} элементов на одном кубите, которые можно выполнить устойчивым к ошибкам образом и которые порождают множество, плотное во множестве элементов на одном кубите; например, $(\pi/8)$ -оператор и оператор Адамара. Разработайте элегантный, эффективный и достаточно компактный метод, который по произвольному элементу U на одном кубите и некоторому числу $\varepsilon > 0$ выдает последовательность элементов из устойчивого к ошибкам набора, дающую ε -приближение к U (с точностью до общего фазового множителя).

История и дополнительная литература

Результаты этого приложения были доказаны Соловеем в 1995 г. (неопубликованная работа) и независимо Китаевым, который схематично изложил доказательство в работе [213]. Кроме того, Китаев заметил, что результат может быть обобщен на многие группы Ли, отличные от $SU(2)$; главное использовавшееся в доказательстве свойство группы $SU(2)$ — это утверждение, что $[S_\varepsilon, S_\varepsilon]_{\text{gp}} \supseteq S_{\Omega(\varepsilon^2)}$, поэтому для других групп Ли, обладающих таким же свойством, тоже выполняется некоторый аналог теоремы Соловея–Китаева. Например, эта теорема верна для группы Ли $SU(d)$ — группы унитарных матриц размера $d \times d$ с единичным детерминантом. После знакомства с этим фактом Соловей впоследствии обобщил свое доказательство сходным образом. Наше изложение данного материала существенно выиграло от лекции Фридмана, прочитанной в 1999 г., а также от обсуждений с Фридманом, Китаевым и Соловеем.

Приложение 4

ТЕОРИЯ ЧИСЕЛ

Для понимания криптографических систем и способов их «взлома» с помощью квантовых компьютеров необходимо знание элементарной теории чисел. В этом приложении приводится обзор некоторых основных утверждений теории чисел.

П4.1 Начальные сведения

Введем некоторые обозначения. Множеством целых чисел называется множество $\{\dots, -2, -1, 0, 1, 2, \dots\}$ (для него используется обозначение \mathbb{Z}). Иногда мы будем использовать термин *натуральные числа*, имея в виду неотрицательные целые числа, но чаще мы будем употреблять понятия *неотрицательные целые* или *положительные целые* числа, чтобы подчеркнуть различие между множеством, включающим нуль, и множеством, не содержащим нуля.

Пусть n — целое число. Говорят, что целое число d делит n (обозначение: $d|n$), если существует такое целое k , что $n = dk$. В таком случае также можно сказать, что n делится на d или что d является делителем числа n . Заметим, что 1 и n всегда являются делителями числа n . Если d не делит n (не является делителем числа n), пишут $d \nmid n$, например: $3|6$, $3|18$, но $3 \nmid 5$, $3 \nmid 7$.

Упражнение П4.1 (транзитивность). Покажите, что если $a|b$ и $b|c$, то $a|c$.

Упражнение П4.2. Покажите, что если $d|a$ и $d|b$, то d также делит линейную комбинацию чисел a и b ($ax + by$, где x и y — целые числа).

Упражнение П4.3. Пусть a и b — положительные целые числа. Докажите, что если $a|b$, то $a \leq b$. Получите следствие этого факта: $a = b$, если $a|b$ и $b|a$.

Простым называют целое число m , большее единицы, которое имеет только два делителя: 1 и m . Перечислим несколько первых простых чисел: 2, 3, 5, 7, 11, 13, 17, ... Оказывается, любое положительное целое число можно однозначно представить в виде произведения простых множителей. Это утверждение известно как *основная теорема арифметики*.

Теорема П4.1 (основная теорема арифметики). Пусть a — положительное целое число, большее единицы. Тогда a можно представить в виде произведения простых множителей:

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \tag{П4.1}$$

где p_1, \dots, p_n — различные простые числа, а a_1, \dots, a_n — положительные целые числа. Более того, это разложение единственno (с точностью до порядка сомножителей).

Доказательство. Читателю, не знакомому с доказательством основной теоремы арифметики, настоятельно рекомендуется попытаться доказать ее самостоятельно. В случае неудачи доказательство можно найти в любом элементарном учебнике по теории чисел; см. ссылки «История и дополнительная литература» в конце приложения. ■

Легко найти разложение на простые множители небольших чисел методом проб и ошибок, например: $20 = 2^2 \cdot 5^1$. Для больших чисел эффективный алгоритм разложения на простые множители с помощью классического компьютера не найден, хотя на его поиски затрачены неимоверные усилия.

Упражнение П4.4. Найдите разложение на простые множители чисел 697 и 36 300.

П4.2 Арифметика остатков и алгоритм Евклида

Приемы обычной арифметики хорошо знакомы каждому. Другим типом арифметики является арифметика остатков. Мы считаем, что читатель хорошо знаком с элементарными идеями арифметики остатков, поэтому лишь кратко напомним основные идеи и обозначения, прежде чем перейти к более сложным областям этой дисциплины.

Из самого названия ясно, что арифметика остатков имеет дело с *остатками*. Если мы делим 18 на 7, то получаем неполное частное 2 и 4 в остатке. Говоря строго, для любых положительных чисел x и n существует (единственное) представление x в виде

$$x = kn + r, \tag{П4.2}$$

где k — неотрицательное целое число (неполное частное, результат деления x на n), а *остаток* r лежит между 0 и $(n - 1)$ (включительно). Арифметика остатков является обычной арифметикой, в которой мы обращаем внимание только на остатки. Будем использовать обозначение $\langle (mod n) \rangle$, чтобы показать, что мы имеем дело с арифметикой остатков. Например, можно написать $2 = 5 = 8 = 11 \langle mod 3 \rangle$, поскольку 2, 5, 8 и 11 дают одинаковый остаток (2) при делении на 3. Обозначение $\langle (mod n) \rangle$ напоминает нам, что мы имеем дело с остатками по модулю n .

Операции сложения, умножения и вычитания для арифметики остатков могут быть определены очевидным образом, но не столь очевидно, как деление. Чтобы понять, как это сделать, введем еще один ключевой термин теории чисел — *наибольший общий делитель* двух целых чисел. Наибольший общий делитель чисел a и b ($НОД(a, b)$) — это наибольшее целое число, которое одновременно делит и число a , и число b . Например, наибольший общий делитель чисел 12 и 18 равен 6. Проще всего в этом убедиться, выписав все положительные делители числа 18 (1, 2, 3, 6, 9, 18) и числа 12 (1, 2, 3, 4, 6, 12), после чего выбрать максимальное число, принадлежащее обоим множествам. Однако этот способ неэффективен, и его нельзя использовать для больших чисел. Суще-

ствует более эффективный способ нахождения наибольшего общего делителя, называемый *алгоритмом Евклида*, который будет описан ниже.

Теорема П4.2 (теорема представления для НОД). Наибольший общий делитель чисел a и b равен наименьшему положительному целому числу, которое можно представить в виде $ax + by$, где x и y — целые числа.

Доказательство. Пусть $s = ax + by$ — наименьшее положительное целое число, которое может быть представлено в виде линейной комбинации a и b . Поскольку $\text{НОД}(a, b)$ делит a и b , он также делит s . Отсюда следует, что $\text{НОД}(a, b) \leq s$. Чтобы завершить доказательство, покажем, что $s \leq \text{НОД}(a, b)$ (доказав, что s является делителем чисел a и b). Будем доказывать «от противного». Предположим, что s не делит a . Тогда $a = ks + r$, где остаток r удовлетворяет условию $1 \leq r \leq (s - 1)$. После переноса слагаемого ks в другую часть получим (учитывая, что $s = ax + by$), что $a(1 - kx) + b(-ky) = r$ — положительное целое число меньшее s , которое можно представить в виде линейной комбинации чисел a и b . Это противоречит нашему определению s как наименьшего целого числа, которое можно записать в виде линейной комбинации a и b . Следовательно, наше предположение неверно, и s делит a . Аналогично доказывается и тот факт, что s делит b . ■

Следствие П4.3 Предположим, что c делит a и b . Тогда c делит $\text{НОД}(a, b)$.

Доказательство. Согласно теореме П4.2, $\text{НОД}(a, b) = ax + by$, где x и y — целые числа. Поскольку число c делит a и b , оно должно также делить $ax + by$.

Зададимся вопросом: в каком случае у числа a есть обратное в арифметике остатков? Иными словами, для каких a и n существует такое b , что $ab \equiv 1 \pmod{n}$? Заметим, например, что $2 \cdot 3 \equiv 1 \pmod{5}$, следовательно, число 3 является обратным для числа 2 в арифметике остатков по модулю 5. В то же время методом проб и ошибок можно убедиться, что у числа 2 нет обратного в арифметике остатков по модулю 4. Оказывается, наличие обратных чисел в арифметике остатков связано с понятием *взаимной простоты* (числа a и b называют *взаимно-простыми*, если их наибольший общий делитель равен единице). Например, 14 и 9 — взаимно-простые числа, поскольку для числа 14 положительными делителями являются 1, 2, 7 и 14, а для числа 9 — числа 1, 3 и 9. Приводимое ниже следствие связывает существование обратных элементов в арифметике остатков со свойством взаимной простоты.

Следствие П4.4 Пусть n — целое число, большее единицы. Для целого числа a существует обратное по модулю n тогда и только тогда, когда $\text{НОД}(a, n) = 1$, т. е. когда a и n — взаимно-простые.

Доказательство. Пусть существует число, обратное a (по модулю n), которое мы обозначим как a^{-1} . Тогда $aa^{-1} \equiv 1 + kn$ для некоторого целого k , следовательно, $aa^{-1} + (-k)n \equiv 1$. Из теоремы П4.2 следует, что $\text{НОД}(a, n) = 1$.

И наоборот, если $\text{НОД}(a, n) = 1$, то должны существовать такие целые числа l и b , что $al + bn \equiv 1$, т. е. $al \equiv 1 \pmod{n}$. Следовательно, l является обратным для числа a , т. е. $l = a^{-1}$. ■

Упражнение П4.5. Пусть p — простое число. Докажите, что для каждого

числа от 1 до $(p - 1)$ включительно существует обратное (по модулю p). Для каких чисел в диапазоне от 1 до $(p^2 - 1)$ включительно не существует обратного по модулю p^2 ?

Упражнение П4.6. Найдите число, обратное 17 по модулю 24.

Упражнение П4.7. Найдите, число, обратное $(n + 1)$ по модулю n^2 , если n — целое число, большее единицы.

Упражнение П4.8 (единственность обратного). Пусть b и b' — числа, обратные a (по модулю n). Докажите, что $b = b' \pmod{n}$.

Следующая ниже теорема чрезвычайно важна для построения алгоритма Евклида нахождения наибольшего общего делителя двух положительных целых чисел.

Теорема П4.5. Пусть a и b — целые числа, r — остаток от деления a на b . Тогда если $r \neq 0$, то

$$\text{НОД}(a, b) = \text{НОД}(b, r). \quad (\text{П4.3})$$

Доказательство. Чтобы доказать равенство (П4.3), покажем, что каждая из его частей делит другую. Сначала докажем, что левая часть делит правую. Заметим, что $r = (a - kb)$ для некоторого целого k . Поскольку $\text{НОД}(a, b)$ делит a , b и любые их линейные комбинации, $\text{НОД}(a, b)$ также делит r . С учетом следствия П4.3 сделаем вывод, что $\text{НОД}(a, b)$ делит $\text{НОД}(b, r)$. Чтобы доказать, что правая часть делит левую, заметим, что $\text{НОД}(b, r)$ делит b , а поскольку $a = r + kb$ — линейная комбинация чисел b и r , получим, что $\text{НОД}(b, r)$ также делит a . С учетом следствия П4.3 можно заключить, что $\text{НОД}(b, r)$ делит $\text{НОД}(a, b)$. ■

Упражнение П4.9. Покажите, как найти $\text{НОД}(a, b)$, если известны разложения чисел a и b на простые множители. Разложите на простые множители числа 6825 и 1430 и вычислите с помощью этих разложений $\text{НОД}(6825, 1430)$.

Алгоритм Евклида для нахождения наибольшего общего делителя двух положительных целых чисел a и b работает следующим образом. (Без ограничения общности можно считать, что $a > b$.) Разделим a на b с остатком, пусть неполное частное равно k_1 , а остаток равен r_1 : $a = k_1b + r_1$. Из теоремы П4.5 следует, что $\text{НОД}(a, b) = \text{НОД}(b, r_1)$. Затем разделим с остатком b на r_1 : $b = k_2r_1 + r_2$. С учетом теоремы П4.5 заключаем, что $\text{НОД}(a, b) = \text{НОД}(b, r_1) = \text{НОД}(r_1, r_2)$. На следующем шаге разделим с остатком r_1 на r_2 : $r_1 = k_3r_2 + r_3$. Согласно теореме П4.5, $\text{НОД}(a, b) = \text{НОД}(b, r_1) = \text{НОД}(r_1, r_2) = \text{НОД}(r_2, r_3)$. Продолжим эту процедуру, каждый раз производя деление с остатком последнего полученного остатка на остаток, полученный на предпоследнем шаге, получая новые остаток и неполное частное. Выполнение алгоритма завершается, когда на очередном шаге мы получим нулевой остаток, т. е. $r_m = k_{m+1}r_{m+1}$ для некоторого m . При этом $\text{НОД}(a, b) = \text{НОД}(r_m, r_{m+1}) = r_{m+1}$, следовательно, результатом работы алгоритма является число r_{m+1} .

Найдем НОД(6825, 1430) с помощью алгоритма Евклида:

$$6825 = 4 \cdot 1430 + 1105, \quad (\text{П4.4})$$

$$1430 = 1 \cdot 1105 + 325, \quad (\text{П4.5})$$

$$1105 = 3 \cdot 325 + 130, \quad (\text{П4.6})$$

$$325 = 2 \cdot 130 + 65, \quad (\text{П4.7})$$

$$130 = 2 \cdot 65. \quad (\text{П4.8})$$

Следовательно, НОД(6825, 1430) = 65.

С помощью модификации алгоритма Евклида несложно найти такие целые числа x и y , что $ax + by = \text{НОД}(a, b)$. Начнем с последовательного выполнения операций деления с остатком (см. два предыдущих абзаца). Затем подставим последнее из полученных в алгоритме Евклида равенств ((П4.8) в нашем примере) в предпоследнее. Переформулированное таким образом предпоследнее равенство подставим в стоящее перед ним и т. д. вплоть до первого. Тогда имеем следующий результат:

$$65 = 325 - 2 \cdot 130 = \quad (\text{П4.9})$$

$$= 325 - 2 \cdot (1105 - 3 \cdot 325) = -2 \cdot 1105 + 7 \cdot 325 = \quad (\text{П4.10})$$

$$= -2 \cdot 1105 + 7 \cdot (1430 - 1 \cdot 1105) = 7 \cdot 1430 - 9 \cdot 1105 = \quad (\text{П4.11})$$

$$= 7 \cdot 1430 - 9 \cdot (6825 - 4 \cdot 1430) = -9 \cdot 6825 + 37 \cdot 1430. \quad (\text{П4.12})$$

Итак, мы получили интересующее нас представление числа НОД(6825, 1430) = 65, а именно: $65 = 6825 \cdot (-9) + 1430 \cdot 37$.

Какие ресурсы используются в алгоритме Евклида? Пусть каждое из чисел a и b представляется строкой битов длиной не более L . Очевидно, что тогда все неполные частные k_i и остатки r_i также могут быть записаны строками из L бит, так что можно считать, что все вычисления выполняются в L -битовой арифметике. Ключевым моментом для оценки используемых ресурсов является то обстоятельство, что $r_{i+2} \leq r_i/2$. Для доказательства этого факта рассмотрим два случая:

- $r_{i+1} \leq r_i/2$. Ясно, что $r_{i+2} \leq r_{i+1}$, поэтому $r_{i+2} \leq r_i/2$.
- $r_{i+1} > r_i/2$. Тогда $r_i = 1 \cdot r_{i+1} + r_{i+2}$, следовательно, $r_{i+2} = r_i - r_{i+1} \leq r_i/2$.

Поскольку $r_{i+2} \leq r_i/2$, операция деления с остатком в алгоритме Евклида должна быть выполнена не более чем $2\lceil \log a \rceil = O(L)$ раз (где $\lceil x \rceil$ — минимальное целое, не меньшее x). Каждое деление с остатком требует $O(L^2)$ операций, так что для всего алгоритма Евклида потребуется $O(L^3)$ операций. Нахождение таких чисел x и y , что $ax + by = \text{НОД}(a, b)$, требует еще и $O(L)$ подстановок, для каждой из которых необходимо выполнить $O(L^2)$ операций, поэтому всего понадобится $O(L^3)$ операций.

Алгоритм Евклида также может быть использован для эффективного поиска мультипликативных обратных в арифметике остатков. Это неявно вытекало

из доказательства следствия П4.4; теперь можно доказать это в явном виде. Пусть числа a и n — взаимно простые, и мы хотим найти a^{-1} по модулю n . Поскольку $\text{НОД}(a, n) = 1$, с помощью алгоритма Евклида можно найти такие целые числа x и y , что

$$ax + ny = 1. \quad (\text{П4.13})$$

Заметим, что $ax = 1 - ny = 1 \pmod{n}$, т. е. число x является мультипликативным обратным числу a (по модулю n). Более того, этот алгоритм эффективен с точки зрения затраченных ресурсов — требуется только $O(L^3)$ операций, где L — количество битов в записи числа n .

Теперь нам известен эффективный способ поиска мультипликативных обратных в арифметике остатков. С его помощью легко решать простые линейные уравнения вида

$$ax + b = c \pmod{n}. \quad (\text{П4.14})$$

Пусть a и n — взаимно простые целые числа. С помощью алгоритма Евклида можно быстро найти число a^{-1} — обратное a (по модулю n), а следовательно, и решение предыдущего уравнения:

$$x = a^{-1}(c - b) \pmod{n}. \quad (\text{П4.15})$$

Следующим важным результатом является *китайская теорема об остатках*, расширяющая круг уравнений, которые мы можем решить. Из этой теоремы вытекает метод решения систем уравнений в арифметике остатков.

Теорема П4.6 (китайская теорема об остатках). Пусть m_1, \dots, m_n — такие положительные целые числа, что любые два из них m_i и m_j ($i \neq j$) — взаимно простые. Тогда система уравнений

$$x = a_1 \pmod{m_1}, \quad (\text{П4.16})$$

$$x = a_2 \pmod{m_2}, \quad (\text{П4.17})$$

\dots

$$x = a_n \pmod{m_n} \quad (\text{П4.18})$$

имеет решение. Более того, любые два решения этой системы дают одинаковый остаток по модулю $M = m_1 m_2 \times \dots \times m_n$.

Доказательство. Доказательство будет заключаться в явном построении решения системы уравнений. Введем обозначение $M_i \equiv M/m_i$ и заметим, что m_i и M_i — взаимно простые числа. Поэтому для числа M_i существует мультипликативное обратное (обозначим его N_i) по модулю m_i . Обозначим $x \equiv \sum_i a_i M_i N_i$. Заметим, что $M_i N_i = 1 \pmod{m_i}$ и $M_i N_i = 0 \pmod{m_j}$ при $i \neq j$, поэтому $x = a_i \pmod{m_i}$, отсюда следует существование решения исходной системы уравнений.

Предположим, существуют два решения исходной системы уравнений: x и x' . Тогда $x - x' = 0 \pmod{m_i}$ для всех i , поэтому m_i делит $x - x'$ для любого i . Поскольку все числа m_i попарно взаимно простые, произведение $M = m_1 \times \dots \times m_n$ также делит $x - x'$, т. е. $x = x' \pmod{M}$, что и требовалось доказать.



Алгоритм Евклида и китайская теорема об остатках — наиболее яркие достижения алгоритмической теории чисел. Тем более забавно, что именно они играют важную роль в последовательности идей, ведущих к RSA-криптосистемам, защищенность которых базируется на *сложности выполнения* некоторых алгоритмических задач в теории чисел. Переходим к основам теории чисел, необходимым для понимания RSA-криптосистем. Основная идея заключена в знаменитом факте классической теории чисел — *малой теореме Ферма*, которую следует отличать от последней («Великой») теоремы Ферма, а также в выполненном Эйлером обобщении малой теоремы Ферма. Доказательство малой теоремы Ферма опирается на следующую красавицу лемму.

Лемма П4.7. Пусть p — простое число, k — целое число, лежащее в диапазоне от 1 до $(p - 1)$. Тогда p делит $\binom{p}{k}$.

Доказательство. Запишем тождество

$$p(p - 1) \times \dots \times (p - k + 1) = \binom{p}{k} k(k - 1) \times \dots \times 1. \quad (\text{П4.19})$$

Поскольку $k \geq 1$, левая часть (а следовательно и правая) делится на p . Учитывая, что $k \leq p - 1$, заключаем, что множитель $k(k - 1) \times \dots \times 1$ не делится на p . Следовательно, множитель $\binom{p}{k}$ должен делиться на p . ■

Теорема П4.8 (малая теорема Ферма). Пусть p — простое число, a — любое целое. Тогда $a^p \equiv a \pmod{p}$. Если a не делится на p , то $a^{p-1} \equiv 1 \pmod{p}$.

Доказательство. Второе утверждение теоремы следует из первого, поскольку если число a не делится на p , то для него существует мультипликативное обратное по модулю p , поэтому $a^{p-1} = a^{-1}a^p = a^{-1}a = 1 \pmod{p}$. Докажем первое утверждение теоремы для положительного a (случай неположительного a является простым следствием) индукцией по a . При $a = 1$ получим $a^p = 1 = a \pmod{p}$. Предположим, первое утверждение теоремы выполнено для a , т. е. $a^p \equiv a \pmod{p}$ и докажем его для $(a + 1)$. Запишем биноминальное разложение

$$(1 + a)^p = \sum_{k=0}^p \binom{p}{k} a^k. \quad (\text{П4.20})$$

Согласно лемме П4.7, p делит $\binom{p}{k}$ при $1 \leq k \leq p - 1$, поэтому все члены, кроме первого и последнего, дают остаток 0 по модулю p : $(1 + a)^p \equiv (1 + a^p) \pmod{p}$. Поскольку $a^p \equiv a \pmod{p}$, получим $(1 + a)^p \equiv (1 + a) \pmod{p}$, что и требовалось доказать. ■

Существует замечательное обобщение малой теоремы Ферма, принадлежащее Эйлеру. Оно использует понятие *функции Эйлера* φ : $\varphi(n)$ определяется как число положительных целых чисел, меньших n и взаимно простых с n . Например, нетрудно заметить, что все положительные целые числа, меньшие простого p , взаимно просты с p , следовательно, $\varphi(p) = p - 1$. С числом p^α будут взаимно простыми только числа, кратные p : $p, 2p, 3p, \dots, (p^{\alpha-1} - 1)p$. Отсюда следует, что

$$\varphi(p^\alpha) = (p^\alpha - 1) - (p^{\alpha-1} - 1) = p^{\alpha-1}(p - 1). \quad (\text{П4.21})$$

Далее, если a и b взаимно простые, то в соответствии с китайской теоремой об остатках имеем

$$\varphi(ab) = \varphi(a)\varphi(b). \quad (\text{П4.22})$$

Чтобы доказать этот факт, рассмотрим систему уравнений $x = x_a \pmod{a}$, $x = x_b \pmod{b}$. Применяя китайскую теорему об остатках к этой системе уравнений, легко установить взаимно однозначное соответствие между такими парами (x_a, x_b) , что $1 \leq x_a < a$, $1 \leq x_b < b$, $\text{НОД}(x_a, a) = 1$, $\text{НОД}(x_b, b) = 1$, и такими целыми числами x , что $1 \leq x < ab$, $\text{НОД}(x, ab) = 1$. Всего существует $\varphi(a)\varphi(b)$ таких пар (x_a, x_b) и $\varphi(ab)$ чисел x ; таким образом, равенство (П4.22) доказано.

