

53

3-335



**Учебник
Воронежского
государственного
университета**

С. А. Запрягаев

**ВВЕДЕНИЕ В КВАНТОВЫЕ
ИНФОРМАЦИОННЫЕ СИСТЕМЫ**



МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО
ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

*Учебник Воронежского
государственного университета*

С. А. Запрягаев

**ВВЕДЕНИЕ В КВАНТОВЫЕ
ИНФОРМАЦИОННЫЕ
СИСТЕМЫ**

Учебное пособие

Воронеж
Издательский дом ВГУ
2015

УДК 531:530.145
ББК 22.314.1
3-33

Р е ц е н з е н т ы :

доктор физико-математических наук, профессор *A. Ф. Клиничких*;
кандидат физико-математических наук, доцент *C. В. Власов*

Запрягаев С. А.

3-33 Введение в квантовые информационные системы : учебное пособие /
С. А. Запрягаев ; Воронежский государственный университет. – Воронеж : Издательский дом ВГУ, 2015. – 219 с. – (Учебник Воронежского го-
сударственного университета).

ISBN 978-5-9273-2173-5

Учебное пособие обеспечивает введение в быстро развивающуюся область
информационных систем, находящихся на пересечении компьютерных, фи-
зических, математических наук и вычислительной техники.

Рекомендуется для студентов старших курсов, магистров и аспирантов
инженерных направлений подготовки, а также бакалавров направления
«Математика. Компьютерные науки». Представленный учебный материал
отражает содержание семестрового курса «Квантовые информационные сис-
темы», который в течение последних десяти лет преподаётся на факультете
компьютерных наук Воронежского государственного университета для на-
правлений «Информационные системы и технологии» и «Математика. Ком-
пьютерные науки». Весь необходимый учебный материал изложен в пособии
с учётом разницы в базовых курсах инженерного и математического профи-
ля. Положения квантовой теории представлены на основе аксиоматического
подхода с учётом уровня подготовки в бакалавриате.

Работа выполнена при поддержке Российского научного фонда, проект
№ 14-12-00583.

УДК 531:530.145
ББК 22.314.1

ISBN 978-5-9273-2173-5

© Запрягаев С. А., 2015
© Воронежский государственный
университет, 2015
© Оформление, оригинал-макет.
Издательский дом ВГУ, 2015

Оглавление

Предисловие	5
Часть I Квантовая теория	9
Глава 1 Основы квантовой теории	10
1.1 Постулат состояния	10
1.2 Алгебра операторов	15
1.3 Принцип суперпозиции состояний	19
1.4 Постулат соответствия оператора физической величине	21
1.5 Постулат об измерении физической величины	24
1.6 Постулат об эволюции квантовых состояний	27
1.7 Представление квантовых состояний и операторов	28
1.8 Кубит	37
1.9 Трансформационные свойства квантовых состояний	39
1.10 Квантовая теория на основе уравнения Шрёдингера	44
1.11 Простые примеры решения уравнения Шрёдингера	47
Глава 2 Спин	57
2.1 Спин электрона	57
2.2 Свойства матриц Паули	59
2.3 Собственные векторы оператора спина	61
2.4 Вращение собственных векторов матриц Паули	64
2.5 Уравнение Паули	67
2.6 Спиновый резонанс для свободного электрона	68
2.7 Двухуровневая система	70
Глава 3 Матрица плотности	73
3.1 Чистые и смешанные состояния	73
3.2 Эволюция оператора плотности	81
3.3 Вектор поляризации. Спиновая матрица плотности	83
3.4 Теорема Шмидта	87
Часть II Классические вычисления	91
Глава 4 Компьютерные технологии	92
4.1 Основные понятия алгебры логики	93
4.2 Классические логические гейты	95
4.3 Обратимые логические гейты	103