Уравнения (П4.21) и (П4.22) приводят к формуле для $\varphi(n)$, использующей разложение числа n на простые множители ($n = p_1^{\alpha_1} \times \dots \times p_k^{\alpha_k}$):

$$\varphi(n) = \prod_{j=1}^k p_j^{\alpha_j - 1} (p_j - 1). \quad (\text{П4.23})$$

Упражнение П4.10. Найдите $\varphi(187)$.

Упражнение П4.11. Докажите, что

$$n = \sum_{d|n} \varphi(d), \quad (\text{П4.24})$$

где суммирование ведется по всем целым положительным делителям d числа n , включая 1 и n . (Указание: сначала докажите это утверждение для $n = p^\alpha$, а для завершения доказательства воспользуйтесь свойством (П4.22).)

Существует следующее (доказанное Эйлером) красивое обобщение малой теоремы Ферма.

Теорема П4.9. Пусть числа a и n — взаимно-простые. Тогда $a^{\varphi(n)} = 1 \pmod{n}$.

Доказательство. Сначала покажем индукцией по α , что $a^{\varphi(p^\alpha)} = 1 \pmod{p^\alpha}$. Для $\alpha = 1$ это утверждение сводится к малой теореме Ферма. Предположим, что утверждение верно для $\alpha \geq 1$, т. е.

$$a^{\varphi(p^\alpha)} = 1 + kp^\alpha \quad (\text{П4.25})$$

для некоторого целого k . Тогда согласно уравнению (П4.21) имеем

$$a^{\varphi(p^{\alpha+1})} = a^{\varphi(p^\alpha)(p-1)} = \quad (\text{П4.26})$$

$$= a^{p\varphi(p^\alpha)} = \quad (\text{П4.27})$$

$$= (1 + kp^\alpha)^p = \quad (\text{П4.28})$$

$$= 1 + \sum_{j=1}^p \binom{p}{j} k^j p^{j\alpha}. \quad (\text{П4.29})$$

Используя лемму П4.2, легко показать, что $p^{\alpha+1}$ делит все члены, стоящие под знаком суммы, так что

$$a^{\varphi(p^{\alpha+1})} = 1 \pmod{p^{\alpha+1}}, \quad (\text{П4.30})$$

т. е. индуктивный переход доказан. Для завершения доказательства теоремы следует заметить, что для произвольного $n = p_1^{\alpha_1} \times \dots \times p_m^{\alpha_m}$ при каждом j выполняется равенство $a^{\varphi(n)} = 1 \pmod{p_j^{\alpha_j}}$, поскольку $\varphi(n)$ делится на $\varphi(p_j^{\alpha_j})$. Применяя конструкцию, построенную при доказательстве китайской теоремы об остатках, можно заметить, что любое решение системы уравнений $x = 1 \pmod{p_j^{\alpha_j}}$ должно удовлетворять условию $x = 1 \pmod{n}$, поэтому $a^{\varphi(n)} = 1 \pmod{n}$. ■

Введем обозначение Z_n^* для множества всех элементов Z_n , для которых существуют мультиликативные обратные элементы по модулю n , т. е. для множества тех элементов Z_n , которые взаимно простые с n . Легко видеть, что множество Z_n^* является группой по умножению (это означает, что Z_n^* содержит единичный элемент, мультиликативные обратные для всех своих элементов, а также произведение любых двух элементов; обзор элементарной теории групп дан в Приложении 2), а ее мощность равна $\varphi(n)$. Оказывается, группа Z_n^* обладает весьма интересной структурой, если n является степенью нечетного простого числа p ($n = p^\alpha$). Такая группа $Z_{p^\alpha}^*$ является циклической, т. е. существует элемент g из $Z_{p^\alpha}^*$, порождающий группу $Z_{p^\alpha}^*$: любой элемент x группы $Z_{p^\alpha}^*$ может быть представлен в виде $x = g^k \pmod{n}$ с некоторым неотрицательным k .

Теорема П4.10. Пусть p — нечетное простое число, α — положительное целое число. Тогда группа $Z_{p^\alpha}^*$ является циклической.

Доказательство. Доказательство этой теоремы выходит за рамки нашей книги. Его можно найти в разных учебниках по теории чисел, см., например, разд. 3.2 книги Кнута [225]. ■

Упражнение П4.12. Докажите, что Z_n^* — группа относительно операции умножения по модулю n , а ее мощность равна $\varphi(n)$.

Упражнение П4.13. Пусть a — произвольный элемент группы Z_n^* . Докажите, что множество $S \equiv \{1, a, a^2, \dots\}$ образует подгруппу в Z_n^* и что мощность S равна наименьшему целому числу r , удовлетворяющему уравнению $a^r = 1 \pmod{n}$.

Упражнение П4.14. Пусть g — образующая группы Z_n^* . Покажите, что порядок элемента g равен $\varphi(n)$.

Упражнение П4.15. Теорема Лагранжа (теорема П2.1) утверждает, что мощность подгруппы делит мощность группы. Докажите теорему П4.9 ($a^{\varphi(n)} = 1 \pmod{n}$ для любого $a \in Z_n^*$) другим способом — с использованием теоремы Лагранжа.

П4.3 Сведение разложения на простые множители к нахождению порядка элемента

Задача разложения на простые множители с помощью классического компьютера оказывается эквивалентна другой задаче — *нахождению порядка*. Этот факт очень важен, поскольку с помощью квантового компьютера можно быстро решать задачу нахождения порядка, а значит, можно осуществить и быстрое разложение на простые множители. В этом разделе мы покажем эквивалентность этих двух задач, фокусируя внимание читателя именно на сведении разложения на простые множители к нахождению порядка.

Пусть N — положительное целое число, x — число, взаимно простое с N и $1 \leq x < N$. *Порядком* числа x по модулю N называют наименьшее положительное целое число, для которого $x^r \equiv 1 \pmod{N}$. *Задача нахождения порядка* заключается в определении r по заданным x и N .

Упражнение П4.16. Докажите, используя теорему П4.9, что порядок числа x по модулю N делит число $\varphi(N)$.

Процедура сведения разложения на простые множители к нахождению порядка элемента включает два основных шага: 1) необходимо показать, что можно найти множитель числа n , если мы умеем находить нетривиальное решение $x \neq \pm 1 \pmod{N}$ уравнения $x^2 = 1 \pmod{N}$; 2) необходимо доказать, что произвольно выбранное взаимно простое с N число y с большой вероятностью имеет порядок r , который является четным числом и $y^{r/2} \neq \pm 1 \pmod{N}$, т. е. $x \equiv y^{r/2} \pmod{N}$ — решение уравнения $x^2 = 1 \pmod{N}$.

Теорема П4.11. Пусть N — составное число длиной L бит, x — нетривиальное решение уравнения $x^2 = 1 \pmod{N}$ в диапазоне $1 \leq x \leq N$, т. е. $x \neq 1 \pmod{N}$, $x \neq N - 1 = -1 \pmod{N}$. Тогда по крайней мере одно из чисел $\text{НОД}(x - 1, N)$ и $\text{НОД}(x + 1, N)$ является нетривиальным делителем числа N , и его можно вычислить за $O(L^3)$ операций.

Доказательство. Поскольку $x^2 = 1 \pmod{N}$, число N делит $x^2 - 1 = (x + 1)(x - 1)$, следовательно, N должно иметь общий делитель либо с $(x + 1)$, либо с $(x - 1)$. Но по предположению $1 < x < (N - 1)$, поэтому $(x - 1) < (x + 1) < N$, т. е. общий множитель не может равняться N . Используя алгоритм Евклида, найдем $\text{НОД}(x - 1, N)$ и $\text{НОД}(x + 1, N)$, а следовательно, и нетривиальный делитель числа N (на это потребуется $O(L^3)$ операций). ■

Лемма П4.12. Пусть p — нечетное простое число; 2^d — максимальная степень числа 2, делящая $\varphi(p^\alpha)$. Тогда с вероятностью ровно $1/2$ число 2^d делит порядок по модулю p^α элемента из $\mathbb{Z}_{p^\alpha}^*$, выбранного случайно и равновероятно.

Доказательство. Заметим, что число $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ — четное, поскольку p — нечетное, следовательно, $d \geq 1$. Согласно теореме П4.10 существует образующая g группы $\mathbb{Z}_{p^\alpha}^*$, поэтому произвольный элемент этой группы может

быть записан в виде $g^k \pmod{p^\alpha}$ для некоторого k в диапазоне от 1 до $\varphi(p^\alpha)$. Пусть r — порядок элемента g^k по модулю p^α . Рассмотрим два случая. Первый случай: k — нечетное число. Поскольку $g^{kr} = 1 \pmod{p^\alpha}$, можно сделать заключение, что $\varphi(p^\alpha) | kr$, поэтому $2^d | r$, так как число k — нечетное. Второй случай: k — четное число. Тогда имеем

$$g^{k\varphi(p^\alpha)/2} = \left(g^{\varphi(p^\alpha)}\right)^{k/2} = 1^{k/2} = 1 \pmod{p^\alpha}. \quad (\text{П4.31})$$

Поэтому $r | (\varphi(p^\alpha)/2)$, отсюда следует, что 2^d не делит r .

Итак, группу $\mathbb{Z}_{p^\alpha}^*$ можно разбить на две части равной мощности: элементы, которые могут быть представлены в виде g^k с нечетным k (для них $2^d | r$, где r — порядок g^k) и в виде g^k с четным k (для них $2^d \nmid r$). Поэтому с вероятностью $1/2$ число 2^d делит порядок r произвольно выбранного элемента группы $\mathbb{Z}_{p^\alpha}^*$. ■

Теорема П4.13. Пусть $N = p_1^{\alpha_1} \times \dots \times p_m^{\alpha_m}$ — разложение нечетного составного числа на простые множители. Пусть x — элемент из \mathbb{Z}_N^* , выбранный случайно и равновероятно, r — порядок элемента x (по модулю N). Тогда

$$p(r \text{ четное и } x^{r/2} \neq -1 \pmod{N}) \geq 1 - \frac{1}{2^m}. \quad (\text{П4.32})$$

Доказательство. Покажем, что

$$p(r \text{ нечетное или } x^{r/2} = -1 \pmod{N}) \leq \frac{1}{2^m}. \quad (\text{П4.33})$$

Согласно китайской теореме об остатках, выбор случайного числа x с равномерно распределенной по множеству \mathbb{Z}_N^* вероятностью равносителен выбору чисел x_j с равномерно распределенными по множествам $\mathbb{Z}_{p_j^{\alpha_j}}^*$ вероятностями

(при условии $x = x_j \pmod{p_j^{\alpha_j}}$ для всех j). Пусть r_j — порядок элемента x_j по модулю $p_j^{\alpha_j}$. Пусть 2^{d_j} — максимальная степень числа 2, которая делит r_j , а 2^d — максимальная степень числа 2, которая делит r . Рассмотрим следующее условие: r нечетно или $x^{r/2} = -1 \pmod{N}$. Покажем, что для его выполнения необходимо, чтобы d_j принимало одно и то же значение для всех j . Отсюда будет следовать утверждение теоремы, поскольку, согласно лемме П4.12, вероятность выполнения вышеуказанного условия не меньше $1/2^m$.

Сначала рассмотрим случай нечетного r . Легко заметить, что $r_j | r$ для всех j , поэтому r_j нечетно, т. е. $d_j = 0$ для всех $i = 1, \dots, k$. Второй и последний случай — r четно и $x^{r/2} = -1 \pmod{N}$. Тогда $x^{r/2} = -1 \pmod{p_j^{\alpha_j}}$, т. е. $r_j \nmid (r/2)$. Поскольку $r_j | r$, то $d_j = d$ для всех j . ■

На основе теорем П4.11 и П4.13 можно построить алгоритм, который с большой вероятностью находит нетривиальный делитель составного числа N . С помощью классического компьютера могут быть эффективно выполнены все шаги этого алгоритма, кроме (по крайней мере, так считается на данный момент) «подпрограммы» нахождения порядка. Повторяя алгоритм достаточно

число раз, мы разложим число N на простые множители. Полное описание алгоритма приводится ниже.

1. Если N четное, выдать делитель 2.
2. Определить (с использованием упр. 5.17), имеет ли число N вид a^b для целых чисел $a \geq 1$ и $b \geq 2$; если имеет, то выдать делитель a .
3. Выбрать случайное число x в диапазоне от 1 до $(N-1)$. Если $\text{НОД}(x, N) > 1$, выдать делитель $\text{НОД}(x, N)$.
4. Найти порядок r элемента x по модулю N (используя процедуру нахождения порядка).
5. Если r четное и $x^{r/2} \neq -1 \pmod{N}$, то вычислить $\text{НОД}(x^{r/2} - 1, N)$ и $\text{НОД}(x^{r/2} + 1, N)$. Проверить, какое из этих двух чисел является нетривиальным делителем, и выдать это число. В противном случае алгоритм не дает результата.

Шаги 1 и 2 данного алгоритма либо выдают делитель, либо сообщают, что N является нечетным числом с более чем одним простым делителем. Для выполнения этих шагов требуется $O(1)$ и $O(L^3)$ операций соответственно. Шаг 3 либо выдает делитель, либо выбирает случайный элемент x из Z_N^* . Шаг 4 вызывает процедуру нахождения порядка элемента, вычисляя порядок r элемента x по модулю N . Шаг 5 завершает алгоритм, поскольку в соответствии с теоремой П4.13, с вероятностью не менее $1/2$ число r четно и при этом $x^{r/2} \neq -1 \pmod{N}$, а теорема П4.11 утверждает, что либо $\text{НОД}(x^{r/2} - 1, N)$, либо $\text{НОД}(x^{r/2} + 1, N)$ является нетривиальным делителем числа N .

Упражнение П4.17 (сведение нахождения порядка к разложению на простые множители). Выше было доказано, что, умея быстро находить порядок элемента, можно быстро разложить числа на простые множители. Покажите, что эффективный алгоритм разложения на простые множители позволяет эффективно находить порядок по модулю N любого взаимно простого с N числа x .

П4.4 Цепные дроби

Здесь будет дано небольшое введение в теорию *цепных дробей*. Эта тема имеет существенное значение для применения быстрых квантовых алгоритмов нахождения порядка и разложения на простые множители, описанных в гл. 5.

В качестве примера цепной дроби рассмотрим число s , определяемое выражением

$$s \equiv \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \dots}}}. \quad (\text{П4.34})$$

При неформальном подходе можно написать уравнение $s = 1/(2 + s)$, откуда следует, что $s = \sqrt{2} - 1$. Идея метода цепных дробей заключается в описании действительных чисел только с помощью целых, используя выражения,

аналогичные (П4.34). *Конечная цепная дробь* определяется конечным набором целых положительных чисел a_0, \dots, a_N ,

$$[a_0, \dots, a_N] \equiv a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots + \frac{1}{a_N}}}}. \quad (\text{П4.35})$$

Будем называть n -й подходящей дробью ($0 \leq n \leq N$) к этой цепной дроби набор $[a_0, \dots, a_n]$.

Теорема П4.14. Пусть x — рациональное число, не меньшее единицы. Тогда существует представление числа x в виде цепной дроби: $x = [a_0, \dots, a_N]$, которое может быть найдено с помощью алгоритма нахождения цепных дробей, построенного на основе алгоритма Евклида.

Доказательство. Идею цепных дробей легче всего понять на конкретном примере. Найдем представление числа $31/13$ в виде цепной дроби. Первый шаг алгоритма заключается в выделении в числе $31/13$ целой и дробной частей:

$$\frac{31}{13} = 2 + \frac{5}{13}. \quad (\text{П4.36})$$

Далее мы переносим дробную часть в знаменатель:

$$\frac{31}{13} = 2 + \frac{1}{\frac{13}{5}}. \quad (\text{П4.37})$$

Эти операции — выделение целой и дробной частей и перенос дробной части в знаменатель — теперь применим к дроби $13/5$:

$$\frac{31}{13} = 2 + \frac{1}{2 + \frac{3}{5}} = 2 + \frac{1}{2 + \frac{1}{\frac{5}{3}}}. \quad (\text{П4.38})$$

Далее выполним эти операции применительно к дроби $5/3$:

$$\frac{31}{13} = 2 + \frac{1}{2 + \frac{1}{1 + \frac{2}{3}}} = 2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{\frac{3}{2}}}}. \quad (\text{П4.39})$$

На этом шаге разложение в цепную дробь заканчивается, поскольку $3/2 = 1 + 1/2$, в слагаемом $1/2$ в числитеle стоит единица, и перенос этой дробной части в знаменатель не требуется. Окончательное представление числа $31/13$ в виде цепной дроби выглядит следующим образом:

$$\frac{31}{13} = 2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{2}{3}}}}. \quad (\text{П4.40})$$

Ясно, что алгоритм нахождения цепной дроби завершится после конечного числа шагов «разбиения на целую и дробную части и переноса дробной части

в знаменатель», поскольку числители (в нашем примере 31, 3, 2, 1) образуют последовательность убывающих целых положительных чисел. Как быстро алгоритм завершит свое выполнение? Этот вопрос будет рассмотрен ниже. ■

Доказанная выше теорема относилась к числам $x \geq 1$; на практике удобно отказаться от условия $a_0 > 0$ и допустить, чтобы число a_0 принимало любые целые значения, что сделает ограничение $x \geq 1$ излишним. В частности, если x лежит в диапазоне от 0 до 1 (что характерно для применений в квантовых алгоритмах), то в разложении в цепную дробь число a_0 будет равно нулю.

Алгоритм разложения в цепную дробь дает однозначный способ нахождения цепной дроби для заданного рационального числа. Неопределенность может возникнуть только на последнем шаге, поскольку целое число можно представить двумя разными способами: $a_n = a_n$ или $a_n = (a_n - 1) + 1/1$, что дает два разных представления в виде цепной дроби. Эта неопределенность очень важна, поскольку при этом можно считать, что в разложении рационального числа содержится либо четное, либо нечетное число «этажей». Тогда в зависимости от требований задачи можно выбирать дробь с четным или нечетным числом «этажей».

Упражнение П4.18. Выпишите разложение в виде цепных дробей для чисел $x = 19/17$ и $x = 77/65$.

Теорема П4.15. Пусть a_0, \dots, a_N — последовательность положительных чисел. Тогда

$$[a_0, \dots, a_n] = \frac{p_n}{q_n}, \quad (\text{П4.41})$$

где p_n и q_n — действительные числа, определяемые по индукции следующим образом: $p_0 \equiv a_0$, $q_0 \equiv 1$, $p_1 \equiv 1 + a_0 a_1$, $q_1 \equiv a_1$,

$$p_n \equiv a_n p_{n-1} + p_{n-2}, \quad (\text{П4.42})$$

$$q_n \equiv a_n q_{n-1} + q_{n-2}, \quad (\text{П4.43})$$

где $2 \leq n \leq N$. В случае, когда все a_j — целые положительные числа, таковыми же являются все числа p_j и q_j .

Доказательство. Проведем индукцию по n . Утверждение легко проверяется для $n = 0, 1, 2$. По определению, для $n \geq 3$ имеем

$$[a_0, \dots, a_n] = [a_0, \dots, a_{n-2}, a_{n-1} + 1/a_n]. \quad (\text{П4.44})$$

Применим предположение индукции. Введем обозначение \tilde{p}_j/\tilde{q}_j для последовательности подходящих дробей цепной дроби в правой части равенства (П4.41):

$$[a_0, \dots, a_{n-2}, a_{n-1} + 1/a_n] = \frac{\tilde{p}_{n-1}}{\tilde{q}_{n-1}}. \quad (\text{П4.45})$$

Очевидно, что $\tilde{p}_{n-3} = p_{n-3}$, $\tilde{p}_{n-2} = p_{n-2}$ и $\tilde{q}_{n-3} = q_{n-3}$, $\tilde{q}_{n-2} = q_{n-2}$, поэтому

$$\frac{\tilde{p}_{n-1}}{\tilde{q}_{n-1}} = \frac{(a_{n-1} + 1/a_n)p_{n-2} + p_{n-3}}{(a_{n-1} + 1/a_n)q_{n-2} + q_{n-3}} \quad (\text{П4.46})$$

$$= \frac{p_{n-1} + p_{n-2}/a_n}{q_{n-1} + q_{n-2}/a_n}. \quad (\text{П4.47})$$

Умножая числитель и знаменатель правой части на a_n , обнаруживаем, что

$$\frac{\tilde{p}_{n-1}}{\tilde{q}_{n-1}} = \frac{p_n}{q_n}. \quad (\text{П4.48})$$

Из уравнений (П4.48), (П4.44) и (П4.45) следует равенство

$$[a_0, \dots, a_n] = \frac{p_n}{q_n}, \quad (\text{П4.49})$$

что и требовалось доказать. ■

Упражнение П4.19. Покажите, что $q_n p_{n-1} - p_n q_{n-1} = (-1)^n$ для $n \geq 1$. Докажите (используя этот факт), что $\text{НОД}(p_n, q_n) = 1$. (*Указание:* примените индукцию по n .)

Насколько много значений a_n необходимо вычислить, чтобы получить разложение в цепную дробь для рационального числа $x = p/q > 1$, где p и q — взаимно простые числа? Пусть a_0, \dots, a_N — положительные целые числа. Из определения чисел p_n и q_n следует, что p_n и q_n образуют возрастающие последовательности. Поэтому $p_n = a_n p_{n-1} + p_{n-2} \geq 2p_{n-2}$ (аналогично $q_n \geq 2q_{n-2}$), а следовательно, $p_n, q_n \geq 2^{\lfloor n/2 \rfloor}$ (где выражение $\lfloor x \rfloor$ обозначает целую часть числа x). Значит, $2^{\lfloor N/2 \rfloor} \leq q \leq p$, т. е. $N = O(\log p)$. А следовательно, если $x = p/q$ — рациональное число и числа p и q записываются с помощью L бит каждое, то разложение числа x в цепную дробь может быть вычислено за $O(L^3)$ операций: $O(L)$ операций «выделения целой и дробной частей и переноса дробной части в знаменатель», каждая из которых требует $O(L^2)$ элементов для простейших арифметических операций.

Теорема П4.16. Пусть x — рациональное число, а p/q — такое рациональное число, что

$$\left| \frac{p}{q} - x \right| \leq \frac{1}{2q^2}. \quad (\text{П4.50})$$

Тогда p/q — некоторая подходящая дробь для числа x .

Доказательство. Пусть $[a_0, \dots, a_n]$ — разложение в виде цепной дроби для числа p/q . Определим p_j и q_j , как в теореме П4.15, причем $p_n/q_n = p/q$. Зададим число δ соотношением

$$x \equiv \frac{p_n}{q_n} + \frac{\delta}{2q_n^2} \quad (\text{П4.51})$$

(очевидно, что $|\delta| < 1$). Определим число λ соотношением

$$\lambda \equiv 2 \left(\frac{q_n p_{n-1} - p_n q_{n-1}}{\delta} \right) - \frac{q_{n-1}}{q_n}. \quad (\text{П4.52})$$

Из определения числа λ следует, что

$$x = \frac{\lambda p_n + p_{n-1}}{\lambda q_n + q_{n-1}}, \quad (\text{П4.53})$$

а следовательно, $x = [a_0, \dots, a_n, \lambda]$. Сделав n четным числом, с учетом упр. П4.19 легко убедиться в справедливости равенства

$$\lambda = \frac{2}{\delta} - \frac{q_{n-1}}{q_n}. \quad (\text{П4.54})$$

Поскольку числа q_n образуют возрастающую последовательность, имеем

$$\lambda = \frac{2}{\delta} - \frac{q_{n-1}}{q_n} > 2 - 1 > 1. \quad (\text{П4.55})$$

Следовательно, λ — рациональное число, большее единицы, поэтому его можно представить в виде конечной цепной дроби $\lambda = [b_0, \dots, b_m]$, т. е. $x = [a_0, \dots, a_n, b_0, \dots, b_m]$ — конечная цепная дробь, а p/q — подходящая дробь для этой цепной дроби. ■

Задача П4.1 (оценка количества простых чисел). Пусть $\pi(n)$ — количество простых чисел, меньших n . Утверждение, известное как *асимптотический закон распределения простых чисел* (доказательство которого весьма нетривиально) гласит, что $\lim_{n \rightarrow \infty} \pi(n) \ln n / n = 1$, а следовательно, $\pi(n) \approx n / \ln n$. Данная задача является более слабым аналогом теоремы о простых числах и дает неплохую нижнюю оценку для количества простых чисел.

1. Докажите, что $n \leq \log \binom{2n}{n}$.

2. Покажите, что

$$\log \binom{2n}{n} \leq \sum_{p \leq 2n} \left\lfloor \frac{\log 2n}{\log p} \right\rfloor \log p, \quad (\text{П4.56})$$

где суммирование ведется по всем простым p , не превосходящим $2n$.

3. Используя два предыдущих пункта, покажите, что

$$\pi(2n) \geq \frac{n}{\log 2n} \quad (\text{П4.57})$$

История и дополнительная литература

По теории чисел написано много превосходных учебников. Мы существенно использовали материал из книги Коблитца [227], которая содержит начальные сведения как по теории чисел, так и по алгоритмам и криптографии. Глава 33 книги Кормена, Лейзерсона и Ривеста [92] (представляющей собой всесторонний труд, посвященный, в основном, алгоритмам) содержит схожую подборку вводных курсов. Введение в теорию цепных дробей в данном приложении базируется на гл. 10 классического учебника по теории чисел [195]. Задача П4.4 взята из работы [312].

Приложение 5

КРИПТОГРАФИЯ С ОТКРЫТЫМ КЛЮЧОМ И СИСТЕМА RSA

Криптография — это искусство тайного общения двух лиц. Например, если клиент собирается сделать покупку с помощью Интернета, он хотел бы передать номер своей кредитной карты по сети так, чтобы его узнала только та компания, где он делает покупку. Приведем более жесткий пример: во время войны каждая из воюющих сторон хочет иметь возможность конфиденциального общения. Для обеспечения этого используется *криптографический протокол*, или *крипtosистема*. Эффективная крипtosистема позволяет двум сторонам взаимодействовать, делая при этом «подслушивание» со стороны затруднительным.

Очень важным классом крипtosистем являются *крипtosистемы с открытым ключом*. Основная идея шифрования с открытым ключом проиллюстрирована на рис. П5.1. Алиса устанавливает почтовый ящик, обладающий следующими свойствами: *любой человек* может оставить сообщение для нее, но только она может забрать почту из ящика. Чтобы обеспечить такую возможность, в ящике предусмотрены две дверцы. На крышке ящика имеется закрывающаяся входная дверца, и любой, кто может ее открыть, может бросить письмо в ящик. Но эта щель «односторонняя», т. е. через нее нельзя вынуть почту из ящика. Алиса предоставляет ключ от верхней щели всем — это *открытый ключ*, т. е. она может получать почту *от любого человека*. На передней стенке ящика имеется вторая дверца, через которую можно достать находящуюся внутри почту. Единственный ключ от этой дверцы находится у Алисы — это ее *секретный ключ*. Такая система с двумя ключами — открытым и секретным — позволяет любому желающему передавать Алисе конфиденциальные сообщения.

Криптографические системы с открытым ключом работают по схожим правилам. Предположим, Алиса хочет получать сообщения, используя такую систему. Она должна создать два *криптографических ключа*: *открытый P* и *секретный S*. Конкретный вид этих ключей зависит от особенностей используемой криптографической системы. В некоторых криптографических системах в качестве ключей используются простые объекты, например, числа, в других — более сложные математические объекты, такие, как эллиптические кривые. После того как Алиса создала свои ключи, она «публикует» открытый ключ, т. е. предоставляет доступ к нему всем желающим.

Пусть теперь Боб хочет послать Алисе конфиденциальное сообщение. Сначала он получает созданный Алисой открытый ключ *P*, потом *шифрует* сообщение, предназначенное для отправки Алисе, с помощью этого открытого клю-

ча. Способ шифрования зависит от устройства конкретной криптографической системы. Принципиальный момент заключается в том, что для обеспечения защиты информации (невозможности «подслушивания») необходимо, чтобы расшифровку было трудно выполнить, даже используя открытый ключ. Это похоже на верхнюю дверцу в описанном выше почтовом ящике: если сообщение уже положено в ящик, его невозможно забрать, даже если у вас есть ключ от верхней дверцы. Поскольку «подслушивающему» лицу доступны только открытый ключ и зашифрованное сообщение, оно не сможет восстановить исходное сообщение. У Алисы же имеется дополнительная информация — секретный ключ S . Последний определяет второе преобразование, которое применяется к зашифрованному сообщению. Такое преобразование называют *десифрованием* — это действие, обратное шифрованию. Оно позволяет Алисе восстановить исходное сообщение.

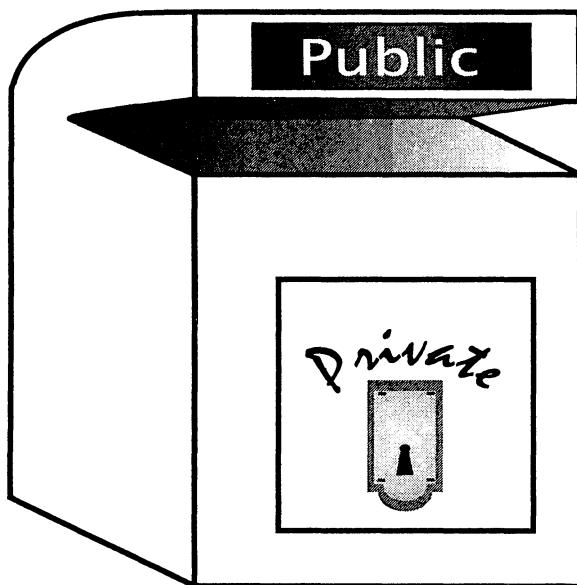


Рис. П5.1. Реализация идеи криптографии с открытым ключом По существу эта же схема реализована почтовыми службами во многих странах

Мы описали принцип действия криптографии с открытым ключом в идеальном случае. К сожалению, к моменту написания данной книги неизвестно, существуют ли подобные надежно защищенные схемы, позволяющие осуществлять шифрование с открытым ключом. Известно лишь несколько схем, которые считают достаточно надежными — их регулярно используют на практике, например, при продаже товаров через Интернет. Однако это не означает, что доказана высокая степень защиты таких схем. Считаются, что эти схемы обладают хорошей защитой от несанкционированного доступа потому, что были приложены (безрезультатно!) огромные усилия для их «взлома». Из крипто-

графических систем с открытым ключом наиболее широкое распространение получила система RSA (ее название образовано от инициалов создателей — Ривеста, Шамира и Адлемана). Предполагаемая конфиденциальность системы RSA опирается, как мы увидим, на очевидную сложность разложения числа на простые множители на классическом компьютере. Для понимания работы этой системы требуется знание основ теории чисел (см. разд. П4.1 и П4.2 Приложения 4).

Чтобы создать открытый и секретный ключи для использования в RSA-крипtosистеме, Алиса должна выполнить следующие действия.

1. Выбрать два больших простых числа p и q .
2. Вычислить их произведение $n \equiv pq$.
3. Выбрать случайным образом небольшое нечетное целое число e , взаимно-простое с $\varphi(n) = (p - 1)(q - 1)$.
4. Вычислить число d , являющееся мультипликативным обратным к e по модулю $\varphi(n)$.
5. Открытым RSA-ключом будет пара $P = (e, n)$, секретным RSA-ключом — пара $S = (d, n)$.

Пусть теперь Боб хочет зашифровать сообщение M с использованием открытого ключа P , чтобы отправить зашифрованное сообщение Алисе. Будем считать, что сообщение M содержит не более $\lfloor \log n \rfloor$ бит (более длинные сообщения можно разбить на блоки длиной $\lfloor \log n \rfloor$ бит и отправлять по очереди). Шифрование сообщения состоит в вычислении величины

$$E(M) = M^e \pmod{n}. \quad (\text{П5.1})$$

$E(M)$ и будет зашифрованным вариантом сообщения M , который Боб передаст Алисе. Алиса сможет быстро дешифровать сообщение, используя свой секретный ключ $S = (d, n)$, для этого нужно просто возвести сообщение в d -ю степень:

$$E(M) \rightarrow D(E(M)) = E(M)^d \pmod{n}. \quad (\text{П5.2})$$

Докажем, что при такой операции действительно получится исходное сообщение. В самом деле, $ed = 1 \pmod{\varphi(n)}$, а следовательно, $ed = 1 + k\varphi(n)$ с некоторым целым k . Рассмотрим два случая. В первом число M — взаимно простое с n . Как следует из теоремы Эйлера (П4.9), обобщающей малую теорему Ферма, $M^{k\varphi(n)} = 1 \pmod{n}$, поэтому

$$D(E(M)) = E(M)^d \pmod{n} \quad (\text{П5.3})$$

$$= M^{ed} \pmod{n} \quad (\text{П5.4})$$

$$= M^{1+k\varphi(n)} \pmod{n} \quad (\text{П5.5})$$

$$= M \cdot M^{k\varphi(n)} \pmod{n} \quad (\text{П5.6})$$

$$= M \pmod{n}, \quad (\text{П5.7})$$

т. е. в этом случае Алиса действительно получает исходное сообщение. Во втором случае число M не является взаимно простым с n , так что M делится хотя бы на одно из двух чисел p и q . Для определенности будем считать, что M делится на p и не делится на q (остальные случаи рассматриваются аналогично). Поскольку p делит M , выполняется равенство $M \equiv 0 \pmod{p}$, а значит, $M^{ed} \equiv 0 \equiv M \pmod{p}$. Поскольку q не делит M , согласно малой теореме Ферма получим, что $M^{q-1} \equiv 1 \pmod{q}$, а следовательно, $M^{\varphi(n)} \equiv 1 \pmod{q}$, поскольку $\varphi(n) = (p-1)(q-1)$. Из равенства $ed = 1 + k\varphi(n)$ следует, что $M^{ed} \equiv M \pmod{q}$. Согласно китайской теореме об остатках, $M^{ed} \equiv M \pmod{n}$, поэтому во втором случае (когда числа M и n не являются взаимно простыми) в результате дешифрования также получается исходное сообщение.

Упражнение П5.1. Выполните самостоятельно шифрование с использованием системы RSA. Закодируйте слово «КВАНТОВЫЙ», взяв $p = 3$, $q = 11$ (если пронумеровать буквы от 0 до 31, исключив букву «ё», то каждую букву можно записать пятью битами; для каждой буквы отдельно вычисляется ее зашифрованный «образ»; подходящие значения для e и d выберите самостоятельно).

Насколько эффективно может быть реализована система RSA? Существуют две проблемы. Первая — создание открытых и секретных ключей для криптографических систем. Если этот процесс не выполняется эффективно, RSA плохо подходит для практического использования. Узким местом здесь является «генерирование» простых чисел p и q . На практике используется следующий метод: выбирается произвольное число требуемой длины, а затем проверяется, является ли это число простым или составным. Имеются быстрые способы проверки простых чисел, например тест Миллера–Рабина, с помощью которого примерно за $O(L^3)$ операций выясняется, является ли число простым (здесь L — длина ключа). Если выясняется, что число составное, процедура повторяется еще один или несколько раз — пока не будет выбрано простое число. Из оценки количества простых чисел (см. задачу П4.1) следует, что вероятность для числа из L бит быть простым примерно равна $1/\log(2^L) = 1/L$, поэтому с большой вероятностью за $O(L)$ попыток можно найти простое число. Таким образом, всего потребовалось $O(L^4)$ операций.

Рассмотрим теперь эффективность шифрования и дешифрования при использовании системы RSA. Мы используем возведение в степень в арифметике остатков, которое, как известно, требует $O(L^3)$ операций (см. вставку 5.2). Таким образом, все операции, необходимые для шифрования с помощью системы RSA, могут быть быстро выполнены на классическом компьютере, и при достаточно скромных вычислительных мощностях можно работать с ключами длиной в тысячи битов.

Как можно взломать систему RSA? Опишем ниже два метода, которые дают надежду на взлом системы RSA: в первом используется нахождение порядка элемента, во втором — разложение числа на множители. Пусть Ева прочитала зашифрованное сообщение $M^e \pmod{n}$ и ей известен открытый ключ (e, n) , использованный при шифровании сообщения. Предположим, она может находить порядок зашифрованного сообщения, т. е. такое наименьшее положитель-

ное число r , что $(M^e)^r = 1 \pmod{n}$. (Не ограничивая общности, можно считать, что такое число существует, т. е. что число M^e — взаимно простое с n . В противном случае у чисел $M^e \pmod{n}$ и n имеется общий делитель, который можно найти с помощью алгоритма Евклида, после чего система RSA может быть взломана, как это описывается ниже для второго метода.) Согласно упр. П4.16, r делит $\varphi(n)$. Поскольку e взаимно простое с $\varphi(n)$, оно должно также быть взаимно простым и с r , а следовательно, иметь мультипликативный обратный элемент по модулю r (обозначим его d'). Это означает, что $ed' = 1 + kr$ для некоторого целого k . Тогда Ева может восстановить исходное сообщение M , возведя зашифрованное сообщение в d' -ю степень:

$$(M^e)^{d'} \pmod{n} = M^{1+kr} \pmod{n} \quad (\text{П5.8})$$

$$= M \cdot M^{kr} \pmod{n} \quad (\text{П5.9})$$

$$= M \pmod{n}. \quad (\text{П5.10})$$

Следует отметить, что Ева никогда не узнает секретный ключ (d, n) — ей известны только (d', n) . Конечно, числа d' и d тесно связаны, поскольку d' является обратным к e по модулю r , d — обратным к e по модулю $\varphi(n)$, а r делит $\varphi(n)$. Тем не менее наше объяснение показывает, что систему RSA можно взломать, не выясняя точного значения секретного ключа. Конечно, этот метод действует только в том случае, если Ева умеет эффективно находить порядок элемента, а к настоящему моменту такой алгоритм для классического компьютера неизвестен. Но с помощью квантового компьютера задача нахождения порядка может быть эффективно решена (это описано в разд. 5.3.1), поэтому система RSA может быть взломана.

Упражнение П5.2. Покажите, что d также является обратным элементом к e по модулю r , т. е. $d = d' \pmod{r}$.

Второй метод взлома системы RSA позволяет полностью определить секретный ключ. Пусть Ева умеет находить разложение числа n (вычислять p и q , произведение которых равно n). Следовательно, она может эффективно находить $\varphi(n) = (p-1)(q-1)$. После этого легко вычисляется d , являющееся обратным к e по модулю $\varphi(n)$. Таким образом, полностью определяется секретный ключ (d, n) . Видно, что если бы существовал быстрый способ разложения числа на простые множители, систему RSA было бы очень легко взломать.

Предполагаемая защита системы RSA опирается на тот факт, что для ее взлома требуется отыскать решение одной из двух задач, которые, как считается, трудно разрешить с помощью классического компьютера (хотя это и не доказано). Эти задачи — нахождение порядка элемента и разложение числа на множители. К сожалению, достоверно неизвестно даже, является ли система RSA надежно защищенной, если обе эти проблемы трудноразрешимы. (Может оказаться так, что обе указанные проблемы действительно сложны для решения на классическом компьютере, однако есть какой-то другой способ взлома системы RSA.) Несмотря на высказанное в течение двух с лишним десятилетий все попытки взлома системы RSA не привели к «успеху», и именно поэтому принято считать, что система RSA надежно защищена от взлома с использованием классического компьютера.

Задача П5.1.

Напишите программу на любом языке программирования, которая выполняет шифрование и дешифрование с использованием системы RSA. Найдите два 20-битовых простых числа и с их помощью закодируйте 40-битовое сообщение.

История и дополнительная литература

Криптографические системы с открытым ключом были придуманы Диффи и Хеллманом в 1976 г. [120], а также независимо Мерклом (примерно в то же время, хотя его работа была опубликована только в 1978 г. [280]). Вскоре после этого Ривест, Шамир и Адлеман [342] изобрели систему RSA. В 1997 г. было обнаружено, что эти идеи — криптография с открытым ключом, а также системы Диффи–Хелкмана и RSA — были на самом деле изобретены в конце 1960-х и начале 1970-х годов исследователями из Британской разведывательной службы GCHQ. Отчет об этих работах находится в Интернете по адресу: <http://www.cesg.gov.uk/about/nsecret/>. Проверки на простые числа (тесты Миллера–Рабина и Соловея–Штрассена) описаны в замечательной книге Коблица [227] по теории чисел и криптографии, содержащей также дополнительный материал по криптографии с открытым ключом. Эти способы проверки простоты чисел были первыми примерами вероятностных алгоритмов, более эффективных, чем соответствующие детерминированные. Алгоритм Соловея–Штрассена описан в [367], а алгоритм Миллера–Рабина — в работах [281] и [331].

Приложение 6

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ ЛИБА

Одним из самых важных и полезных результатов в теории обработки квантовой информации является *неравенство сильной субаддитивности* для энтропии фон Неймана: для трех квантовых систем A , B и C выполняется условие

$$S(A, B, C) + S(B) \leq S(A, B) + S(B, C). \quad (\text{П6.1})$$

К сожалению, наглядное доказательство этого факта неизвестно. В гл. 11 приведено достаточно простое доказательство с использованием так называемой *теоремы Либа*. В данном Приложении приводится ее доказательство. Начнем с обозначений.

Пусть $f(A, B)$ — действительнозначная функция матриц A и B . Функция f называется *совместно-вогнутой* по A и B , если для любого λ , удовлетворяющего условию $0 \leq \lambda \leq 1$, выполняется неравенство

$$f(\lambda A_1 + (1 - \lambda)A_2, \lambda B_1 + (1 - \lambda)B_2) \geq \lambda f(A_1, B_1) + (1 - \lambda)f(A_2, B_2). \quad (\text{П6.2})$$

Будем говорить, что $A \leq B$, если матрица $B - A$ является неотрицательно определенной. Соответственно $A \geq B$ означает, что $B \leq A$. Пусть A — произвольная матрица. Определим *норму* матрицы A следующим образом:

$$\|A\| = \max_{\langle u | u \rangle = 1} |\langle u | A | u \rangle|. \quad (\text{П6.3})$$

При доказательстве теоремы Либа понадобятся следующие легко проверяемые утверждения.

Упражнение П6.1 (отношение « \leq » сохраняется при сопряжении). Покажите, что если $A \leq B$, то $XAX^\dagger \leq XBX^\dagger$ для любой матрицы X .

Упражнение П6.2. Докажите, что $A \geq 0$ тогда и только тогда, когда A — неотрицательно определенный оператор.

Упражнение П6.3 (отношение « \leq » задает частичный порядок). Покажите, что отношение \leq задает частичный порядок на операторах, т. е. транзитивно ($A \leq B, B \leq C \implies A \leq C$), антисимметрично ($A \leq B, B \leq A \implies A = B$) и рефлексивно ($A \leq A$).

Упражнение П6.4. Пусть матрица A обладает собственными значениями λ_i . Обозначим максимальный элемент множества $|\lambda_i|$ буквой « λ ». Докажите, что

1. $\|A\| \geq \lambda$;
2. если матрица A эрмитова, то $\|A\| = \lambda$;

3. если

$$A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \quad (\text{П6.4})$$

то $\|A\| = 3/2 > 1 = \lambda$.

Упражнение П6.5. Докажите, что матрицы AB и BA имеют одинаковые собственные значения. (Указание: Докажите для обратимой матрицы A , что $\det(xI - AB) = \det(xI - BA)$, а следовательно, собственные значения матриц AB и BA одинаковые. По непрерывности это утверждение можно распространить и на случай необратимой матрицы A .)

Упражнение П6.6. Пусть матрицы A и B таковы, что AB — эрмитова матрица. Используя предыдущие два упражнения, покажите, что $\|AB\| \leq \|BA\|$.

Упражнение П6.7. Пусть A — неотрицательно определенная матрица. Покажите, что $\|A\| \leq 1$ тогда и только тогда, когда $A \leq I$.