Часть III Квантовая модель вычислений	111
Глава 5 Квантовые компьютерные технологии	112
5.1 Введение	112
5.2 Однокубитовые гейты	114
5.3 Квантовый интерферометр	118
5.4 Квантовый регистр	120
5.5 Многокубитовые квантовые гейты	124
5.6 Невозможность клонирования кубита	131
5.7 Состояния Белла	132
5.8 Декогеренция	135
5.9 Квантовый параллелизм	137
Глава 6 Квантовые алгоритмы	141
6.1 Алгоритм Дойча (Deutsch)	141
6.2 Алгоритм Дойча – Джозса (Deutsch – Jozsa)	146
6.3 Алгоритм Саймона	151
6.4 Квантовое преобразование Фурье	156
6.5 Квантовый алгоритм преобразования Фурье	158
6.6 Оценка фазы	166
6.7 Возврат фазы в регистр данных	172
6.8 Оценка собственного значения унитарного оператора	174
6.9 Алгоритм Шора	177
6.10 Алгоритм Гровера (поиск в базе данных)	188
Часть IV Телепортация и связь	195
Глава 7 Телепортация и сверхплотное кодирование	196
7.1 Квантовая телепортация	196
7.2 Сверхплотное кодирование	202
Часть V Защита информации	205
Глава 8 Элементарные основы квантовой криптографии	206
8.1 Классическое шифрование	206
8.2 Квантовый протокол BB84	210
8.3 Квантовый протокол B92	214
Библиографический список	217

Предисловие

При проведении вычислений, создавая механизированные вычислительные устройства, человечество прошло огромный путь от применения счётных палочек и камешков до современных, высокопроизводительных электронных компьютеров. При этом основной и наиболее революционный шаг был сделан в середине XX в., когда появились первые электронные вычислительные машины. Первоначально электронные устройства использовали систему переключателей на основе электромагнитных реле. Затем в этих устройствах вместо электромеханических реле стали использовать радиолампы, а впоследствии полупроводники и транзисторы. Наконец, появление технологии создания больших интегральных схем на основе выращенных кристаллических структур, которые включали в себя миллионы транзисторов, образующих электронные цепи, превратило электронные вычислительные машины в персональные компьютеры, а общество в целом — в информационное общество.

Эволюция электронных вычислительных устройств на всех этапах сводилась к последовательному наращиванию быстродействия и достижению всё большей миниатюризации. Если ламповые устройства занимали целые комнаты, то современные компьютеры, использующие процессоры, построенные на принципах нанотехнологий, имеют миниатюрные размеры в сравнении с их гигантскими предшественниками.

К чему приведёт процесс постоянной миниатюризации в дальнейшем? Технологии, по сути, приблизили вычислительные устройства к области атомов, молекул, макромолекул, ядер, элементарных частиц. Поэтому перспектива последующей миниатюризации — это переход на системы, функционирующие на отдельных молекулах или атомах, т. е. переход на уровень микромира. Однако такой переход не является просто переходом к другому масштабу, он содержит в себе переход к новому качеству и к новым проявлениям физических свойств материи, отличных от известных в классической физике.

Все существующие электронные вычислительные устройства основаны на совокупности элементов с двумя возможными строго детерминирован-

ными состояниями. Данные состояния принято обозначать 0 и 1. Этими состояниями могут быть состояния “включено-выключено” в цепи реле, наличие напряжений или их отсутствие на пластинах конденсатора в цепи радиоламп или транзисторов, наличие тока или его отсутствие в электронных устройствах и т. п. Два возможных состояния 0 или 1 называются битами, а компьютеры, построенные на таких классических, с точки зрения физики, устройствах, – классическими.

Исследование возможностей применения классических компьютеров в различных отраслях науки и техники продемонстрировало их существенно ограниченные возможности при решении ряда важных задач. Примером такой ограниченности может служить фундаментальная задача разложения больших чисел на простые множители. Какой бы примитивной ни казалась такая математическая задача, её значение трудно переоценить, например, в задачах криптографической защиты информации. Оказалось, что даже лучшие алгоритмы разложения числа на множители приводят к экспоненциальному росту вычислительных ресурсов с ростом исследуемого числа. И для диапазона чисел, применяемых в криптографии, требуется время, существенно большее времени жизни поколений, что делает бессмысленными попытки раскрытия шифров в современной криптографии. Имеется и ряд других практических задач, которые немыслимо решить на современных суперкомпьютерах за время, сравнимое с временем жизни одного поколения.