Упражнение П6.8. Пусть A — неотрицательно определенная матрица. Определим супероператор (линейный оператор на множестве матриц) уравнением $\mathcal{A}(X) \equiv AX$. Покажите, что супероператор \mathcal{A} будет неотрицательно определенным относительно скалярного произведения Гильберта–Шмидта. (Это означает, что $\text{tr}(X^\dagger \mathcal{A}(X)) \geq 0$ для любого X .) Покажите аналогичным образом, что и супероператор, определяемый равенством $\mathcal{A}(X) \equiv XA$, будет неотрицательно определенным относительно скалярного произведения Гильберта–Шмидта.

Вооружившись этими фактами, можно приступить к формулировке и доказательству теоремы Либа.

Теорема П6.1 (теорема Либа). Пусть X — матрица, $0 \leq t \leq 1$. Тогда функция

$$f(A, B) \equiv \text{tr}(X^\dagger A^t X B^{1-t}) \quad (\text{П6.5})$$

является совместно вогнутой для неотрицательно определенных матриц A и B .

Теорема Либа легко выводится из следующей леммы.

Лемма П6.2. Пусть $R_1, R_2, S_1, S_2, T_1, T_2$ — такие неотрицательно определенные операторы, что $0 = [R_1, R_2] = [S_1, S_2] = [T_1, T_2]$ и

$$R_1 \geq S_1 + T_1, \quad (\text{П6.6})$$

$$R_2 \geq S_2 + T_2. \quad (\text{П6.7})$$

Тогда для любого t , удовлетворяющего условию $0 \leq t \leq 1$, выполняется следующее матричное неравенство:

$$R_1^t R_2^{1-t} \geq S_1^t S_2^{1-t} + T_1^t T_2^{1-t}. \quad (\text{П6.8})$$

Доказательство. Сначала докажем частный случай утверждения: $t = 1/2$, а потом используем этот случай для доказательства при произвольном t . Удобно

считать матрицы R_1 и R_2 обратимыми (доказательство в случае, когда хотя бы одна из матриц необратима, оставим читателю в качестве несложного упражнения — необходимо только немного модифицировать доказательство, приведенное ниже).

Пусть $|x\rangle$ и $|y\rangle$ — векторы. После двукратного применения неравенства Коши–Шварца и несложных преобразований получим, что

$$\begin{aligned} & |\langle x|(S_1^{1/2}S_2^{1/2} + T_1^{1/2}T_2^{1/2})|y\rangle| \\ & \leqslant |\langle x|S_1^{1/2}S_2^{1/2}|y\rangle| + |\langle x|T_1^{1/2}T_2^{1/2}|y\rangle| \end{aligned} \quad (\text{П6.9})$$

$$\leqslant \|S_1^{1/2}|x\rangle\| \|S_2^{1/2}|y\rangle\| + \|T_1^{1/2}|x\rangle\| \|T_2^{1/2}|y\rangle\| \quad (\text{П6.10})$$

$$\leqslant \sqrt{\left(\|S_1^{1/2}|x\rangle\|^2 + \|T_1^{1/2}|x\rangle\|^2\right) \left(\|S_2^{1/2}|y\rangle\|^2 + \|T_2^{1/2}|y\rangle\|^2\right)} \quad (\text{П6.11})$$

$$= \sqrt{\langle x|(S_1 + T_1)|x\rangle \langle y|(S_2 + T_2)|y\rangle}. \quad (\text{П6.12})$$

Согласно предположению, $S_1 + T_1 \leqslant R_1$, $S_2 + T_2 \leqslant R_2$, поэтому имеем

$$|\langle x|(S_1^{1/2}S_2^{1/2} + T_1^{1/2}T_2^{1/2})|y\rangle| \leqslant \sqrt{\langle x|R_1|x\rangle \langle y|R_2|y\rangle}. \quad (\text{П6.13})$$

Пусть $|u\rangle$ — произвольный вектор единичной длины. Применив формулу (П6.13) с $|x\rangle \equiv R_1^{-1/2}|u\rangle$ и $|y\rangle \equiv R_2^{-1/2}|u\rangle$, получим соотношения

$$\frac{\langle u|R_1^{-1/2}(S_1^{1/2}S_2^{1/2} + T_1^{1/2}T_2^{1/2})R_2^{-1/2}|u\rangle}{\leqslant \sqrt{\langle u|R_1^{-1/2}R_1R_1^{-1/2}|u\rangle \langle u|R_2^{-1/2}R_2R_2^{-1/2}|u\rangle}} \quad (\text{П6.14})$$

$$= \sqrt{\langle u|u\rangle \langle u|u\rangle} = 1, \quad (\text{П6.15})$$

следовательно,

$$\|R_1^{-1/2}(S_1^{1/2}S_2^{1/2} + T_1^{1/2}T_2^{1/2})R_2^{-1/2}\| \leqslant 1. \quad (\text{П6.16})$$

Введем следующие обозначения:

$$A \equiv R_1^{-1/4}R_2^{-1/4}(S_1^{1/2}S_2^{1/2} + T_1^{1/2}T_2^{1/2})R_2^{-1/2}, \quad (\text{П6.17})$$

$$B \equiv R_2^{1/4}R_1^{-1/4}. \quad (\text{П6.18})$$

Заметим, что AB — эрмитова матрица, поэтому из упр. П6.6 и предыдущих неравенств следует, что

$$\begin{aligned} & \|R_1^{-1/4}R_2^{-1/4}(S_1^{1/2}S_2^{1/2} + T_1^{1/2}T_2^{1/2})R_2^{-1/2}R_1^{-1/4}\| \\ & = \|AB\| \leqslant \|BA\| \end{aligned} \quad (\text{П6.19})$$

$$= \|R_1^{-1/2}(S_1^{1/2}S_2^{1/2} + T_1^{1/2}T_2^{1/2})R_2^{-1/2}\| \quad (\text{П6.20})$$

$$\leqslant 1, \quad (\text{П6.21})$$

где последнее неравенство непосредственно совпадает с (П6.16). Оператор AB является неотрицательно определенным, поэтому из упр. П6.7 и предыдущего неравенства следует соотношение

$$R_1^{-1/4} R_2^{-1/4} (S_1^{1/2} S_2^{1/2} + T_1^{1/2} T_2^{1/2}) R_2^{-1/4} R_1^{-1/4} \leq I. \quad (\text{П6.22})$$

Наконец, из упр. П6.1 и коммутативности матриц R_1 и R_2 получим

$$S_1^{1/2} S_2^{1/2} + T_1^{1/2} T_2^{1/2} \leq R_1^{1/2} R_2^{1/2}, \quad (\text{П6.23})$$

что означает справедливость неравенства (П6.8) при $t = 1/2$.

Пусть теперь I — множество всех чисел t , для которых выполняется неравенство (П6.8). Очевидно, что I содержит $t = 0$ и $t = 1$; кроме того, мы только что убедились, что $t = 1/2$ также принадлежит множеству I . Докажем теперь неравенство (П6.8) для произвольного t , лежащего в диапазоне от 0 до 1. Пусть числа μ и η принадлежат множеству I :

$$R_1^\mu R_2^{1-\mu} \geq S_1^\mu S_2^{1-\mu} + T_1^\mu T_2^{1-\mu}, \quad (\text{П6.24})$$

$$R_1^\eta R_2^{1-\eta} \geq S_1^\eta S_2^{1-\eta} + T_1^\eta T_2^{1-\eta}. \quad (\text{П6.25})$$

Легко видеть, что эта пара неравенств — частный случай пары неравенств (П6.6) и (П6.7). Согласно доказанному для случая $t = 1/2$, получим, что

$$\begin{aligned} (R_1^\mu R_2^{1-\mu})^{1/2} (R_1^\eta R_2^{1-\eta}) &\geq (S_1^\mu S_2^{1-\mu})^{1/2} (S_1^\eta S_2^{1-\eta})^{1/2} + \\ &+ (T_1^\mu T_2^{1-\mu})^{1/2} (T_1^\eta T_2^{1-\eta})^{1/2}. \end{aligned} \quad (\text{П6.26})$$

Используя коммутационные соотношения $0 = [R_1, R_2] = [S_1, S_2] = [T_1, T_2]$, обнаруживаем, что для $\nu \equiv (\mu + \eta)/2$ выполняется неравенство

$$R_1^\nu R_2^{1-\nu} \geq S_1^\nu S_2^{1-\nu} + T_1^\nu T_2^{1-\nu}. \quad (\text{П6.27})$$

Следовательно, если μ и η принадлежат множеству I , то и $(\mu + \eta)/2$ также принадлежит этому множеству. Поскольку 0 и 1 принадлежат I , легко видеть, что любое число от 0 до 1, представимое в виде конечной двоичной дроби, лежит в множестве I . Поэтому множество I всюду плотно на отрезке $[0, 1]$. Для завершения доказательства остается заметить, что выражения, входящие в формулу (П6.8), являются непрерывными функциями переменной t . ■

Доказательство теоремы Либа заключается в простом применении леммы П6.2. Ключевая идея состоит в выборе в качестве операторов в Лемме П6.2 *супероператоров* — линейных отображений операторов. Это следует сделать так, чтобы они были неотрицательно определенными относительного скалярного произведения $(A, B) \equiv \text{tr}(A^\dagger B)$.

Доказательство (теоремы Либа). Пусть $0 \leq \lambda \leq 1$. Определим супероператоры $\mathcal{S}_1, \mathcal{S}_2, \mathcal{T}_1, \mathcal{T}_2, \mathcal{R}_1, \mathcal{R}_2$ следующим образом:

$$\mathcal{S}_1(X) \equiv \lambda A_1 X, \quad (\text{П6.28})$$

$$\mathcal{S}_2(X) \equiv \lambda X B_1, \quad (\text{П6.29})$$

$$\mathcal{T}_1(X) \equiv (1 - \lambda) A_2 X, \quad (\text{П6.30})$$

$$\mathcal{T}_2(X) \equiv (1 - \lambda) X B_2, \quad (\text{П6.31})$$

$$\mathcal{R}_1(X) \equiv \mathcal{S}_1(X) + \mathcal{T}_1(X), \quad (\text{П6.32})$$

$$\mathcal{R}_2(X) \equiv \mathcal{S}_2(X) + \mathcal{T}_2(X). \quad (\text{П6.33})$$

Заметим, что операторы \mathcal{S}_1 и \mathcal{S}_2 коммутируют (также коммутируют пары \mathcal{T}_1 и \mathcal{T}_2 , \mathcal{R}_1 и \mathcal{R}_2). Согласно упр. П6.8, все эти операторы являются неотрицательно определенными в смысле скалярного произведения Гильберта–Шмидта. Согласно лемме П6.2, справедливо неравенство

$$\mathcal{R}_1^t \mathcal{R}_2^{1-t} \geq \mathcal{S}_1^t \mathcal{S}_2^{1-t} + \mathcal{T}_1^t \mathcal{T}_2^{1-t}. \quad (\text{П6.34})$$

Возьмем след от его обеих частей:

$$\operatorname{tr} [X^\dagger (\lambda A_1 + (1 - \lambda) A_2)^t X (\lambda B_1 + (1 - \lambda) B_2)^{1-t}]$$

$$\geq \operatorname{tr} [X^\dagger (\lambda A_1)^t X (\lambda B_1)^{1-t}] + \operatorname{tr} [X^\dagger ((1 - \lambda) A_2)^t X ((1 - \lambda) B_2)^{1-t}] \quad (\text{П6.35})$$

$$= \lambda \operatorname{tr}(X^\dagger A_1^t X B_1^{1-t}) + (1 - \lambda) \operatorname{tr}(X^\dagger A_2^t X B_2^{1-t}), \quad (\text{П6.36})$$

т. е. мы доказали утверждение о совместной вогнутости. ■

История и дополнительная литература

Теорема Либа связана с доказательством неравенства о сильной субаддитивности для квантовой энтропии; книги об истории данного вопроса перечислены в разд. «История и дополнительная литература» гл. 11.

СПИСОК ЛИТЕРАТУРЫ

Ссылки, обозначенные как “*arXive e-print quant-ph/xxxxxx*”, доступны по адресу в Интернете <http://www.arXiv.org>.

- [1] D. Aharonov and M. Ben-Or. Fault tolerant computation with constant error. In *Proceedings of the Twenty-Ninth Annual ACM Symposium on the Theory of Computing*, pages 176–188, 1997.
- [2] D. Aharonov and M. Ben-Or. Fault-tolerant quantum computation with constant error rate. *SIAM J. Comp.*, page to appear, 1999. *arXive e-print quant-ph/9906129*.
- [3] D. Aharonov, M. Ben-Or, R. Impagliazzo, and N. Nisan. Limitations of noisy reversible computation. *arXive e-print quant-ph/9611028*, 1996.
- [4] L. Adleman, J. Demarrais, and M. A. Huang. Quantum computability. *SIAM J. Comp.*, 26(5): 1524–1540, 1997.
- [5] Leonard M. Adleman. Molecular computation of solutions to combinatorial problems. *Science*; 266: 1021, 1994.
- [6] Leonard M. Adleman. Computing with DNA. *Sci. Am.*, 279: 54–61, Aug. 1998.
- [7] L. Allen and J. H. Eberly. *Optical Resonance and Two-level Atoms*. Dover, New York, 1975.
- [8] D. Aharonov. *Noisy Quantum Computation*. Ph. D. thesis, The Hebrew University, Jerusalem, 1999.
- [9] D. Aharonov. Quantum computation. In D. Stauffer, editor, *Annual Reviews of Computational Physics VI*. World Scientific, Singapore, 1999.
- [10] D. Aharonov, A. Kitaev, and N. Nisan. Quantum circuits with mixed states. *STOC 1997*, 1998. *arXive e-print quant-ph/9806029*.
- [11] H. Araki and E. H. Lieb. Entropy inequalities. *Comm. Math. Phys.*, 18: 160–170, 1970.
- [12] D. S. Abrams and S. Lloyd. Simulation of many-body Fermi systems on a quantum computer. *Phys. Rev. Lett.*, 79(13): 2586–2589, 1997. *arXive e-print quant-ph/9703054*.
- [13] A. Ashikhmin and S. Lytsin. Upper bounds on the size of quantum codes. *IEEE Trans. Inf. Theory*, 45(4): 1206–1215, 1999.
- [14] P. M. Alberti. A note on the transition-probability over c-* algebras. *Lett. in Math. Phys.*, 7(1): 25–32, 1983.
- [15] Andris Ambainis. Quantum lower bounds by quantum arguments. *arXive e-print quant-ph/0002066*, 2000.
- [16] T. Ando. Concavity of certain maps on positive definite matrices and applications to Hadamard products. *Linear Algebra Appl.*, 26: 203–241, 1979.

- [17] A. Ashikhmin. Remarks on bounds for quantum codes. *arXive e-print quant-ph/9705037*, 1997.
- [18] Edward Barton. A reversible computer using conservative logic. Unpublished MIT 6.895 term paper, 1978.
- [19] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, IEEE, New York, 1984. Bangalore, India, December 1984.
- [20] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *J. Cryptology*, 5: 3–28, 1992.
- [21] E. Biham, M. Boyer, G. Brassard, J. van de Graaf, and T. Mor. Security of quantum key distribution against all collective attacks. *arXive e-print quant-ph/9801022*, 1998.
- [22] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani. Strengths and weaknesses of quantum computing. *SIAM J. Comput.*, 26(5): 1510–1523, 1997. *arXive e-print quant-ph/9701001*.
- [23] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters. Teleporting an unknown quantum state via dual classical and EPR channels. *Phys. Rep. Lett.*, 70: 1895–1899, 1993.
- [24] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter. Elementary gates for quantum computation. *Phys. Rev. A*, 52: 3457–3467, 1995. *arXive e-print quant-ph/9503016*.
- [25] Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf. Quantum lower bounds by polynomials. In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS'98)*, pages 352–361, IEEE, Los Alamitos, California, November 1998. *arXive e-print quant-ph/9802049*.
- [26] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer. Generalized privacy amplification. *IEEE Trans. Inf. Theory*, 41: 1915–1923, 1995.
- [27] C. H. Bennett, G. Brassard, and A. K. Ekert. Quantum cryptography. *Sci. Am.*, 267(4): 50, Oct. 1992.
- [28] M. Boyer, G. Brassard, P. Hoyer, and A. Tapp. Tight bounds on quantum searching. *Fortsch. Phys. — Prog. Phys.*, 46(4–5): 493–505, 1998.
- [29] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu. Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein–Podolski–Rosen channels. *Phys. Rev. Lett.*, 80: 1121–1125, 1998. *arXive e-print quant-ph/9710013*.
- [30] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.*, 76: 722, 1996. *arXive e-print quant-ph/9511027*.

- [31] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher. Concentrating partial entanglement by local operations. *Phys. Rev. A*, 53(4): 2046–2052, 1996. *arXive e-print quant-ph/9511030*.
- [32] C. H. Bennett, G. Brassard, and J. M. Robert. Privacy amplification by public discussion. *SIAM J. Comp.*, 17: 210–229, 1988.
- [33] D. Beckman, A. N. Chari, S. Devabhaktuni, and J. Preskill. Efficient networks for quantum factoring. *Phys. Rev. A*, 54(2): 1034, 1996. *arXive e-print quant-ph/9602016*.
- [34] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher. Noncom-muting mixed states cannot be broadcast. *Phys. Rev. Lett.*, 76(15): 2828–2821, 1996. *arXive e-print quant-ph/9511010*.
- [35] S. L. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack. Separability of very noisy mixed states and implications for NMR quantum computing. *Phys. Rev. Lett.*, 83(5): 1054–1057, 1999.
- [36] G. K. Brennen, C. M. Caves, P. S. Jessen, and I. H. Deutsch. Quantum logic gates in optical lattices. *Physical Review Letters*, 82: 1060–1063, 1999.
- [37] Charles H. Bennett and David P. DiVincenzo. Quantum information and computation. *Nature*, 404: 247–55, 2000.
- [38] J. L. Balcazar, J. Diaz, and J. Gabarro. *Structural Complexity*, Volume I. Springer-Verlag, Berlin, 1988.
- [39] J. L. Balcazar, J. Diaz, and J. Gabarro. *Structural Complexity*, Volume II. Springer-Verlag, Berlin, 1988.
- [40] R. G. Brewer, R. G. DeVoe, and R. Kallenbach. Planar ion microtraps. *Phys. Rev. A*, 46(11): R6781–4, 1992.
- [41] C. H. Bennett, D. P. DiVincenzo, and J. A. Smolin. Capacities of quantum erasure channels. *Phys. Rev. Lett.*, 78(16): 3217–3220, 1997. *arXive e-print quant-ph/9701015*.
- [42] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed state entanglement and quantum error correction. *Phys. Rev. A*, 54: 3824, 1996. *arXive e-print quant-ph/9604024*.
- [43] John S. Bell. On the Einstein–Podolsky–Rosen paradox. *Physics*, 1: 195–200, 1964. Reprinted in J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics*, Cambridge University Press, Cambridge, 1987.
- [44] C. H. Bennett. Logical reversibility of computation. *IBM J. Res. Dev.*, 17(6): 525–32, 1973.
- [45] P. Benioff. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines, *J. Stat. Phys.*, 22(5): 563–591, 1980.
- [46] C. H. Bennett. The thermodynamics of computation — a review. *Int. J. Theor. Phys.*, 21: 905–40, 1982.
- [47] C. H. Bennett. Demons, engines and the second law. *Sci. Am.*, 295(5): 108, 1987.
- [48] C. H. Bennett. Time-space trade-offs for reversible computation. *SIAM J. Comput.*, 18: 766–776, 1989.

- [49] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68(21): 3121–3124, 1992.
- [50] Thomas Beth. *Methoden der Schnellen Fouriertransformation*. Teubner, Leipzig, 1984.
- [51] Samuel L. Braunstein, Christopher A. Fuchs, Daniel Gottesman, and Hoi-Kwong Lo. A quantum analog of Huffman coding. *arXive e-print quant-ph/9805080*, 1998.
- [52] H. Barnum, C. A. Fuchs, R. Jozsa, and B. Schumacher. General fidelity limit for quantum channels. *Phys. Rev. A*, 54: 4707, 1996. *arXive e-print quant-ph/9603014*.
- [53] R. Bhatia. *Matrix Analysis*. Springer-Verlag, New York, 1997.
- [54] G. Brassard, P. Hoyer, and A. Tapp. Quantum counting. *arXive e-print quant-ph/9805082*, 1998.
- [55] Y. B. Braginsky and F. Y. Khahili. *Quantum Measurement*. Cambridge University Press, Cambridge, 1992.
- [56] Samuel L. Braunstein and H. J. Kimble. Teleportation of continuous quantum variables. *Phys. Rev. Lett.*, 80: 869–72, 1998.
- [57] S. B. Bravyi and A. Y. Kitaev. Quantum codes on a lattice with boundary. *arXive e-print quant-ph/9811052*, 1998.
- [58] Samuel L. Braunstein and H. J. Kimble. Dense coding for continuous variables. *arXive e-print quant-ph/9910010*, 1999.
- [59] D. Bacon, J. Kempe, D. A. Lidar, and K. B. Whaley. Universal fault-tolerant computation on decoherence-free subspaces. *arXive e-print quant-ph/9909058*, 1999.
- [60] H. Barnum, E. Knill, and M. A. Nielsen. On quantum fidelities and channel capacities. *arXive e-print quant-ph/9809010*, 1998.
- [61] Daniel Boneh and Richard J. Lipton. Quantum cryptoanalysis of hidden linear functions (extended abstract). In Don Coppersmith, editor, *Lecture notes in computer science — Advances in Cryptology — CRYPTO'95*, pages 424–437, Springer-Verlag, Berlin, 1995.
- [62] P. Oscar Boykin, Tal Mor, Matthew Pulver, Ywani Roychowdhury, and Farrokh Yatan. On universal and fault-tolerant quantum computing. *arXive e-print quant-ph/9906054*, 1999.
- [63] H. Barnum, M. A. Nielsen, and B. W. Schumacher. Information transmission through a noisy quantum channel. *Phys. Rev. A*, 57: 4153, 1998.
- [64] D. Bohm. *Quantum Theory*. Prentice-Hall, Englewood Cliffs, New Jersey, 1951.
- [65] S. M. Barnett and S. J. D. Phoenix. Information-theoretic limits to quantum cryptography. *Phys. Rev. A*, 48(1): R5–R8, 1993.
- [66] D. Bouwmeester, J. W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger. Experimental quantum teleportation. *Nature*, 390(6660): 575–579, 1997.

- [67] D. S. Bethune and W. P. Risk. An autocompensating quantum key distribution system using polarization splitting of light. In *IQEC'98 Digest of Postdeadline Papers*, pages QPD12–2, Optical Society of America, Washington, DC, 1998.
- [68] Donald S. Bethune and William P. Risk. An autocompensating fiber-optic quantum cryptography system based on polarization splitting of light. *J. Quantum Electronics*, 36(3): 100, 2000.
- [69] G. Brassard. A bibliography of quantum cryptography. Université de Montréal preprint, pages 1–10, 3 December 1993. A preliminary version of this appeared in *Sigact News*, vol. 24(3), 1993, pages 16–20.
- [70] Samuel L. Braunstein. Error correction for continuous quantum variables. *Phys. Rev. Lett.*, 80: 4084–4087, 1998. *arXive e-print quant-ph/9711049*.
- [71] G. Brassard and L. Salvail. Secret-key reconciliation by public discussion. In T. Helleseth, editor, *Lecture Notes in Computer Science: Advances in Cryptology — EUROCRYPT'93*, Volume 765, pages 410–423, Springer-Verlag, New York, 1994.
- [72] C. H. Bennett and P. W. Shor. Quantum information theory, *itit*, 44(6): 2724–42, 1998.
- [73] H. Barnum, J. A. Smolin, and B. Terhal. Quantum capacity is properly defined without encodings. *Phys. Rev. A*, 58(5): 3496–3501, 1998.
- [74] B. M. Boghosian and W. Taylor. Simulating quantum mechanics on a quantum computer. *arXive e-print quant-ph/9701019*, 1997.
- [75] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM J. Comput.*, 26(5): 1411–1473, 1997. *arXive e-print quant-ph/9701001*.
- [76] C. H. Bennett and S. J. Wiesner. Communication via one- and two-particle operators on Einstein–Podolsky–Rosen states. *Phys. Rev. Lett.*, 69(20): 2881–2884, 1992.
- [77] N. J. Cerf, C. Adami, and P. Kwiat. Optical simulation of quantum logic. *Phys. Rev. A*, 57: R1477, 1998.
- [78] C. M. Caves. Quantum error correction and reversible operations. *Journal of Superconductivity*, 12(6): 707–718, 1999.
- [79] R. Cleve and D. P. DiVincenzo. Schumacher's quantum data compression as a quantum computation. *Phys. Rev. A*, 54: 2636, 1996. *arXive e-print quant-ph/9603009*.
- [80] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca. Quantum algorithms revisited. *Proc. R. Soc. London A*, 454(1969): 339–354, 1998.
- [81] D. G. Cory, A. F. Fahmy, and T. F. Havel. Ensemble quantum computing by NMR spectroscope. *Proc. Nat. Acad. Sci. USA*, 94: 1634–1639, 1997.
- [82] I. L. Chuang, N. Gershenfeld, and M. Kubinec. Experimental implementation of fast quantum searching. *Phys. Rev. Lett.*, 18(15): 3408–3411, 1998.
- [83] I. L. Chuang, N. Gershenfeld, M. G. Kubinec, and D. Y. Leung. Bulk quantum computation with nuclear-magnetic-resonance: theory and experiment. *Proc. R. Soc. London A*, 454(1969): 447–467, 1998.

- [84] P. R. Chernoff. Note on product formulas for operator semigroups. *J. Functional Analysis*, 2: 238–242, 1968.
- [85] M.-D. Choi. Completely positive linear maps on complex matrices. *Linear Algebra and Its Applications*, 10: 285–290, 1975.
- [86] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 49: 1804–1807, 1969.
- [87] A. Church. An unsolvable problem of elementary number theory. *Am. J. Math. (reprinted in [113])*, 58: 345, 1936.
- [88] I. Csiszár and J. Körner. *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Academic Press, New York, 1981.
- [89] A. O. Caldeira and A. J. Leggett. Quantum tunnelling in a dissipative system. *Ann. Phys.*, 149(2): 374–456, 1983.
- [90] M. Clausen. Fast generalized Fourier transforms. *Theor. Comput. Sci.*, 67: 55–63, 1989.
- [91] R. Cleve. The query complexity of order-finding. *arXive e-print quant-ph/9911124*, 1999.
- [92] T. H. Cormen, C. E. Leiserson, and R. L. Rivest. *Introduction to Algorithms*. MIT Press, Cambridge, Mass., 1990.
- [93] C. Cachin and U. M. Maurer. Linking information reconciliation and privacy amplification. *J. Cryptology*, 10: 97–110, 1997.
- [94] I. L. Chuang and D. Modha. Reversible arithmetic coding for quantum data compression. *IEEE Trans. Inf. Theory*, 46(3): 1104, May 2000.
- [95] D. G. Cory, W. Mass, M. Price, E. Knill, R. Laflamme, W. H. Zurek, T. F. Havel, and S. S. Somaroo. Experimental quantum error correction. *arXive e-print quant-ph/9802018*, 1998.
- [96] I. L. Chuang and M. A. Nielsen. Prescription for experimental determination of the dynamics of a quantum black box. *J. Mod. Opt.*, 44(11–12): 2455–2467, 1997. *arXive e-print quant-ph/9610001*.
- [97] J. H. Conway. Unpredictable iterations. In *Proceedings of the Number Theory Conference*, pages 49–52, Boulder, Colorado, 1972.
- [98] J. H. Conway. Fractran: a simple universal programming language. In T. M. Cover and B. Gopinath, editors, *Open Problems in Communication and Computation*, pages 4–26, Springer-Verlag, New York, 1986.
- [99] S. A. Cook. The complexity of theorem-proving procedures. In *Proc. 3rd Ann. ACM Symp. on Theory of Computing*, pages 151–158, Association for Computing Machinery, New York, 1971.
- [100] D. Coppersmith. An approximate Fourier transform useful in quantum factoring. *IBM Research Report RC 19642*, 1994.
- [101] J. I. Cirac, T. Pellizzari, and P. Zoller. Enforcing coherent evolution in dissipative quantum dynamics. *Science*, 273: 1207, 1996.
- [102] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction and orthogonal geometry. *Phys. Rev. Lett.*, 78: 405–8, 1997.

- [103] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over GF(4). *IEEE Trans. Inf. Theory*, 44(4): 1369–1387, 1998.
- [104] A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54: 1098, 1996. *arXive e-print quant-ph/9512032*.
- [105] R. A. Campos, B. E. A. Saleh, and M. C. Tiech. Quantum-mechanical lossless beamsplitters: SU(2) symmetry and photon statistics. *Phys. Rev. A*, 40: 1371, 1989.
- [106] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. John Wiley and Sons, New York, 1991.
- [107] C. Cohen-Tannoudji, B. Diu, and F. Laloë. *Quantum Mechanics, Vol. I*. John Wiley and Sons, New York, 1977.
- [108] C. Cohen-Tannoudji, B. Diu, and F. Laloë. *Quantum Mechanics, Vol. II*. John Wiley and Sons, New York, 1977.
- [109] I. L. Chuang, L. M. K. Vandersypen, X. L. Zhou, D. W. Leung, and S. Lloyd. Experimental realization of a quantum algorithm. *Nature*, 393(6681): 143–146, 1998.
- [110] H. F. Chau and F. Wilczek. Simple realization of the Fredkin gate using a series of two-body operators. *Phys. Rev. Lett.*, 75(4): 748–50, 1995. *arXive e-print quant-ph/9503005*.
- [111] I. L. Chuang and Y. Yamamoto. Simple quantum computer. *Phys. Rev. A*, 52: 3489–3496, 1995. *arXive e-print quant-ph/9505011*.
- [112] J. I. Cirac and P. Zoller. Quantum computations with cold trapped ions. *Phys. Rev. Lett.*, 74: 4091, 1995.
- [113] M. D. Davis. *The Undecidable*. Raven Press, Hewlett, New York, 1965.
- [114] E. B. Davies. *Quantum Theory of Open Systems*. Academic Press, London, 1976.
- [115] D. Deutsch, A. Barenco, and A. Ekert. Universality in quantum computation. *Proc. R. Soc. London A*, 449(1937): 669–677, 1995.
- [116] D. Deutsch. Uncertainty in quantum measurements. *Phys. Rev. Lett.*, 50(9): 631–633, 1983.
- [117] D. Deutsch. Quantum theory, the Church-Turing Principle and the universal quantum computer. *Proc. R. Soc. Lond. A*, 400: 97, 1985.
- [118] D. Deutsch. Quantum computational networks. *Proc. R. Soc. London A*, 425: 73, 1989.
- [119] L.-M. Duan and G.-C. Guo. Probabilistic cloning and identification of linearly independent quantum states. *Phys. Rev. Lett.*, 80: 4999–5002, 1998. *arXive e-print quant-ph/9804064*.
- [120] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Trans. Inf. Theory*, IT-22(6): 644–54, 1976.
- [121] C. Dürr and P. Hoyer. A quantum algorithm for finding the minimum. *arXive e-print quant-ph/9607014*, 1996.
- [122] D. Dieks. Communication by EPR devices. *Phys. Lett. A*, 92(6): 271–272, 1982.

- [123] D. P. DiVincenzo. Quantum computation. *Science*, 270: 255, 1995. *arXive e-print quant-ph/9503016*.
- [124] D. P. DiVincenzo. Two-bit gates are universal for quantum computation. *Phys. Rev. A*, 51(2): 1015–1022, 1995.
- [125] D. P. DiVincenzo. Quantum gates and circuits. *Proc. R. Soc. London A*, 454: 261–276, 1998.
- [126] D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. *Proc. R. Soc. London A*, 439: 553, 1992.
- [127] W. Diffie and S. Landau. *Privacy on the Line: the Politics of Wiretapping and Encryption*. MIT Press, Cambridge Massachusetts, 1998.
- [128] L. Davidovich, A. Maali, M. Brune, J. M. Raimond, and S. Haroche. *Phys. Rev. Lett.*, 71: 2360, 1993.
- [129] P. Diaconis and D. Rockmore. Efficient computation of the Fourier transform on finite groups. *J. Amer. Math. Soc.*, 3(2): 297–332, 1990.
- [130] L. Davidovich, J. M. Raimond, M. Brune, and S. Haroche. *Phys. Rev. A*, 36: 3771, 1987.
- [131] P. Domokos, J. M. Raimond, M. Brune, and S. Haroche. Simple cavity-QED two-bit universal quantum logic gate: The principle and expected performances. *Phys. Rev. Lett.*, 52: 3554, 1995.
- [132] D. P. DiVincenzo and P. W. Shor. Fault-tolerant error correction with efficient quantum codes. *Phys. Rev. Lett.*, 77: 3260, 1996.
- [133] D. P. DiVincenzo, P. W. Shor, and J. Smolin. Quantum-channel capacities of very noisy channels. *Phys. Rev. A*, 57(2): 830–839, 1998.
- [134] S. Earnshaw. On the nature of the molecular forces which regulate the constitution of the luminiferous ether. *Trans. Camb. Phil. Soc.*, 7: 97–112, 1842.
- [135] R. R. Ernst, G. Bodenhausen, and A. Wokaun. *Principles of Nuclear Magnetic Resonance in One and Two Dimensions*. Oxford University Press, Oxford, 1987.
- [136] M. Ettinger and P. Høyer. On quantum algorithms for noncommutative hidden subgroups. In *Symposium on Theoretical Aspects in Computer Science*. University of Trier, 1999. *arXive e-print quant-ph/9801029*.
- [137] M. Ettinger, P. Høyer, and E. Knill. Hidden subgroup states are almost orthogonal. *arXive e-print quant-ph/9901034*, 1999.
- [138] A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres. Eavesdropping on quantum-cryptographical systems. *Phys. Rev. A*, 50(2): 1047–1056, 1994.
- [139] A. Ekert and R. Jozsa. Quantum computation and Shor's factoring algorithm. *Rev. Mod. Phys.*, 68: 1, 1996.
- [140] A. Ekert and R. Jozsa. Quantum algorithms: Entanglement enhanced information processing. *Proc. R. Soc. London A*, 356(1743): 1769–82, Aug. 1998. *arXive e-print quant-ph/9803072*.
- [141] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67(6): 661–663, 1991.

- [142] A. Ekert and C. Macchiavello. Error correction in quantum communication. *Phys. Rev. Lett.*, 77: 2585, 1996. *arXive e-print quant-ph/9602022*.
- [143] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47: 777–780, 1935.
- [144] H. Epstein. *Commun. Math. Phys.*, 31: 317–325, 1973.
- [145] M. Fannes. A continuity property of the entropy density for spin lattice systems. *Commun. Math. Phys.*, 31: 291–294, 1973.
- [146] C. A. Fuchs and C. M. Caves. Ensemble-dependent bounds for accessible information in quantum mechanics. *Phys. Rev. Lett.*, 73(23): 3047–3050, 1994.
- [147] W. Feller. *An Introduction to Probability Theory and its Applications*, Volume 1. Wiley, New York, 1968.
- [148] W. Feller. *An Introduction to Probability Theory and its Applications*, Volume 2. Wiley, New York, 1968.
- [149] R. P. Feynman. Simulating physics with computers. *Int. J. Theor. Phys.*, 21: 467, 1982.
- [150] E. Farhi and S. Gutmann. An analog analogue of a digital quantum computation. *Phys. Rev. A*, 57(4): 2403–2406, 1998. *arXive e-print quant-ph/9612026*.
- [151] R. P. Feynman, R. B. Leighton, and M. Sands. Volume III of *The Feynman Lectures on Physics*. Addison-Wesley, Reading, Mass., 1965.
- [152] R. P. Feynman, R. B. Leighton, and M. Sands. Volume I of *The Feynman Lectures on Physics*. Addison-Wesley, Reading, Mass., 1965.
- [153] M. H. Freedman and D. A. Meyer. Projective plane and planar quantum codes. *arXive e-print quant-ph/9810055*, 1998.
- [154] A. Fässler and E. Stiefel. *Group Theoretical methods and Their Applications*. Birkhäuser, Boston, 1992.
- [155] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik. Unconditional quantum teleportation. *Science*, 282: 706–709, 1998.
- [156] E. Fredkin and T. Toffoli. Conservative logic. *Int. J. Theor. Phys.*, 21(3/4): 219–253, 1982.
- [157] C. A. Fuchs. *Distinguishability and Accessible Information in Quantum Theory*. Ph. D. thesis, The University of New Mexico, Albuquerque, NM, 1996. *arXive e-print quant-ph/9601020*.
- [158] C. A. Fuchs. Nonorthogonal quantum states maximize classical information capacity. *Phys. Rev. Lett.*, 79(6): 1162–1165, 1997.
- [159] C. W. Gardiner. *Quantum Noise*. Springer-Verlag, Berlin, 1991.
- [160] N. Gershenfeld and I. L. Chuang. Bulk spin resonance quantum computation. *Science*, 275: 350, 1997.
- [161] D. Gottesman and I. L. Chuang. Quantum teleportation is a universal computational primitive. *Nature*, 402: 390–392, 1999. *arXive e-print quant-ph/9908010*.

- [162] M. R. Garey and D. S. Johnson. *Computers and Intractability*. W. H. Freeman and Company, New York, 1979.
- [163] R. B. Griffiths and C.-S. Niu. Semiclassical Fourier transform for quantum computation. *Phys. Rev. Lett.*, 76(17): 3228–3231, 1996. *arXive e-print quant-ph/9511007*.
- [164] J. P. Gordon. Noise at optical frequencies; information theory. In P. A. Miles, editor. *Quantum Electronics and Coherent Light*, Proceedings of the International School of Physics ‘Enrico Fermi’ XXXI, Academic Press, New York, 1964.
- [165] D. Gottesman. Class of quantum error-correcting codes saturating the quantum Hamming bound. *Phys. Rev. A*, 54: 1862, 1996.
- [166] D. Gottesman. *Stabilizer Codes and Quantum Error Correction*. Ph. D. thesis, California Institute of Technology, Pasadena, CA, 1997.
- [167] D. Gottesman. Fault-tolerant quantum computation with higher-dimensional systems. *arXive e-print quant-ph/9802007*, 1998.
- [168] D. Gottesman. Theory of fault-tolerant quantum computation. *Phys. Rev. A*, 57(1): 127–137, 1998. *arXive e-print quant-ph/9702029*.
- [169] D. Gottesman and J. Preskill. The Hitchhiker’s guide to the threshold theorem. *Eternally in preparation*, 1: 1–9120, 2010.
- [170] L. Grover. In *Proc. 28th Annual ACM Symposium on the Theory of Computation*, pages 212–219, ACM Press, New York, 1996.
- [171] L. K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, 79(2): 325, 1997. *arXive e-print quant-ph/9706033*.
- [172] J. Gruska. *Quantum Computing*. McGraw-Hill, London, 1999.
- [173] G. R. Grimmett and D. R. Stirzaker. *Probability and Random Processes*. Clarendon Press, Oxford, 1992.
- [174] R. J. Hughes, D. M. Aide, P. Dyer, G. G. Luther, G. L. Morgan, and M. Schauer. Quantum cryptography. *Contemp. Phys.*, 36(3): 149–163, 1995. *arXive e-print quant-ph/9504002*.
- [175] P. R. Halmos. *Finite-dimensional Vector Spaces*. Van Nostrand, Princeton, N. J., 1958.
- [176] M. Hammermesh. *Group Theory and its Application to Physical Problems*. Dover, New York, 1989.
- [177] J. L. Hennessey, D. Goldberg, and D. A. Patterson. *Computer Architecture: A Quantitative Approach*. Academic Press, New York, 1996.
- [178] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A*, 223(1–2): 1–8, 1996.
- [179] M. Horodecki, P. Horodecki, and R. Horodecki. Mixed-state entanglement and distillation: is there a ‘bound’ entanglement in nature? *Phys. Rev. Lett.*, 80(24): 5239–5242, 1998.
- [180] M. Horodecki, P. Horodecki, and R. Horodecki. General teleportation channel, singlet fraction, and quasidistillation. *Phys. Rev. A*, 60(3): 1888–1898, 1999.

- [181] M. Horodecki, P. Horodecki, and R. Horodecki. Limits for entanglement measures. *arXive e-print quant-ph/9908065*, 1999.
- [182] P. Horodecki, M. Horodecki, and R. Horodecki. Bound entanglement can be activated. *Phys. Rev. Lett.*, 82(5): 1056–1059, 1999.
- [183] R. A. Horn and C. R. Johnson. *Matrix Analysis*. Cambridge University Press, Cambridge, 1985.
- [184] R. A. Horn and C. R. Johnson. *Topics in Matrix Analysis*. Cambridge University Press, Cambridge, 1991.
- [185] P. Horodecki, R. Jozsa, B. Schumacher, M. Westmoreland, and W. K. Wootters. Classical information capacity of a quantum channel. *Phys. Rev. A*, 54: 1869, 1996.
- [186] L. P. Hughston, R. Jozsa, and W. K. Wootters. A complete classification of quantum ensembles having a given density matrix. *Phys. Lett. A*, 183: 14–18, 1993.
- [187] K.-E. Hellwig and K. Kraus. Pure operations and measurements. *Commun. Math. Phys.*, 11: 214–220, 1969.
- [188] K.-E. Hellwig and K. Kraus. Operations and measurements. II. *Commun. Math. Phys.*, 16: 142–147, 1970.
- [189] D. R. Hofstadter. *Gödel, Escher, Bach: an Eternal Golden Braid*. Basic Books, New York, 1979.
- [190] A. S. Holevo. Statistical problems in quantum physics. In Gisiro Maruyama and Jurii V. Prokhorov, editors, *Proceedings of the Second Japan–USSR Symposium on Probability Theory*, pages 104–119, Springer-Verlag, Berlin, 1973. Lecture Notes in Mathematics, vol. 330.
- [191] A. S. Holevo. Capacity of a quantum communications channel. *Problems of Inf. Transm.*, 5(4): 247–253, 1979.
- [192] A. S. Holevo. The capacity of the quantum channel with general signal states. *IEEE Trans. Inf. Theory*, 44(1): 269–273, 1998.
- [193] M. Horodecki. Limits for compression of quantum information carried by ensembles of mixed states. *Phys. Rev. A*, 57: 3364–3369, 1997.
- [194] A. G. Huibers, M. Switkes, C. M. Marcus, K. Campman, and A. C. Gossard. Dephasing in open quantum dots. *Phys. Rev. Lett.*, 82: 200, 1998.
- [195] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*, Fourth Edition. Oxford University Press, London, 1960.
- [196] A. Imamoglu, D. D. Awschalom, G. Burkard, D. P. DiVincenzo, D. Loss, M. Sherwin, and A. Small. Quantum information processing using quantum dot spins and cavity qed. *Phys. Rev. Lett.*, 83(20): 4204–7, 1999.
- [197] A. Imamoglu and Y. Yamamoto. Turnstile device for heralded single photons: Coulomb blockade of electron and hole tunneling in quantum confined p-i-n heterojunctions. *Phys. Rev. Lett.*, 72(2): 210–13, 1994.
- [198] D. James. The theory of heating of the quantum ground state of trapped ions. *arXive e-print quant-ph/9804048*, 1998.
- [199] E. T. Jaynes. Information theory and statistical mechanics, ii. *Phys. Rev.*, 108(2): 171–190, 1957.