Оказалось, что выход из данного тупика можно найти при реализации устройства, которое получило название квантовый компьютер. Идея квантового компьютера состоит в использовании в качестве объектов вычислений не детерминированные битовые состояния, а квантовые состояния, которые являются суперпозицией состояний и обладают свойствами, далеко не похожими на свойства классических состояний. Такие квантовые состояния получили название кубиты (квантовые биты) и реализуются на объектах микромира, которые могут находиться в суперпозиции двух возможных квантовых состояний. Эти состояния по традиции классических информационных систем идентифицируются теми же 0 и 1, но при этом используются специально введённые обозначения $|0\rangle$ и $|1\rangle$. В результате кубит обозначается следующим образом:

$$\text{кубит} \equiv a|0\rangle + b|1\rangle, \quad |a|^2 + |b|^2 = 1.$$

В чём же состоят преимущество и уникальные возможности использования кубит перед классическими битами? Всё это рассмотрено в содер-

жении данного пособия, однако для первоначального ознакомления достаточно рассмотреть вычисление в классическом компьютере некоторой функции $f(x)$, где $x = 0$ или $x = 1$. Если необходимо вычислить оба значения этой функции, потребуется выполнить два вычисления функции $f(0)$ и $f(1)$ по одному и тому же алгоритму. При использовании кубита за одно вычисление будут вычислены оба значения функции параллельно! Параллелизм вычислений и экспоненциальный рост числа состояний на совокупности кубита являются основными свойствами квантовых компьютеров, которые делают эти устройства привлекательными для их использования в сравнении с классическими системами. Как эти свойства реализовать в квантовых компьютерах, рассматривается ниже. Практически квантовый компьютер представляет совокупность (регистр) кубит, с которыми осуществляются преобразования по определённым процедурам. Для практической реализации, сравнимой с существующими компьютерами, необходим регистр, содержащий порядка 1000 кубит. В том, что квантовый компьютер удастся реализовать, сомневались до середины 1990-х гг., но первый квантовый компьютер, имевший лишь два ядерных спина (два кубита), был представлен уже в 1998 г. Через год число спинов (кубит) возросло до трёх, в 2000 г. – до пяти, а в 2001 г. число ядерных спинов, или кубит, достигло семи и такой компьютер сумел установить "фантастический результат": множителями числа 15 являются числа 5 и 3. В ближайшем будущем от квантового компьютера можно ожидать ещё одного сокрушительного удара в виде феноменального вычисления делителей числа 56. И хотя эти рекорды смешны с точки зрения классических компьютеров, они являются прямым доказательством возможности реализации квантовых вычислительных систем с их невероятно огромными возможностями, превосходящими возможности современных суперкомпьютеров.

Однако кроме чисто вычислительных задач при использовании квантовых объектов можно решить и другие важные проблемы. Среди них создание квантовых криптографических систем и квантовых каналов связи, которые обладают поистине уникальными свойствами, недоступными для классических аналогов. В этом смысле комплекс устройств, реализованных на различных проявлениях квантовых свойств объектов микромира, формирует квантовые информационные системы, которые и являются предметом настоящего изложения.

Данный материал отражает содержание учебного курса "Квантовые информационные системы", который автор читал на факультете компьютерных наук Воронежского государственного университета с 2002 г. для сту-

дентов и магистров, обучающихся по направлениям "Информационные системы и технологии" и "Математика. Компьютерные науки". Содержание данного учебного курса основано на ряде монографий, написанных специалистами в области теоретической физики и квантовой теории информации [6], [9], [11].

В целом, курс ориентирован на студентов, обучающихся по инженерным специальностям, в рамках которых не предусматривается отдельное изучение квантовой теории. В пособии для решения этой проблемы излагаются формальные основы квантовой теории, понимание которых позволяет усвоить материал, относящийся к собственно применению квантовых информационных систем и ознакомлению с их реальными возможностями.

Автор выражает благодарность А.Н. Куракову за помощь при оформлении многочисленного иллюстративного материала и поддержку при использовании возможностей \TeX .