- [200] J. A. Jones and M. Mosca. Implementation of a quantum algorithm to solve Deutsch's problem on a nuclear magnetic resonance quantum computer. *arXive e-print quant-ph/9801027*, 1998.
- [201] J. A. Jones, M. Mosca, and R. H. Hansen. Implementation of a quantum search algorithm on a nuclear magnetic resonance quantum computer. *Nature*, 393(6683): 344, 1998. *arXive e-print quant-ph/9805069*.
- [202] K. R. W. Jones. Fundamental limits upon the measurement of state vectors. *Phys. Rev. A*, 50: 3682–3699, 1994.
- [203] R. Jozsa. Fidelity for mixed quantum states, *J. Mod. Opt.*, 41: 2315–2323, 1994.
- [204] R. Jozsa. Quantum algorithms and the Fourier transform. *arXive e-print quant-ph/9707033*, 1997.
- [205] D. Jonathan and M. B. Plenio. Entanglement-assisted local manipulation of pure states. *Phys. Rev. Lett.*, 83: 3566–3569, 1999.
- [206] R. Jozsa and B. Schumacher. A new proof of the quantum noiseless coding theorem. *J. Mod. Opt.*, 41: 2343–2349, 1994.
- [207] D. Kahn. *Codebreakers: the Story of Secret Writing*. Scribner, New York, 1996.
- [208] B. Kane. A silicon-based nuclear spin quantum computer. *Nature*, 393: 133–137, 1998.
- [209] R. M. Karp. Reducibility among combinatorial problems. In *Complexity of Computer Computations*, pages 85–103, Plenum Press, New York, 1972.
- [210] E. Knill, I. Chuang, and R. Laflamme. Effective pure states for bulk quantum computation. *Phys. Rev. A*, 57(5): 3348–3363, 1998. *arXive e-print quant-ph/9706053*.
- [211] A. Y. Kitaev. Quantum measurements and the Abelian stabilizer problem. *arXive e-print quant-ph/9511026*, 1995.
- [212] A. Y. Kitaev. Fault-tolerant quantum computation by anyons. *arXive e-print quant-ph/9707021*, 1997.
- [213] A. Y. Kitaev. Quantum computations: algorithms and error correction. *Russ. Math. Surv.*, 52(6): 1191–1249, 1997.
- [214] A. Y. Kitaev. Quantum error correction with imperfect gates. In A. S. Holevo, O. Hirota and C. M. Caves, editors, *Quantum Communication, Computing, and Measurement*, pages 181–188, Plenum Press, New York, 1997.
- [215] S. Kullback and R. A. Leibler. On information and sufficiency. *Ann. Math. Stat.*, 22: 79–86, 1951.
- [216] E. Knill and R. Laflamme. A theory of quantum error-correcting codes. *Phys. Rev. A*, 55: 900, 1997. *arXive e-print quant-ph/9604034*.
- [217] E. Knill and R. Laflamme. Quantum computation and quadratically signed weight enumerators. *arXive e-print quant-ph/9909094*, 1999.
- [218] O. Klein. *Z. Phys.*, 72: 767–775, 1931.
- [219] E. Knill, R. Laflamme, and L. Viola. Theory of quantum error correction for general noise. *arXive e-print quant-ph/9908066*, 1999.

- [220] E. Knill, R. Laflamme, and W. H. Zurek. Resilient quantum computation. *Science*, 279(5349): 342–345, 1998. *arXive e-print quant-ph/9702058*.
- [221] E. Knill, R. Laflamme, and W. H. Zurek. Resilient quantum computation: error models and thresholds. *Proc. R. Soc. London A.* 454(1969): 365–384, 1998. *arXive e-print quant-ph/9702058*.
- [222] P. G. Kwiat, J. R. Mitchell, P. D. D. Schwindt, and A. G. White. Grover’s search algorithm: An optical approach. *arXive e-print quant-ph/9905086*, 1999.
- [223] E. Knill. Approximating quantum circuits. *arXive e-print quant-ph/9508006*, 1995.
- [224] D. E. Knuth. *Fundamental Algorithms 3rd Edition*, Volume 1 of *The Art of Computer Programming*. Addison-Wesley, Reading, Massachusetts, 1997.
- [225] D. E. Knuth. *Seminumerical Algorithms 3rd Edition*, Volume 2 of *The Art of Computer Programming*. Addison-Wesley, Reading, Massachusetts, 1998.
- [226] D. E. Knuth. *Sorting and Searching 2nd Edition*, Volume 3 of *The Art of Computer Programming*. Addison-Wesley, Reading, Massachusetts, 1998.
- [227] N. Koblitz. *A Course in Number Theory and Cryptography*. Springer-Verlag, New York, 1994.
- [228] C. King and M. B. Ruskai. Minimal entropy of states emerging from noisy quantum channels. *arXive e-print quant-ph/9911079*, 1999.
- [229] K. Kraus. *States, Effects, and Operations: Fundamental Notions of Quantum Theory*. Lecture Notes in Physics, Vol. 190. Springer-Verlag, Berlin, 1983.
- [230] K. Kraus. Complementary observables and uncertainty relations. *Phys. Rev. D*, 35(10): 3070–3075, 1987.
- [231] P. G. Kwiat, A. M. Steinberg, R. Y. Chiao, P. H. Eberhard, and M. D. Petroff. Absolute efficiency and time-response measurement of single-photon detectors. *Appl. Opt.*, 33(10): 1844–1853, 1994.
- [232] M. Kitagawa and M. Ueda. Nonlinear-interferometric generation of numberphase correlated Fermion states. *Phys. Rev. Lett.*, 67(14): 1852, 1991.
- [233] L. Landau. Däs dampfungsproblem in der wellenmechanik. *Z. Phys.*, 45: 430–441, 1927.
- [234] R. Landauer. Irreversibility and heat generation in the computing process. *IBM J. Res. Dev.*, 5: 183, 1961.
- [235] S. Lloyd and S. Braunstein. Quantum computation over continuous variables. *Phys. Rev. Lett.*, 82: 1784–1787, 1999. *arXive e-print quant-ph/9810082*.
- [236] D. A. Lidar, D. A. Bacon, and K. B. Whaley. Concatenating decoherence free subspaces with quantum error correcting codes. *Phys. Rev. Lett.*, 82(22): 4556–4559, 1999.
- [237] H. Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283: 2050–2056, 1999. *arXive e-print quant-ph/9803006*.
- [238] D. A. Lidar, I. L. Chuang, and K. B. Whaley. Decoherence-free subspaces for quantum computation. *Phys. Rev. Lett.*, 81(12): 2594–2597, 1998.

- [239] D. Loss and D. P. DiVincenzo. Quantum computation with quantum dots. *Phys. Rev. A*, 57: 120–126, 1998.
- [240] Y. Lecerf. Machines de Turing réversibles. *Comptes Rendus*, 257: 2597–2600, 1963.
- [241] U. Leonhardt. *Measuring the Quantum State of Light*. Cambridge University Press, New York, 1997.
- [242] L. Levin. Universal sorting problems. *Probl. Peredaci Inf.*, 9: 115–116, 1973. Original in Russian. English translation in *Probl. Inf. Transm. USSR* 9: 265–266 (1973).
- [243] E. H. Lieb. Convex trace functions and the Wigner–Yanase–Dyson conjecture. *Ad. Math.*, 11: 267–288, 1973.
- [244] E. H. Lieb. *Bull. AMS*, 81: 1–13, 1975.
- [245] G. Lindblad. Completely positive maps and entropy inequalities. *Commun. Math. Phys.*, 40: 147–151, 1975.
- [246] G. Lindblad. On the generators of quantum dynamical semigroups. *Commun. Math. Phys.*, 48: 199, 1976.
- [247] G. Lindblad. Quantum entropy and quantum measurements. In C. Bendjaballah, O. Hirota, and S. Reynaud, editors. *Quantum Aspects of Optical Communications*, Lecture Notes in Physics, vol. 378, pages 71–80, Springer-Verlag, Berlin, 1991.
- [248] R. Lipton. DNA solution of hard computational problems. *Science*, 268: 512–525, 1995.
- [249] N. Linden, E. Kupce, and R. Freeman. NMR quantum logic gates for homonuclear spin systems. *arXive e-print quant-ph/9907003*, 1999.
- [250] A. K. Lenstra and H. W. Lenstra Jr., editors. *The Development of the Number Field Sieve*. Springer-Verlag, New York, 1993.
- [251] S. Lloyd. A potentially realizable quantum computer. *Science*, 261: 1569, 1993.
- [252] S. Lloyd. Necessary and sufficient conditions for quantum computation. *J. Mod. Opt.*, 41(12): 2503, 1994.
- [253] S. Lloyd. Almost any quantum logic gate is universal. *Phys. Rev. Lett.*, 75(2): 346, 1995.
- [254] S. Lloyd. Universal quantum simulators. *Science*, 273: 1073, 1996.
- [255] S. Lloyd. The capacity of the noisy quantum channel. *Phys. Rev. A*, 56: 1613, 1997.
- [256] R. E. Ladner, N. A. Lynch, and A. L. Selman. A comparison of polynomial-time reducibilities. *Theor. Comp. Sci.*, 1: 103–124, 1975.
- [257] R. Laflamme, C. Miquel, J.-P. Paz, and W. H. Zurek. Perfect quantum error correction code. *Phys. Rev. Lett.*, 77: 198, 1996. *arXive e-print quant-ph/9602019*.
- [258] D. W. Leung, M. A. Nielsen, I. L. Chuang, and Y. Yamamoto. Approximate quantum error correction can lead to better codes. *Phys. Rev. A*, 56: 2567–2573, 1997. *arXive e-print quant-ph/9704002*.

- [259] H. Lo. A simple proof of the unconditional security of quantum key distribution. *arXive e-print quant-ph/9904091*, 1999.
- [260] J. S. Lomont. *Applications of Finite Groups*. Dover, New York, 1987.
- [261] W. H. Louisell. *Quantum Statistical Properties of Radiation*. Wiley, New York, 1973.
- [262] H.-K. Lo and S. Popescu. Concentrating local entanglement by local actions — beyond mean values. *arXive e-print quant-ph/9707038*, 1997.
- [263] N. Linden and S. Popescu. Good dynamics versus bad kinematics. Is entanglement needed for quantum computation? *arXive e-print quant-ph/9906008*, 1999.
- [264] O. E. Lanford and D. Robinson. Mean entropy of states in quantum-statistical mechanics. *J. Math. Phys.*, 9(7): 1120–1125, 1968.
- [265] E. H. Lieb and M. B. Ruskai. A fundamental property of quantum-mechanical entropy. *Phys. Rev. Lett.*, 30(10): 434–436, 1973.
- [266] E. H. Lieb and M. B. Ruskai. Proof of the strong subadditivity of quantum mechanical entropy. *J. Math. Phys.*, 14: 1938–1941, 1973.
- [267] H. Leff and R. Rex. *Maxwell's Demon: Entropy, Information, Computing*. Princeton University Press, Princeton, NJ, 1990.
- [268] L. J. Landau and R. F. Streater. On Birkhoff theorem for doubly stochastic completely positive maps of matrix algebras. *Linear Algebra Appl.*, 193: 107–127, 1993.
- [269] S. Lloyd and J. E. Slotine. Analog quantum error correction. *Phys. Rev. Lett.*, 80: 4088–4091, 1998.
- [270] H.-K. Lo, T. Spiller, and S. Popescu. *Quantum information and computation*. World Scientific, Singapore, 1998.
- [271] M. Li, J. Tromp, and P. Vitanyi. Reversible simulation of irreversible computation by pebble games. *Physica D*, 120: 168–176, 1998.
- [272] M. Li and P. Vitanyi. Reversibility and adiabatic computation: trading time and space for energy. *Proc. R. Soc. London A*, 452: 769–789, 1996. *arXive e-print quant-ph/9703022*.
- [273] D. W. Leung, L. M. K. Vandersypen, X. Zhou, M. Sherwood, C. Yannoni, M. Kubinec, and I. L. Chuang. Experimental realization of a two-bit phase damping quantum code. *Phys. Rev. A*, 60: 1924, 1999.
- [274] Y. Manin. *Computable and Uncomputable* (in Russian). Sovetskoye Radio, Moscow, 1980.
- [275] Y. I. Manin. Classical computing, quantum computing, and Shor's factoring algorithm. *arXive e-print quant-ph/9903008*, 1999.
- [276] U. M. Maurer. Secret key agreement by public discussion from common information. *IEEE Trans. Inf. Theory*, 39: 733–742, 1993.
- [277] J. C. Maxwell. *Theory of Heat*. Longmans, Green, and Co., London, 1871.
- [278] D. Mayers. Unconditional security in quantum cryptography. *arXive e-print quant-ph/9802025*, 1998.
- [279] M. Mosca and A. Ekert. The hidden subgroup problem and eigenvalue estimation on a quantum computer. *arXive e-print quant-ph/9903071*, 1999.

- [280] R. Merkle. Secure communications over insecure channels. *Comm. of the ACM*, 21: 294–299, 1978.
- [281] G. L. Miller. Riemann’s hypothesis and tests for primality. *J. Comput. Syst. Sci.*, 13(3): 300–317, 1976.
- [282] G. J. Milburn. Quantum optical Fredkin gate. *Phys. Rev. Lett.*, 62(18): 2124, 1989.
- [283] D. A. B. Miller. Optics for low energy communications inside digital processors: quantum detectors, sources, and modulators as efficient impedance converters. *Opt. Lett.*, 14: 146, 1989.
- [284] G. J. Milburn. A quantum mechanical Maxwell’s demon. Unpublished, 1996.
- [285] G. J. Milburn. *Scrödinger’s Machines: the Quantum Technology Reshaping Everyday Life*. W. H. Freeman, New York, 1997.
- [286] G. J. Milburn. *The Feynman Processor: Quantum Entanglement and the Computing Revolution*. Perseus Books, Reading, Mass., 1998.
- [287] M. L. Minsky. *Computation: finite and infinite machines*. Prentice-Hall, Englewood Cliffs, N.J., 1967.
- [288] M. Marcus and H. Mine. *A Survey of Matrix Theory and Matrix Inequalities*. Dover, New York, 1992.
- [289] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland. Demonstration of a fundamental quantum logic gate. *Phys. Rev. Lett.*, 75: 4714, 1995.
- [290] A. W. Marshall and I. Olkin. *Inequalities: Theory of Majorization and its Applications*. Academic Press, New York, 1979.
- [291] J. E. Mooij, T. P. Orlando, L. Levitov, L. Tian, C. H. van der Waal, and S. Lloyd. Josephson persistent-current qubit. *Science*, 285: 1036–1039, 1999.
- [292] T. Mor. No-cloning of orthogonal states in composite systems. *Phys. Rev. Lett.*, 80: 3137–3140, 1998.
- [293] M. Mosca. Quantum searching, counting and amplitude amplification by eigenvector analysis. In R. Freivalds, editor, *Proceedings of International Workshop on Randomized Algorithms*, pages 90–100, 1998.
- [294] M. Mosca. *Quantum Computer Algorithms*. Ph.D. thesis, University of Oxford, 1999.
- [295] R. Motwani, and P. Raghavan. *Randomized Algorithms*. Cambridge University Press, Cambridge, 1995.
- [296] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-correcting Codes*. North-Holland, Amsterdam, 1977.
- [297] H. Maassen and J. H. B. Uffink. Generalized entropic uncertainty relations. *Phys. Rev. Lett.*, 60(12): 1105–1106, 1988.
- [298] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.
- [299] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger. Dense coding in experimental quantum communication. *Phys. Rev. Lett.*, 76(25): 4656–4659, 1996.

- [300] A. Muller, H. Zbinden, and N. Gisin. Quantum cryptography over 23 km in installed under-lake telecom fibre. *Euro-phys. Lett.*, 33: 334–339, 1996.
- [301] M. A. Nielsen and C. M. Caves. Reversible quantum operations and their application to teleportation. *Phys. Rev. A*, 55(4): 2547–2556, 1997.
- [302] M. A. Nielsen, C. M. Caves, B. Schumacher, and H. Barnum. Information-theoretic approach to quantum error correction and reversible measurement. *Proc. R. Soc. London A*, 454(1969): 277–304, 1998.
- [303] M. A. Nielsen. *Quantum Information Theory*. Ph. D. thesis, University of New Mexico, 1998.
- [304] M. A. Nielsen. Conditions for a class of entanglement transformations. *Phys. Rev. Lett.*, 83(2): 436–439, 1999.
- [305] M. A. Nielsen. Probability distributions consistent with a mixed state. *arXive e-print quant-ph/9909020*, 1999.
- [306] M. A. Nielsen, E. Knill, and R. Laflamme. Complete quantum teleportation using nuclear magnetic resonance. *Nature*, 396(6706): 52–55, 1998.
- [307] Y. Nakamura, Y. A. Pashkin, and J. S. Tsai. Coherent control of macroscopic quantum states in a single-cooper-pair box. *Nature*, 398: 786–788, 1999.
- [308] M. Ohya and D. Petz. *Quantum Entropy and Its Use*. Springer-Verlag, Berlin, 1993.
- [309] A. Pais. *Subtle is the Lord: The Science and the Life of Albert Einstein*. Oxford University Press, Oxford, 1982.
- [310] A. Pais. *Inward Bound: Of Matter and Forces in the Physical World*. Oxford University Press, Oxford, 1986.
- [311] A. Pais. *Niels Bohr's Times: In Physics, Philosophy, and Polity*. Oxford University Press, Oxford, 1991.
- [312] C. M. Papadimitriou. *Computational Complexity*. Addison-Wesley, Reading, Massachusetts, 1994.
- [313] R. Paturi. On the degree of polynomials that approximate symmetric Boolean functions (preliminary version). *Proc. 24th Ann. ACM Symp. on Theory of Computing (STOC'92)*, pages 468–474, 1992.
- [314] J. F. Poyatos, J. I. Cirac, and P. Zoller. Complete characterization of a quantum process: the two-bit quantum gate. *Phys. Rev. Lett.*, 78(2): 390–393, 1997.
- [315] P. M. Platzman and M. I. Dykman. Quantum computing with electrons floating on liquid helium. *Science*, 284: 1967, 1999.
- [316] R. Penrose. *The Emperor's New Mind*. Oxford University Press, Oxford, 1989.
- [317] S. Perlis. *Theory of Matrices*. Addison-Wesley, Reading, Mass., 1952.
- [318] A. Peres. How to differentiate between non-orthogonal states. *Phys. Lett. A*, 128: 19, 1988.
- [319] A. Peres. *Quantum Theory: Concepts and Methods*. Kluwer Academic, Dordrecht, 1993.
- [320] A. Peres. Higher order schmidt decompositions. *Phys. Lett. A*, 202: 16–17, 1995.

- [321] D. Petz. Quasi-entropies for finite quantum systems. *Rep. Math. Phys.*, 23(1): 57–65, 1986.
- [322] Physics Today Editor. Quantum cryptography defies eavesdropping. *Physics Today*, page 21, November 1992.
- [323] M. B. Plenio and P. L. Knight. Realistic lower bounds for the factorization time of large numbers on a quantum computer. *Phys. Rev. A*, 53: 2986–2990, 1996.
- [324] M. B. Plenio and P. L. Knight. The quantum-jump approach to dissipative dynamics in quantum optics. *Rev. Mod. Phys.*, 70(1): 101–144, 1998.
- [325] R. P. Poplavskii. Thermodynamical models of information processing (in Russian). *Usp. Fiz. Nauk*, 115(3): 465–501, 1975.
- [326] M. Pueschel, M. Roetteler, and T. Beth. Fast quantum Fourier transforms for a class of non-abelian groups. *arXive e-print quant-ph/9807064*, 1998.
- [327] J. Preskill. Fault-tolerant quantum computation. *arXive e-print quant-ph/9712048*, 1997.
- [328] J. Preskill. Fault-tolerant quantum computation. In H.-K. Lo, T. Spiller, and S. Popescu, editors. *Quantum information and computation*. World Scientific, Singapore, 1998.
- [329] J. Preskill. *Physics 229: Advanced Mathematical Methods of Physics — Quantum Computation and Information*. California Institute of Technology, 1998. URL: <http://www.theory.caltech.edu/people/preskill/ph229/>
- [330] J. Preskill. Reliable quantum computers. *Proc. R. Soc. London A*, 454(1969): 385–410, 1998.
- [331] M. O. Rabin. Probabilistic algorithm for testing primality. *J. Number Theory*, 12: 128–138, 1980.
- [332] H. Z. Rahim. Richard Feynman and Bill Gates: an imaginary encounter. 1999. URL: <http://www.trnsoft.com/features/1rfbg.htm>
- [333] E. M. Rains. Quantum weight enumerators. *IEEE Trans. Inf. Theory*, 44(4): 1388–1394, 1998.
- [334] E. M. Rains. Monotonicity of the quantum linear programming bound. *IEEE Trans. Inf. Theory*, 45(7): 2489–2492, 1999.
- [335] E. M. Rains. Nonbinary quantum codes. *IEEE Trans. Inf. Theory*, 45(6): 1827–1832, 1999.
- [336] E. M. Rains. Quantum shadow enumerators. *IEEE Trans. Inf. Theory*, 45(7): 2361–2366, 1999.
- [337] M. Roetteler and T. Beth. Polynomial-time solution to the hidden subgroup problem for a class of non-abelian groups. *arXive e-print quant-ph/9812070*, 1998.
- [338] A. Ressler. *The Design of a Conservative Logic Computer and A Graphical Editor Simulator*. Master's thesis, Massachusetts Institute of Technology, 1981.
- [339] E. M. Rains, R. H. Hardin, P. W. Shor, and N. J. A. Sloane. Nonadditive quantum code. *Phys. Rev. Lett.*, 79(5): 953–954, 1997.

- [340] A. Rovin. Reduced dynamics with initial correlations, and time-dependent environment and Hamiltonians. *Phys. Rev. Lett.*, 77(16): 3272–3275, 1996.
- [341] I. V. Robinson and D. Ruelle. *Commun. Math. Phys.*, 5: 288, 1967.
- [342] R. L. Rivest, A. Shamir, and L. M. Adleman. A method of obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, 21(2): 120–126, 1978.
- [343] M. B. Ruskai. Beyond strong subadditivity: improved bounds on the contraction of generalized relative entropy. *Rev. Math. Phys.*, 6(5A): 1147–1161, 1994.
- [344] S. Ramo, J. R. Whinnery, and T. van Duzer. Fields and waves in communication electronics. Wiley, New York, 1984.
- [345] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani. Experimental realization of any discrete unitary operator. *Phys. Rev. Lett.*, 73(1): 58–61, 1994.
- [346] J. J. Sakurai. *Modern Quantum Mechanics*. Addison-Wesley, Reading, Mass., 1995.
- [347] R. Schack and C. M. Caves. Classical model for bulk-ensemble NMR quantum computation. *Phys. Rev. A*, 60(6): 4354–4362, 1999.
- [348] E. Schmidt. Zur theorie der linearen und nichtlinearen integralgleichungen. *Math. Annalen.*, 63: 433–476, 1906.
- [349] E. Schrödinger. Probability relations between separated systems. *Proc. Cambridge Philos. Soc.*, 32: 446–452, 1936.
- [350] B. Schumacher. Quantum coding. *Phys. Rev. A*, 51: 2738–2747, 1995.
- [351] B. Schneier. *Applied Cryptography*. John Wiley and Sons, New York, 1996.
- [352] B. W. Schumacher. Sending entanglement through noisy quantum channels. *Phys. Rev. A*, 54: 2614, 1996.
- [353] C. E. Shannon. A mathematical theory of communication. *Bell System Tech. J.*, 27: 379–423, 623–656, 1948.
- [354] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings, 35th Annual Symposium on Foundations of Computer Science*, IEEE Press, Los Alamitos, CA, 1994.
- [355] P. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52: 2493, 1995.
- [356] P. W. Shor. Fault-tolerant quantum computation. In *Proceedings, 37th Annual Symposium on Fundamentals of Computer Science*, pages 56–65, IEEE Press, Los Alamitos, CA, 1996.
- [357] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comp.*, 26(5): 1484–1509, 1997.
- [358] B. Simon. *Trace Ideals and Their Applications*. Cambridge University Press, Cambridge, 1979.
- [359] D. Simon. On the power of quantum computation. In *Proceedings, 35th Annual Symposium on Foundations of Computer Science*, pages 116–123, IEEE Press, Los Alamitos, CA, 1994.