Часть I

Квантовая теория

Глава 1

Основы квантовой теории

Квантовая теория является современной математической моделью для описания физических свойств окружающего мира, состоящего из набора физических систем. Квантовая теория опирается на несколько недоказуемых предложений (постулатов), из которых вытекает адекватное описание физических систем. Так, в основе аксиоматической квантовой теории лежат следующие основные утверждения или постулаты:

- постулат состояния;
- принцип суперпозиции состояний;
- постулат соответствия оператор — физическая величина;
- постулат об измерении;
- постулат об эволюции состояний.

Ниже приведено описание этих постулатов, а также некоторые основные следствия, вытекающие из них, необходимые для понимания идеологии квантовой теории.

1.1 Постулат состояния

Стандартное описание произвольной физической системы опирается на понятие *состояние системы*. Так, в классической теории состояние определяется заданием координат и скоростей всех составных частей системы в определённый момент времени. Однако неспособность классической теории представить адекватное описание таких систем, как атомы, молекулы, ядра, “элементарные” частицы, привела к необходимости пересмотра классического понятия *состояние системы*. В современной квантовой

теории состояние определяется не полным набором численных значений координат и скоростей, а меньшим числом данных иной природы.

Квантовое состояние – это полный набор данных (физических величин), определяющих свойства системы.

Так как состояние – это совокупный набор данных, то можно предположить, что состояние есть объект типа “вектор”. В квантовой теории абстрактное понятие “вектор состояния” обозначается символом $| \rangle$. Так, если некоторый набор данных a_1, a_2, \dots, a_k , определяющих физическую систему, обозначить буквой a , то вектор состояния будет иметь обозначение $|a\rangle$ и называться кет-вектором состояния a . Векторы иных состояний или наборов данных могут быть обозначены $|b\rangle, |n\rangle, |\psi\rangle, |a, b, c \dots\rangle$ и т. д.

В использованных понятиях кет-вектор состояния является абстрактным математическим символом, не связанным с каким-либо числом. Чтобы иметь возможность оперировать этими абстрактными символами состояний, устанавливается их соответствие в общем случае комплексным числам или функциям. С этой целью в квантовой теории вводится ещё один тип векторов, получивших название бра-векторы. Для бра-вектора используется обозначение $\langle b|$, где b – некоторый набор данных.

Такие термины были предложены Дираком [6] и произошли от английского слова bracket (скобка) условным разбиением этого слова на две части: $\langle bra |$ – бра-вектор и $| ket \rangle$ – кет-вектор. В соответствии с терминологией линейной алгебры бра-вектор $\langle a |$ называется “дуальным” (или двойственным) кет-вектору $|a\rangle$.

Для справки напомним, что в линейной алгебре для векторов a и b , состоящих из комплексных компонент, вводится так называемое “внутреннее” произведение, обозначаемое символом $\langle b, a \rangle$. Внутреннее произведение – это правило, по которому вычисляется одно комплексное число из набора комплексных чисел $a(a_1, a_2, \dots, a_n)$, $b(b_1, b_2, \dots, b_n)$:

$$\langle b, a \rangle = \sum_{k=1}^n b_k^* \cdot a_k.$$

Здесь $*$ – значок комплексного сопряжения. При этом внутреннее произведение определяется как функция, удовлетворяющая следующим свойствам:

- линейность: $\langle b, \sum_k \lambda_k a_k \rangle = \sum_k \lambda_k \langle b, a_k \rangle$;
- коммутативность: $\langle b, a \rangle = \langle a, b \rangle^*$;
- положительная определённость: $\langle a, a \rangle \geq 0$.

Аналогично в теории квантовых состояний комплексное число рассматривается как некоторое внутреннее (или “скалярное”) произведение бра- и кет-векторов. Соответственно, для обозначения такого произведения используется символ $\langle b | a \rangle$. Приведённый символ внутреннего произведения бра- и кет-векторов не определяет правила его вычисления, а является лишь его условным обозначением.