- [360] D. R. Simon. On the power of quantum computation. *SIAM J. Comput.*, 26(5): 1474–1483, 1997.
- [361] P. W. Shor and R. Laflamme. Quantum analog of the MacWilliams identities for classical coding theory. *Phys. Rev. Lett.*, 78(8): 1600–1602, 1997.
- [362] D. Shasha and C. Lazere. *Out of Their Minds: The Lives and Discoveries of 15 Great Computer Scientists*. Springer-Verlag, New York, 1998.
- [363] D. Slepian, editor. *Keys Papers in the Development of Information Theory*. IEEE Press, New York, 1974.
- [364] C. P. Slichter. *Principles of Magnetic Resonance*. Springer, Berlin, 1996.
- [365] B. W. Schumacher and M. A. Nielsen. Quantum data processing and error correction. *Phys. Rev. A*, 54(4): 2629, 1996. *arXive e-print quant-ph/9604022*.
- [366] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *arXive e-print quant-ph/0003004*, 2000.
- [367] R. Solovay and V. Strassen. A fast Monte-Carlo test for primality. *SIAM J. Comput.*, 6: 84–85, 1976.
- [368] P. W. Shor and J. A. Smolin. Quantum error-correcting codes need not completely reveal the error syndrome. *arXive e-print quant-ph/9604006*, 1996.
- [369] A. T. Sornborger and E. D. Stewart. Higher order methods for simulations on quantum computers. *Phys. Rev. A*, 60(3): 1956–1965, 1999. *arXive e-print quant-ph/9903055*.
- [370] B. E. A. Saleh and M. C. Teich. *Fundamentals of Photonics*. Wiley, NY, 1991.
- [371] A. M. Steane. Error correcting codes in quantum theory. *Phys. Rev. Lett.*, 77: 793, 1996.
- [372] A. M. Steane. Multiple particle interference and quantum error correction. *Proc. R. Soc. London A*, 452: 2551–76, 1996.
- [373] A. Steane. The ion-trap quantum information processor. *Appl. Phys. B – Lasers and Optics*, 64(6): 623–642, 1997.
- [374] A. M. Steane. Efficient fault-tolerant quantum computing. *Nature*, 399: 124–126, May 1999.
- [375] S. Somaroo, C. H. Tseng, T. F. Havel, R. Laflamme, and D. G. Cory. Quantum simulations on a quantum computer. *Phys. Rev. Lett.*, 82: 5381–5384, 1999.
- [376] G. Strang. *Linear Algebra and Its Applications*. Academic Press, New York, 1976.
- [377] L. J. Schulman and U. Vazirani. Molecular scale heat engines and scalable quantum computation. *Proc. 31st Ann. ACM Syrup. on Theory of Computing (STOC'99)*, pages 322–329, 1999.
- [378] C. E. Shannon and W. Weaver. *The Mathematical Theory of Communication*. University of Illinois Press, Urbana, 1949.
- [379] N. J. A. Sloane and A. D. Wyner, editors. *Claude Elwood Shannon: Collected Papers*. IEEE Press, New York, 1993.

- [380] B. Schumacher and M. D. Westmoreland. Sending classical information via noisy quantum channels. *Phys. Rev. A*, 56(1): 131–138, 1997.
- [381] B. Schumacher and M. D. Westmoreland. Quantum privacy and quantum coherence. *Phys. Rev. Lett.*, 80(25): 5695–5697, 1998.
- [382] B. W. Schumacher, M. Westmoreland, and W. K. Wootters. Limitation on the amount of accessible information in a quantum channel. *Phys. Rev. Lett.*, 76: 3453, 1996.
- [383] L. Szilard. Über die entropieverminderung in einen thermodynamischen system bei eingriffen intelligenter wesen. *Z. Phys.*, 53: 840–856, 1929.
- [384] B. M. Terhal and D. P. DiVincenzo. The problem of equilibration and the computation of correlation functions on a quantum computer. *arXive e-print quant-ph/9810063*, 1998.
- [385] Q. A. Turchette, C. J. Hood, V. Lange, H. Mabuchi, and H. J. Kimble. Measurement of conditional phase shifts for quantum logic. *Phys. Rev. Lett.*, 75: 4710, 1995.
- [386] H. F. Trotter. On the product of semigroups of operators. *Proc. Am. Math. Soc.*, 10: 545–551, 1959.
- [387] B. S. Tsirelson. Quantum generalizations of Bell’s inequality. *Lett. Math. Phys.*, 4: 93, 1980.
- [388] A. M. Turing. On computable numbers, with an application to the Entscheidungsproblem. *Proc. Lond. Math. Soc. 2 (reprinted in [113])*, 42: 230, 1936
- [389] Q. A. Turchette. *Quantum optics with single atoms and single photons*. Ph. D. thesis, California Institute of Technology, Pasadena, California, 1997.
- [390] A. Uhlmann. On the Shannon entropy and related functionals on convex sets. *Rep. Math. Phys.*, 1(2): 147–159, 1970.
- [391] A. Uhlmann. Sätze über dichtematrizen. *Wiss. Z. Karl-Marx-Univ. Leipzig*, 20: 633–637, 1971.
- [392] A. Uhlmann. Endlich-dimensionale dichtematrizen I. *Wiss. Z. Karl-Marx-Univ. Leipzig*, 21: 421–452, 1972.
- [393] A. Uhlmann. Endlich-dimensionale dichtematrizen II. *Wiss. Z. Karl-Marx-Univ. Leipzig*, 22: 139–177, 1973.
- [394] A. Uhlmann. The ‘transition probability’ in the state space of a *-algebra. *Rep. Math. Phys.*, 9: 273–279, 1976.
- [395] A. Uhlmann. Relative entropy and the Wigner–Yanase–Dyson–Lieb concavity in an interpolation theory. *Commun. Math. Phys.*, 54: 21–32, 1977.
- [396] H. Umegaki. *Kōdai Math. Sem. Rep.*, 14: 59–85, 1962.
- [397] L. Vaidman. Teleportation of quantum states. *Phys. Rev. A*, 49(2): 1473–6, 1994.
- [398] W. van Dam. Quantum oracle interrogation: getting all information for half the price. In *Proceedings of the 39th FOCS*, 1998. *arXive e-print quant-ph/9805006*.
- [399] S. J. van Enk. No-cloning and superluminal signaling. *arXive e-print quant-ph/9803030*, 1998.

- [400] V. Vedral. Landauer's erasure, error correction and entanglement. *arXive e-print quant-ph/9903049*, 1999.
- [401] G. Vidal. Entanglement monotones. *arXive e-print quant-ph/9807077*, 1998.
- [402] G. Vidal. Entanglement of pure states for a single copy. *Phys. Rev. Lett.*, 83(5): 1046–1049, 1999.
- [403] J. von Neumann. *Göttinger Nachrichten*, page 245, 1927.
- [404] J. von Neumann. Probabilistic logics and the synthesis of reliable organisms from unreliable components. In *Automata Studies*, pages 329–378, Princeton University Press, Princeton, NJ, 1956.
- [405] J. von Neumann. Fourth University of Illinois lecture. In A. W. Burks, editor, *Theory of Self-Reproducing Automata*, page 66, University of Illinois Press, Urbana, 1966.
- [406] V. Vedral and M. B. Plenio. Entanglement measures and purification procedures. *Phys. Rev. A*, 57(3): 1619–1633, 1998.
- [407] K. Vogel and H. Risken. Determination of quasiprobability distributions in terms of probability distributions for the rotated quadrature phase. *Phys. Rev. A*, 40(12): 7113–7120, 1989.
- [408] L. M. K. Vandersypen, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang. Realization of effective pure states for bulk quantum computation. *Phys. Rev. Lett.*, 83: 3085–3088, 1999.
- [409] R. Vrijen, E. Yablonovitch, K. Wang, H. W. Jiang, A. Balandin, V. Roychowdhury, T. Mor, and D. DiVincenzo. Electron spin resonance transistors for quantum computing in silicon-germanium heterostructures. *arXive e-print quant-ph/9905096*, 1999.
- [410] W. Warren. The usefulness of NMR quantum computing. *Science*, 277(5332): 1688, 1997.
- [411] J. Watrous. **PSPACE** has 2-round quantum interactive proof systems. *arXive e-print cs/9901015*, 1999.
- [412] S. Winograd and J. D. Cowan. *Reliable Computation in the Presence of Noise*. MIT Press, Cambridge, MA, 1967.
- [413] A. Wehrl. General properties of entropy. *Rev. Mod. Phys.*, 50: 221, 1978.
- [414] D. J. A. Welsh. *Codes and Cryptography*. Oxford University Press, New York, 1988.
- [415] S. Wiesner. Unpublished manuscript, circa 1969, appeared as [416].
- [416] S. Wiesner. Conjugate coding. *SIGACT Sens*, 15: 77, 1983.
- [417] S. Wiesner. Simulations of many-body quantum systems by a quantum computer. *arXive e-print quant-ph/9603028*, 1996.
- [418] D. Williams. *Probability with Martingales*. Cambridge University Press, Cambridge, 1991.
- [419] E. Winfree. *Algorithmic Self-Assembly of DNA*. Ph.D. thesis, California Institute of Technology, Pasadena, California, 1998.
- [420] D. J. Wineland, C. Monroe, W. M. Itano, D. Leibfried, B. E. King, and D. M. Meekhof. Experimental issues in coherent quantum-state manipulation of trapped atomic ions. *J. Res. Natl. Inst. Stand. Tech.*, 103: 259, 1998.

- [421] M. D. Westmoreland and B. Schumacher. Quantum entanglement and the non-existence of superluminal signals. *arXive e-print quant-ph/9801014*, 1998.
- [422] E. P. Wigner and M. M. Yanase. *Proc. Natl. Acad. Sci. (U.S.A.)*, 49: 910–918, 1963.
- [423] K. Wratanabe and Y. Yamamoto. Limits on tradeoffs between third-order optical nonlinearity, absorption loss, and pulse duration in self-induced transparency and real excitation. *Phys. Rev. A*, 42(3): 1699–702, 1990.
- [424] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299: 802–803, 1982.
- [425] A. C. Yao. Quantum circuit complexity. *Proc. of the 34th Ann. IEEE Symp. on Foundations of Computer Science*, pages 352–361, 1993.
- [426] S. Younis and T. Knight. Non dissipative rail drivers for adiabatic circuits. In *Proceedings, Sixteenth Conference on Advanced Research in VLSI 1995*, pages 404–14, IEEE Computer Society Press, Los Alamitos, CA, 1995.
- [427] Y. Yamamoto, M. Kitagawa, and K. Igeta. In *Proc. 3rd Asia-Pacific Phys. Conf.*, World Scientific, Singapore, 1988.
- [428] H. P. Yuen and M. Ozawa. Ultimate information carrying limit of quantum systems: *Physical Review Letters*, 70: 363–366, 1993.
- [429] F. Yamaguchi and Y. Yamamoto. Crystal lattice quantum computer. *Appl. Phys. A*, pages 1–8, 1999.
- [430] C. Zalka. Simulating quantum systems on a quantum computer. *Proc. R. Soc. London A*, 454(1969): 313–322, 1998.
- [431] P. Zanardi. Stabilizing quantum information. *arXive e-print quant-ph/9910016*, 1999.
- [432] P. Zoller and C. W. Gardiner. Quantum noise in quantum optics: the stochastic Schrödinger equation. In S. Reynaud, E. Giacobino, and J. Zinn-Justin, editors, *Quantum Fluctuations: Les Houches Summer School LXIII*, Elsevier, Amsterdam, 1997.
- [433] K. Zyczkowski, P. Horodecki, A. Sanpera, and M. Lewenstein. Volume of the set of separable states. *Phys. Rev. A*, 58(2): 883–892, 1999.
- [434] W. H. Zurek and R. Laflamme. Quantum logical operations on encoded qubits. *Phys. Rev. Lett.*, 77(22): 4683–4686, 1996.
- [435] X. Zhou, D. W. Leung, and I. L. Chuang. Quantum logic gate constructions with one-bit “teleportation”. *arXive e-print quant-ph/0002039*, 2000.
- [436] P. Zanardi and M. Rasetti. Noiseless quantum codes. *Phys. Rev. Lett.*, 79(17): 3306–3309, 1998.
- [437] W. H. Zurek. Thermodynamic cost of computation, algorithmic complexity and the information metric. *Nature*, 341: 119, 1989.
- [438] W. H. Zurek. Decoherence and the transition from quantum to classical. *Phys. Today*, October 1991.

КНИГИ НА РУССКОМ ЯЗЫКЕ ИЗ ОСНОВНОГО СПИСКА

- [92] Кормен Т. Х., Лейсерсон У. Е., Райвест Р. Л. Алгоритмы: построение и анализ: Пер. с англ. –М.:МЦНМО, 1999.
- [147] Феллер В. Введение в теорию вероятностей и ее приложения. Т. 1: Пер. с англ. – М.: Мир, 1983.
- [148] Феллер В. Введение в теорию вероятностей и ее приложения. Т. 2: Пер. с англ. – М.: Мир, 1983.
- [151] Фейнман Р., Лейтон Р., Сэндс М. Фейнмановские лекции по физике: Пер. с англ. – 3-е изд. – М.: Мир – Вып. 3 и 4: Излучение, волны, кванты. Кинетика, теплота, звук. – 1976.
- [152] Фейнман Р., Лейтон Р., Сэндс М. – То же - Вып. 1 и 2: Современная наука о природе. Законы механики. Пространство. Время. Движение. – 1976.
- [162] Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи: Пер. с англ. – М.: Мир, 1982.
- [183] Хорн Р., Джонсон Ч. Матричный анализ: Пер. с англ. –М.: Мир, 1989.
- [189] Хоффстадтер Д. Гёдель, Эшер, Бах: Эта бесконечная гирлянда: Пер. с англ. – Самара, 2001.
- [217] Кан Д. Взломщики кодов: Пер. с англ. – М., 2000.
- [224] Кнут Д. Искусство программирования для ЭВМ. Т. 1. Основные алгоритмы: Пер. с англ. – М.: Мир, 1976.
- [225] Кнут Д.– То же – Т. 2. Полуисленные алгоритмы. – 1977.
- [226] Кнут Д. – То же – Т. 3. Сортировка и поиск. – 1978.
- [274] Манин Ю. И. Вычислимое и невычислимое. М.: Советское радио, 1980.
- [353] Шеннон К. Работы по теории информации и кибернетике: Пер. с англ. – М.: ИЛ, 1963.

СПИСОК ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ НА РУССКОМ ЯЗЫКЕ

1. Белокуров В. В., Тимофеевская О. Д., Хрусталев О. А. Квантовая телепортация – обыкновенное чудо. Ижевск: НИЦ РХД, 2000, 256 с.
2. Берман Г. П., Делен Г. Д., Майньери Р., Цифринович В.ИИИ. Введение в квантовые компьютеры. — М., Ижевск. Институт компьютерных исследований, 2004, 188 с.
3. Валиев К. А. Квантовые компьютеры и квантовые вычисления. УФН, Т. 175, № 1, 2005, 3–39 с.
4. Валиев К. А., Кокин А. А. Квантовые компьютеры: надежды и реальность, 2-ое издание. — М. – Ижевск, НИЦ РХД, 2002, 329 с.
5. Кадомцев Б. Б. Динамика и информация. — М.: УФН, 1997.
6. Квантовый компьютер и квантовые вычисления. Сб. статей (переводы с английского). Ижевск, 1999, 288 с.
7. Килин С. Я. Квантовая информация. УФН, 1999, т. 169, № 5, с. 507–526.
8. Китаев А., Шень А., Вялый М. Классические и квантовые вычисления. — М.: МЦНМО, — ЧеRo, 1999, 192 с.
9. Кокин А. А. Твердотельные квантовые компьютеры на ядерных спинах. — М., Ижевск. Институт компьютерных исследований, 2004, 204 с.
10. Мандель Л., Вольф Э. Оптическая когерентность и квантовая оптика. Пер. с англ. (под ред. В.В. Самарцева). — М.: Наука, Физматлит, 2000, 896 с.
11. Менский М. Б. Явление декогеренции и теория непрерывных квантовых измерений. УФН. – 1998. – Т. 168, с.1017.
12. Менский М. Б. Квантовые измерения и декогеренция. — М.: Физматлит, 2001, 232 с.
13. Ожигов Ю. И. Квантовые вычисления. Учебное пособие. – М.: Издание факультета ВМК МГУ. – 2003, 152 с.
14. Скалли М. О., Зубайри М. С. Квантовая оптика. Пер. с англ. (под ред. В. В. Самарцева). – М.: Физматлит, 2003, 512 с.
15. Стин Э. Квантовые вычисления. – Ижевск, НИЦ «Регулярная и хаотическая динамика», 2000, 112 с.
16. Туманов В. С. Проекционные операторы в теории квантовых компьютеров. — М.: Физический факультет МГУ , 2001, 84 с.
17. Холево А. С. Вероятностные и статистические аспекты квантовой теории. — М.: Наука, 1980.
18. Холево А. С. Введение в квантовую теорию информации. — М.: МЦНМО, 2002, 128 с.
19. Холево А. С. Статистическая структура квантовой теории. — М., Ижевск. Институт компьютерных исследований, 2003.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

- Абелев стабилизатор 304
Алгоритм 163, 165
– вероятностный 24
– Гровера 311
– Дойча 56
– Дойча–Йожа 58
– Евклида 759
– квантовый 222, 262
– Китаева 307
– поиска 311
– Шора 223
– цепных дробей 290
Аналоговые вычисления 24
Ансамбли квантовых состояний 137
Аппроксимация квантовых схем 251
– унитарных операторов 251
Арифметика остатков 759
Асимптотические обозначения 183
Ассоциативность 740
- Базис 93
– Шмидта 150
Бит 33
Блоковая чувствительность 345
Булева схема 177
– функция 177
- Вектор 92
– двойственный 96
– единичный 97
– нормированный 97
– нулевой 92
– ортонормированный 98
– собственный 100
– состояний 115
Векторная игра 217
Векторные пространства 92
Вес Хэмминга 550
Взаимная информация 616, 694
Временная разметка 416
Вырожденные коды 546
- Гамильтониан 117, 355, 377, 396, 408
– Гейзенберга 431
– Джеймса–Каммингса 378
Гармонический осциллятор 355
Граница Варшамова–Гильберта 550, 604
– Синглтона 550
– Холево 646, 694
– Хэмминга 546
Граф 190
Группа абелева 741
– порядок 741
– циклическая 742
- Двоичная энтропия 613
Двоичный симметричный канал 527
Двойственность кодов 553
Демон Максвелла 211, 691
Деполяризующий канал 470, 492
Динамика одного спина 408
Дискретизация ошибок 540
Дискретный логарифм 300
Дисперсия 740
ДНК-компьютеры 213
- Задача Дойча 304
– коммивояжера 192
– нахождения периода 304
– порядка 273, 284, 304
– об абелевом стабилизаторе 63
– изоморфизме графов 198
– о вершинном покрытии 198, 201
– дискретном логарифме 274
– клике 198
– скрытой подгруппе 63, 279, 302, 304
– суммах подмножеств 198
– определения собственного числа 275, 280
– перечисления 275
– Саймона 304
– факторизации 275, 285

- Задачи вычислительные 180
 – о существовании делителя 189
 -- гамильтоновом цикле 191
 – разрешения 188
 Задание квантового процесса 487
 Закон больших чисел 657
 – Мура 23
 Замкнутость 741
 Запутанность квантовая 31, 510,
 701
 – как физический ресурс 693
 – очищение и разбавление 702, 714
 Затухание амплитуды 49, 472
 – фазы 476
 Значение собственное 100
- Идентификация системы 483
 Измерение конечного результата 353
 – намагниченности 411
 Измерения в формализме
 стабилизаторов 567
 – и энтропия 628
 – образующих стабилизатора 601
 – проективные 129
 – POVM 126
 Интерферометр Цендера–Маха 367
 Информатика 22
 Информация 27
 Ионы в ловушке 386
 Исправление квантовых ошибок
 529, 691
 – локализованных ошибок 572
- Каналы унитарно эквивалентные 534
 Каталлиз запутанности 700
 Квадратичное отклонение 740
 Квантовая граница Синглтона 690
 -- Хэмминга 546
 – информация 36, 37, 78, 681
 – криптография 706
 -- экспериментальная 717
 – механика 134
 – различимость 85, 122
 – телепортация 49, 148
 -- в квантовых каналах 82, 681
 -- представление 349
 -- теория информации 644
 – электродинамика 371
 – эффективность 361
- Квантовое моделирование 64
 – неравенство обработки
 данных 685, 694
 – перечисление 327
 – распределение ключей 711
 Квантовомеханические обозначения 93
 Квантовые алгоритмы 64, 223, 422
 – вычисления 38, 65, 357, 362,
 382, 581
 -- устойчивые к ошибкам 581
 – измерения 120
 – источники информации 519
 – логические элементы 420
 – преобразования 441, 444
 -- представление операторной
 суммой 445
 -- применения 479
 -- примеры 464
 -- реализация 455
 – состояния Белла 48
 -- смешанные 139
 -- чистые 139
 -- ЭПР 48
 – схемы 38, 76, 578
 – элементы универсальные 241
 Квантовый алгоритм поиска 311, 321
 – компьютер на оптических
 фотонах 359
 – параллелизм 54
 – поиск 226, 326, 331
 – шум 348
 Китайская теорема об остатках 763
 Класс преобразований ЛОКК 695
 – сложности 66
 -- BPP 67, 256
 -- BQP 67, 255
 -- EXP 200
 -- L 200
 -- MAXSNP 201
 -- NP 66, 188
 -- P 66, 188
 -- PSPACE 67, 199, 255
 -- TIME 189, 200
 Ключ 30, 775
 Когерентная информация 694
 Код Стина 556
 – Шора 533
 Кодирование сверхплотное 27, 91, 135
 – симплектического кода 605