Введённое выше обозначение для произведения квантовых состояний $\langle b | a \rangle$ можно по аналогии со скалярным произведением в обычном пространстве рассматривать как “проекцию” вектора $|a\rangle$ на вектор $\langle b|$. Или говорят, что $\langle b | a \rangle$ есть комплексная функция состояния $|a\rangle$ в представлении переменных вектора $\langle b|$. В стандартных обозначениях это может быть записано в виде $\varphi(a, b) \equiv \varphi_a(b) \equiv \langle b | a \rangle$. Правила построения комплексных функций типа $\langle b | a \rangle$ изложены ниже в теории представлений и на данном этапе не существенны для изложения принципов теории.

Так как спроектировать вектор квантового состояния $|a\rangle$ можно на различные бра-векторы, в квантовой теории возникает множественность представления состояния $|a\rangle$ или, другими словами, различное конкретное описание данного квантового состояния системы $\varphi_a(x) = \langle x | a \rangle$ или в другом представлении $\phi_a(u) = \langle u | a \rangle$. Обычно в квантовой теории принята следующая нотация:

$$\varphi_{\text{состояние}}(\text{представление}) = \langle \text{представление} | \text{состояние} \rangle.$$

В связи с возможностью различных способов представления состояния в аксиоматической квантовой теории для сокращения выражений вводится формальная система обозначений, позволяющая избежать конкретного представления квантового состояния. Данную систему обозначений можно проиллюстрировать следующим примером. Пусть есть комплексная функция состояния $|a\rangle$ в представлении $\langle x|$, т. е. $\varphi_a(x) = \langle x | a \rangle$. Очевидно, что данную комплексную функцию можно умножить на комплексное число c : $c\varphi_a(x) = c\langle x | a \rangle$. Так как операция умножения не зависит от выбора представления, то для сокращения можно говорить о возможности умножения вектора состояния на комплексное число и использовать упрощённое обозначение вида $c|a\rangle$.

В общем случае допускается, что введённые векторы квантового состояния можно умножать на комплексное число $c|a\rangle$ и складывать между собой, образуя новые векторы, например:

$$|y\rangle = c_1 |a\rangle + c_2 |b\rangle, \quad (1.1)$$

где c_1 и c_2 — комплексные числа.

В квантовой теории вводится специальное предположение о взаимосвязи бра- и кет-векторов. Бра-вектор, соответствующий кет-вектору $|a\rangle$, есть $\langle a|$. Бра-вектор, соответствующий сумме кет-векторов $|a\rangle + |b\rangle$, является суммой бра-векторов $\langle a| + \langle b|$. Бра-вектор, соответствующий кет-вектору $c|a\rangle$, равен $c^* \langle a|$, здесь c — комплексное число, а c^* — комплексно сопряженное число. В общем виде связь векторов может быть записана следующим образом [6]:

$$(c|a\rangle)^\dagger = c^* \langle a| \quad \text{и} \quad (c\langle a|)^\dagger = c^* |a\rangle, \quad (1.2)$$

где \dagger — значок сопряжения (соответствия двух типов векторов), а c — комплексная константа.

Таким образом, внутреннее (скалярное) произведение квантовых состояний удовлетворяет равенству

$$\langle b|a\rangle = \langle a|b\rangle^*. \quad (1.3)$$

Если выбрать в (1.3) $|b\rangle \equiv |a\rangle$, то число $\langle a|a\rangle$ вещественно и в случае $\langle a|a\rangle \neq 0$ положительно определено:

$$\langle a|a\rangle > 0. \quad (1.4)$$

Как видно, дираковское определение квантового состояния соотносится с определениями, используемыми в линейной алгебре для комплексных векторов. Учитывая “геометрическую” терминологию, введённую для векторов состояния, можно говорить о пространстве векторов состояний. В рассматриваемом пространстве векторов состояний векторы $|a\rangle$ и $|b\rangle$ называются *ортогональными*, если

$$\langle a|b\rangle = 0, \quad (1.5)$$

а соответственно *длина* вектора состояния определяется равенством

$$\|a\| = \sqrt{\langle a|a\rangle}. \quad (1.6)$$

Квантовая теория вводит очень важное предположение о том, что состояние определяется лишь “направлением” вектора в общем пространстве векторов квантовых состояний. Это означает, что сумма состояния с самим собой не приводит к возникновению нового состояния, т. е.

$$c_1|a\rangle + c_2|a\rangle = (c_1 + c_2)|a\rangle \equiv |a\rangle. \quad (1.7)$$

Вектор $(c_1 + c_2)|a\rangle$ соответствует тому же состоянию, что и вектор $|a\rangle$, если $c_1 + c_2 \neq 0$. Другими словами, если вектор состояния умножить на любое не равное нулю комплексное число, то полученный вектор соответствует тому же квантовому состоянию.