- случайное 666
- с помощью телепортации 607
- Кодирующий ключ 707
- Кодовое расстояние 551
- Коды Грея 245
- вырожденные 546
- исправляющие квантовые ошибки 23, 527
- Кальдебранка–Шора–Стина (CSS) 526, 552
- каскадные 587
- классические линейные 548
- симплектические 557
- Коллизионная энтропия 709
- Коммутатор операторов 110
- Кот Шрёдингера 478
- Криптографический протокол 775
- Криптография 30
 - квантовая 22, 30
 - с закрытым (секретным) ключом 707, 775
 - открытым ключом 706, 774
- Кубит 16, 27, 33, 224
- дополнительный 176
- Лемма Шура 744
- Линейный код 545
 - функционал 95
- Логическая разметка 419
- Малая теорема Ферма 764
- Марковские цепи 622
- Мастер-уравнения 481
- Математическое ожидание 740
- Матрица изменения бита 117
 - переворачивания фазы 117
 - плотности 137
 - порождающая 548
 - проверка на четность 549
 - унитарная 40
- Матрицы двухуровневые
 - унитарные 242
 - Паули 96
- Машина Минского 216
 - Тьюринга 22, 166
 - обратимая 218
 - универсальная 172
- Метрика Колмогорова 493
 - Хэмминга 495, 550
- Множество порождающее 93
- Модели независимых ошибок 543
- Моделирование квантовых систем 259
- Наблюдаемые 123
- Наибольший общий делитель 759
- Нахождение порядка 767
- Неравенство Араки–Либа 630
 - Белла 152
 - Клейна 622, 638
 - Коши–Шварца 100
 - обработки данных 620, 684, 694
 - Фано 622, 684, 694
 - Цирельсона 160
 - Чебышёва 740
 - Чернова 203, 740
 - CHSH 158
- Носитель эрмитова оператора 145
- Обозначения Дирака 91
 - бра-вектор 93
 - кет-вектор 92
- Обработка данных 622
- Образующие группу 743
- нормализатора 589
- Обратное распространение ошибок 593
- Обращение вычислений 208
- Одноразовый блокнот 707
- Оператор Адамара 108
 - измерения 120, 141
 - бита 448
 - линейный 94
 - матричное представление 95
 - неотрицательно определенный 14, 95, 105
 - плотности 91, 108, 137, 140
 - поворота 226
 - положительно определенный 14
 - сопряженный 102
 - унитарный 351
 - эрмитов 102
- Операторы двухуровневые 242
 - Линдблада 481
- Операции на одном кубите 225
- Оракул 311
- Ортогонализация Грама–Шмидта 98
- Ортогональность векторов 97
 - групп 745

- Основная теорема арифметики 759
 Осцилляции Раби 379
 Оценка количества простых чисел 773
 Ошибка классическая 493
 – фазовая 493
- Парадокс Эйнштейна–Подольского–Розена 152
 Параметр Лэмба–Дика 390
 Переворот фазы 116, 492
 Подгруппа 741
 – циклическая 743
 Пороговая теорема 587, 588, 603
 Порядок группы 741
 – перестановки 304
 – числа 767
 – элемента 741
 Последовательности нетипичные 655
 – типичные 655
 Постоянная Планка 117
 Построение кодов квантовых 547
 – симплектических 570
 Постулаты квантовой механики 114
 Правило Байеса 459
 Представление групп 744
 – в виде операторной суммы 445, 448
 – регулярное 746
 – точное 746
 Преобразование запутанности 87, 695
 – исправления ошибок 536
 – сопряжения 109
 – Уолша–Адамара 54
 – Фурье 275, 747
 – быстрое 279
 – дискретное 275
 – квантовое 223, 276, 279
 Приводимость групп 744
 Принцип Ландауэра 204
 – неопределенности Гейзенберга 124, 612
 – отложенного измерения 238
 – суперпозиции 131
 Проблема остановки 173
 Проверочная матрица 561
 Проективные измерения 122
 Проектор 102
 Пространственная разметка 423
- Пространство состояний 114, 141
 Пропускная способность канала 665
 Протокол 131, 224
 – BB84 712, 714, 731
 – B92 715
 – CSS кодов 728
 – исправления ошибок 724
 – КРК 721
 – Ло–Чу 723, 725
 – ЭПР 716
 Псевдокод 170
- Различие квантовых состояний 122, 645
 Разложение на простые множители 769
 – полярное 112
 – по сингулярным числам 112
 – спектральное 104
 – Шмидта 91, 149
 Распределение вероятностей 15
 Расстройка 378
 Расширения до чистого состояния 91, 149, 151
 Резонатор Фабри–Перо 372
 Рефокусировка 413
- Сводимость языка 192
 Связь по каналу с шумом 665, 673
 Секретность и когерентная информация 718
 Сжатие ансамбля квантовых состояний 664
 – данных 652
 – схема 664
 – Шумахера 663
 Симплектические коды 557, 576
 Синдром ошибки 530, 559
 Система DES 225
 – RSA 776
 – вспомогательная 132
 Скрытая линейная функция 304
 Следовая матрица 750
 – метрика 497, 501, 506
 Сложность квантовых вычислений 165, 184, 255
 Случайная переменная 739
 Случайное кодирование 666, 674
 Смежные классы 743

- Согласование информации 708
Сопряженность 742
Составные системы 131
Состояния Белла 48
– расширение до чистого 149
– ЭПР 48
Спин 388
Спонтанное излучение 395
Степень совпадения 506
– монотонность 513
– цепное свойство 517
Субаддитивность 631
– сильная 634
– условной энтропии 638
Существование единицы 741
– обратного 732
Сфера Блоха 36, 144
– Хэмминга 667
- Тезис Чёрча–Тьюринга 22, 169, 186
Телепортация 491
Тензорное произведение 104
Теорема Биркгофа 697
– Готтесмана–Нилла 569
– Кука–Левина 193
– Лагранжа 742
– Либа 631, 780
– об иерархии по памяти 200
– временной 200
– о невозможности копирования 20,
 646
– типичном подпространстве 672
– типичных последовательностях
 655
– основная арифметики 758
– представления для НОД 759
– Соловея–Китаева 251, 749, 751
– Ульмана 508
– Ферма малая 764
– фундаментальная 745
– Холево–Шумахера–Вестморленда
 82, 678, 694
– Шеннона о кодировании 27, 80,
 611, 653, 670
– Шумахера 83, 661, 694
– Эйлера 191
Теория групп 741
– информации 706
– сложности вычислений 66, 185
– чисел 758
Тесты случайной выборки 714
Типичные последовательности 658
Томография процесса 441, 483, 487
– квантового состояния 419
Тьюринговы номера 169
- Унитальность квантового процесса 480
Унитальные каналы 492
Унитарные группы матриц 744
– элементы 563
Уравнение Шредингера 117
– квантовое моделирование 265
Усиление конфиденциальности 708
Условие полноты 99
Условия исправления квантовых
 ошибок 537
Условная вероятность 739
Устойчивое к ошибкам измерение 596
Устойчивость к ошибкам 582,
 584, 588
Устойчивый к ошибкам элемент
 Тоффоли 596
– $\pi/8$ 594
- Фаза 116, 130
Фазовращатель 363
Фазовый множитель 117
Факторизация 285, 293
Фонон 388
Формализм стабилизаторов 557
– POVM 126
Формальный язык 188
Формула Байеса 739
– Бейкера–Кэмпбелла–Хаусдорфа 265
– полной вероятности 739
– Тrottера 263
Фрактран 218
Фундаментальная теорема
 о группе 745
- Характер группы 744
Характеристический
 многочлен 100
Хеш-функции 709
- Целевой слот 649
Целочисленное программирование 198
Цепные дроби 769

- Цикл 190
- Эйлера 191
- Числа натуральные 758
 - простые 758, 773
 - сингулярные 113
 - целые 758
- Число собственное 100
 - Шмидта 150
- Шифр Вернама 707
- Шифрование 30
- Шум Джонса 390
 - квантовый 440
- Эволюция квантовой системы 116, 141
- Эквивалентность групп 744
- Эксперимент Штерна–Герлаха 68
- Элемент Адамара 15, 117, 228
 - бит 17
 - измерение 17
 - кубит 17
 - логический 38, 174
 - многокубитовый 41
 - обмен 16
 - однокубитовый 43
 - Паули 16, 228
 - Тоффоли 16, 52, 205
 - управляемый 16, 228
 - управляющий 228
 - фазовый 16, 228
 - Фредкина 17, 206
 - СNOT 16, 229, 231
- NOT 16
- $\pi/8$ 16, 228
- Элементы вычислительного базиса 258
 - логические 39
 - однокубитовые 39
 - универсальные 42
- Энергия 205
 - основного состояния 118
- Энтропия 15, 613
 - вогнутость 628
 - квантовая 622
 - классическая 627
 - непрерывность 622
 - обменная 681
 - основные свойства 612, 624
 - относительная 614, 622
 - обобщенная 640
 - смеси квантовых состояний 630
 - совместная 616
 - условная 616
 - фон Неймана 83, 621, 694
 - Холево 638
 - Шеннона 80, 609, 694
- Эффект Мёссбауэра 390
- Эффективность квантовых вычислений 65
- Ядерные спины 436
- Ядерный магнитный резонанс 77, 404, 410
- Язык формальный 188

ОГЛАВЛЕНИЕ

Предисловие к русскому изданию	5
Предисловие	7
Благодарности	13
Терминология и обозначения	14
I Фундаментальные принципы	18
1 Введение и общий обзор	18
1.1 Глобальные перспективы	19
1.1.1 История квантовых вычислений и квантовой информации	19
1.1.2 Направления будущих исследований	32
1.2 Квантовые биты	33
1.2.1 Несколько кубитов	37
1.3 Квантовые вычисления	38
1.3.1 Однокубитовые элементы	39
1.3.2 Многокубитовые элементы	42
1.3.3 Измерения в базисах, отличных от вычислительного	44
1.3.4 Квантовые схемы	45
1.3.5 Схема копирования кубита?	47
1.3.6 Пример: состояния Белла	48
1.3.7 Пример: квантовая телепортация	49
1.4 Квантовые алгоритмы	52
1.4.1 Классические вычисления на квантовом компьютере	52
1.4.2 Квантовый параллелизм	54
1.4.3 Алгоритм Дойча	56
1.4.4 Алгоритм Дойча-Йожа	58
1.4.5 Классификация квантовых алгоритмов	61
1.5 Экспериментальная обработка квантовой информации	68
1.5.1 Эксперимент Штерна–Герлаха	68
1.5.2 Перспективы практической обработки квантовой информации	72
1.6 Квантовая информация	78
1.6.1 Квантовая теория информации: примеры задач	80
1.6.2 Квантовая информация в более широком контексте	87

2 Введение в квантовую механику	90
2.1 Линейная алгебра	91
2.1.1 Базисы и линейная независимость	93
2.1.2 Линейные операторы и матрицы	94
2.1.3 Матрицы Паули	96
2.1.4 Скалярное произведение	96
2.1.5 Собственные векторы и собственные значения	100
2.1.6 Сопряженные и эрмитовы операторы	102
2.1.7 Тензорное произведение	104
2.1.8 Операторные функции	108
2.1.9 Коммутатор и антакоммутатор	110
2.1.10 Полярное разложение и разложение по сингулярным числам	112
2.2 Постулаты квантовой механики	114
2.2.1 Пространство состояний	114
2.2.2 Эволюция	116
2.2.3 Квантовые измерения	120
2.2.4 Различие квантовых состояний	122
2.2.5 Проективные измерения	122
2.2.6 POVM-измерения	126
2.2.7 Фаза	130
2.2.8 Составные системы	131
2.2.9 Квантовая механика: общий взгляд	134
2.3 Сверхплотное кодирование	135
2.4 Оператор плотности	137
2.4.1 Ансамбли квантовых состояний	137
2.4.2 Общие свойства операторов плотности	140
2.4.3 Редуцированный оператор плотности	145
2.5 Разложение Шмидта и расширения до чистого состояния	149
2.6 Парадокс Эйнштейна - Подольского - Розена и неравенство Белла	152
3 Введение в информатику	163
3.1 Вычислительные модели	165
3.1.1 Машины Тьюринга	166
3.1.2 Схемы	175
3.2 Анализ вычислительных задач	180
3.2.1 Как количественно оценивать компьютерные ресурсы	182
3.2.2 Сложность вычислений	184
3.2.3 Задачи разрешения и классы сложности P и NP	188
3.2.4 Другие классы сложности	199
3.2.5 Вычисления и энергия	202
3.3 Перспективы информатики	212

II Квантовые вычисления	221
4 Квантовые схемы	221
4.1 Квантовые алгоритмы	222
4.2 Операции на одном кубите	224
4.3 Условные операции	229
4.4 Измерение	238
4.5 Универсальные квантовые элементы	241
4.5.1 Универсальность двухуровневых унитарных операторов	242
4.5.2 Универсальность набора из однокубитовых элементов и CNOT	244
4.5.3 Конечный набор универсальных операций	247
4.5.4 Трудность аппроксимации общего унитарного оператора в общем случае	253
4.5.5 Сложность квантовых вычислений	255
4.6 Модель квантовых схем вычислений	257
4.7 Моделирование квантовых систем	259
4.7.1 Моделирование в действии	260
4.7.2 Алгоритм квантового моделирования	262
4.7.3 Пример	265
4.7.4 Перспективы квантового моделирования	268
5 Квантовое преобразование Фурье и его приложения	274
5.1 Квантовое преобразование Фурье	275
5.2 Определение собственного числа	280
5.2.1 Оценка скорости работы и вероятности ошибки	282
5.3 Приложения: нахождение порядка и факторизация	285
5.3.1 Нахождение порядка	286
5.3.2 Факторизация	293
5.4 Общие приложения квантового преобразования Фурье	297
5.4.1 Нахождение периода	297
5.4.2 Дискретный логарифм	300
5.4.3 Задача о скрытой подгруппе	302
5.4.4 Возможны ли другие квантовые алгоритмы?	305
6 Квантовые алгоритмы поиска	311
6.1 Квантовый алгоритм поиска	311
6.1.1 Оракул	311
6.1.2 Процедура	314
6.1.3 Геометрическая интерпретация	315
6.1.4 Эффективность	317
6.2 Квантовый поиск как квантовое моделирование	321
6.3 Квантовое перечисление	327
6.4 Ускорение решения NP-полных задач	329
6.5 Квантовый поиск в неструктурированной базе данных	331

6.6	Оптимальность алгоритма поиска	335
6.7	Ограничение алгоритмов в модели черного ящика	339
7	Квантовые компьютеры: физическая реализация	346
7.1	Основные принципы	347
7.2	Условия для квантового вычисления	348
7.2.1	Представление квантовой информации	349
7.2.2	Реализация унитарных операторов	351
7.2.3	Приготовление начального состояния	352
7.2.4	Измерение конечного результата	353
7.3	Гармонический осциллятор как модель квантового компьютера .	354
7.3.1	Физическая аппаратура	354
7.3.2	Гамильтониан	355
7.3.3	Квантовые вычисления	357
7.3.4	Недостатки	358
7.4	Квантовый компьютер на оптических фотонах	359
7.4.1	Физическая аппаратура	359
7.4.2	Квантовые вычисления	362
7.4.3	Недостатки	370
7.5	Квантовая электродинамика в оптических резонаторах	371
7.5.1	Физическая аппаратура	372
7.5.2	Гамильтониан	377
7.5.3	Поглощение и преломление для одиночного фотона и одиночного атома	378
7.5.4	Квантовые вычисления	382
7.6	Ионы в ловушке	386
7.6.1	Физическая аппаратура	386
7.6.2	Гамильтониан	396
7.6.3	Квантовые вычисления	398
7.6.4	Эксперимент	400
7.7	Ядерный магнитный резонанс	404
7.7.1	Физическая аппаратура	406
7.7.2	Гамильтониан	407
7.7.3	Квантовые вычисления	413
7.7.4	Эксперимент	419
7.8	Другие варианты реализации	427
III	Квантовая информация	440
8	Квантовый шум и квантовые преобразования	440
8.1	Классический шум и марковские процессы	441
8.2	Квантовые преобразования	444
8.2.1	Обзор	444
8.2.2	Окружающая среда и квантовые преобразования	445

8.2.3	Представление операторной суммой	448
8.2.4	Аксиоматический подход к квантовым преобразованиям	455
8.3	Примеры квантового шума и квантовых преобразований	464
8.3.1	След и частичный след	465
8.3.2	Геометрическая картина квантового преобразования одного кубита	466
8.3.3	Каналы с классической ошибкой и переворотом фазы	467
8.3.4	Деполяризующий канал	470
8.3.5	Затухание амплитуды	471
8.3.6	Затухание фазы	476
8.4	Применения квантовых преобразований	480
8.4.1	Мастер-уравнения	481
8.4.2	Томография квантовых процессов	483
8.5	Ограничения формализма квантовых преобразований	490
9	Меры различия квантовой информации	495
9.1	Меры различия классической информации	495
9.2	Насколько близки два квантовых состояния?	499
9.2.1	Следовая метрика	499
9.2.2	Степень совпадения	506
9.2.3	Связь между мерами различия	513
9.3	Насколько квантовый канал сохраняет информацию?	514
10	Исправление квантовых ошибок	525
10.1	Введение	526
10.1.1	Трехкубитовый код, исправляющий классические ошибки	527
10.1.2	Трехкубитовый код, исправляющий фазовые ошибки	531
10.2	Код Шора	533
10.3	Теория исправления квантовых ошибок	536
10.3.1	Дискретизация ошибок	540
10.3.2	Модели независимых ошибок	543
10.3.3	Вырожденные коды	546
10.3.4	Квантовая граница Хэмминга	546
10.4	Построение квантовых кодов	547
10.4.1	Классические линейные коды	547
10.4.2	Коды Кальдербанка–Шора–Стина	552
10.5	Симплектические коды	557
10.5.1	Формализм стабилизаторов	557
10.5.2	Унитарные операторы и формализм стабилизаторов	563
10.5.3	Измерения в формализме стабилизаторов	567
10.5.4	Теорема Готтесмана–Нилла	569
10.5.5	Построение симплектических кодов	570
10.5.6	Примеры	572
10.5.7	Стандартная форма симплектического кода	576

10.5.8 Квантовые схемы для кодирования, декодирования и исправления ошибок	578
10.6 Квантовые вычисления, устойчивые к ошибкам	581
10.6.1 Устойчивость к ошибкам, общая картина	582
10.6.2 Устойчивые к ошибкам квантовые логические элементы .	589
10.6.3 Устойчивое к ошибкам измерение	596
10.6.4 Элементы надежного квантового вычисления	602
11 Энтропия и информация	609
11.1 Шенноновская энтропия	609
11.2 Основные свойства энтропии	612
11.2.1 Двоичная энтропия	612
11.2.2 Относительная энтропия	614
11.2.3 Условная энтропия и взаимная информация	616
11.2.4 Неравенство обработки данных	620
11.3 Энтропия фон Неймана	621
11.3.1 Квантовая относительная энтропия	622
11.3.2 Основные свойства энтропии	624
11.3.3 Измерения и энтропия	626
11.3.4 Субаддитивность	627
11.3.5 Вогнутость энтропии	628
11.3.6 Энтропия смеси квантовых состояний	630
11.4 Сильная субаддитивность	631
11.4.1 Доказательство сильной субаддитивности	632
11.4.2 Сильная субаддитивность: основные применения	634
12 Квантовая теория информации	642
12.1 Различие квантовых состояний и доступная информация	643
12.1.1 Граница Холево	646
12.1.2 Примеры применения границы Холево	649
12.2 Сжатие данных	652
12.2.1 Теорема Шеннона о кодировании для канала без шума .	653
12.2.2 Теорема Шумахера о кодировании для квантового канала без шума	659
12.3 Передача классической информации по квантовым каналам с шумом	665
12.3.1 Связь по классическому каналу с шумом	665
12.3.2 Связь по квантовым каналам с шумом	673
12.4 Квантовая информация в квантовых каналах с шумом	681
12.4.1 Обменная энтропия и квантовое неравенство Фано	682
12.4.2 Квантовое неравенство обработки данных	684
12.4.3 Квантовая граница Синглтона	690
12.4.4 Исправление квантовых ошибок, охлаждение и демон Максвелла	691
12.5 Запутанность как физический ресурс	693

12.5.1	Преобразование запутанности чистого состояния системы из двух компонент	695
12.5.2	Очищение и разбавление запутанности	701
12.5.3	Очищение запутанности и исправление квантовых ошибок	704
12.6	Квантовая криптография	706
12.6.1	Криптография с закрытым ключом	707
12.6.2	Усиление конфиденциальности и согласование информации	708
12.6.3	Квантовое распределение ключей	711
12.6.4	Секретность и когерентная информация	718
12.6.5	Безопасность квантового распределения ключей	720
Приложение 1. Некоторые сведения из теории вероятностей.....		739
Приложение 2. Теория групп		741
P2.1	Основные определения	741
P2.1.1	Образующие	742
P2.1.2	Циклические группы	743
P2.1.3	Смежные классы	743
P2.2	Представления	744
P2.2.1	Эквивалентность и приводимость	744
P2.2.2	Ортогональность	745
P2.2.3	Регулярное представление	746
P2.2.4	Преобразования Фурье	747
Приложение 3. Теорема Соловея–Китаева.....		749
Приложение 4. Теория чисел		758
P4.1	Начальные сведения	758
P4.2	Арифметика остатков и алгоритм Евклида	759
P4.3	Сведение разложения на простые множители к нахождению порядка элемента	767
P4.4	Цепные дроби	769
Приложение 5. Криптография с открытым ключом и система RSA		774
Приложение 6. Доказательство теоремы Либа		780
Список литературы.....		785
Книги на русском языке из основного списка		808
Список дополнительной литературы на русском языке		809
Предметный указатель		810

Учебное издание

Майкл А. Нильсен, Исаак Л. Чанг

**КВАНТОВЫЕ ВЫЧИСЛЕНИЯ
И КВАНТОВАЯ ИНФОРМАЦИЯ**

Зав. редакцией Т. Г. Хохлова

Ведущие редакторы Л. А. Паршина и Л. П. Якименко

Художник Ф. П. Инфанте

Технический редактор Е. В. Денюкова

*Оригинал макет подготовлен В. Н. Титаренко в пакете LATEX2ε
с использованием кириллических шрифтов семейства LH*

Подписано к печати 12.12.2005. Формат 70×100^{1/16}. Бумага газетная
Печать офсетная. Объем 25,75 бум. л. Усл. печ. л 66,95.
Изд. № 6/9939. Тираж 1500 экз. Заказ 1965.

Издательство «Мир»
Министерства культуры и массовых коммуникаций РФ
107996, ГСП-6, Москва, 1-й Рижский пер., д. 2.

Диапозитивы изготовлены в издательстве «Мир»

Отпечатано с готовых диапозитивов
в ГУП «Брянское областное полиграфическое объединение»
241019, г. Брянск, пр-т Ст. Димитрова, 40