Так как для вектора состояния (в соответствии с постулатами теории) существенно лишь его “направление”, то он определен с точностью до произвольного численного множителя. Поэтому можно принять соглашение о единой длине рассматриваемых векторов состояния, которую удобно выбрать равной единице. Такой выбор длины вектора называется *нормировкой*, а вектор — нормированным. Нормировка вектора состояния не определяет его полностью, так как нормированный вектор всё ещё можно умножить на комплексное число, по модулю равное единице, что также не изменит единичной длины вектора, а полученный вектор будет соответствовать тому же состоянию:

$$|a\rangle \equiv e^{i\phi}|a\rangle, \quad \phi - \text{Re.} \quad (1.8)$$

Определённое выше “пространство” квантовых состояний соответствует известному в математике гильбертову пространству, а вектор состояния — лучу в гильбертовом пространстве.

Для справки: *гильбертovo пространство* (**H**) определяется в математике как векторное пространство комплексных чисел **C**, образованных скалярным произведением векторов или лучей в **H**, обозначение которых совпадает с принятым выше обозначением для векторов состояний $|a\rangle$. При этом скалярное произведение лучей $\langle a | b \rangle$ в **H** удовлетворяет следующим свойствам:

- скалярное произведение $\langle a | a \rangle$ положительно определено: $\langle a | a \rangle > 0$;
- скалярное произведение лучей гильбертова пространства удовлетворяет условию линейности вида: $\langle a | c_1 b + c_2 c \rangle = c_1 \langle a | b \rangle + c_2 \langle a | c \rangle$, где c_1 и c_2 — комплексные числа;
- скалярное произведение удовлетворяет эрмитовскому сопряжению: $\langle a | b \rangle = \langle b | a \rangle^*$;
- пространство лучей нормировано по норме: $\|a\| = \sqrt{\langle a | a \rangle}$.

Как видно, данное определение в точности соответствует определению пространства векторов квантовых состояний. По этой причине говорят, что векторы квантовых состояний образуют гильбертово пространство состояний.

1.2 Алгебра операторов

Как определено выше, с векторами квантового состояния можно выполнять определённые математические операции, приводящие к преобразованию состояний. Пусть, например, кет-вектору квантового состояния $|a\rangle$ по определённому правилу соответствует кет-вектор $|b\rangle$. В этом случае можно сказать, что вектор $|b\rangle$ является функцией F от вектора $|a\rangle$. В общем случае перевод состояния $|a\rangle$ в состояние $|b\rangle$ можно рассматривать как выполнение математической операции или как действие оператора \hat{F} на вектор $|a\rangle$ в пространстве векторов состояния. “Шляпка” над буквой отличает символ оператора от обозначения числа или функции. Символически математическая операция преобразования вектора состояния $|a\rangle$ в вектор состояния $|b\rangle$ обозначается соотношением

$$|b\rangle = \hat{F}|a\rangle, \quad (1.9)$$

где \hat{F} – оператор. Естественно, что данное равенство на языке комплексных функций необходимо понимать как $\langle x|b\rangle = \hat{F}_x\langle x|a\rangle$. С учётом определения оператора и вектора квантового состояния операторы, действующие в пространстве векторов состояний, различны при разных представлениях векторов состояний.

По определению оператор – это формальное изображение математической операции. Совокупность общих правил для математических операций образует раздел математики, который называется “Алгебра операторов”. Алгебра операторов не является содержательным элементом физической квантовой теории. Это удобный математический язык, на котором часто излагаются общие принципы теории. В рамках этого языка на примере приложений к векторам состояний вводится несколько важных положений квантовой теории. В связи с этим ниже представлены некоторые общие определения и обозначения, используемые в алгебре операторов.

Обычно предполагается, что оператор обозначает математическую операцию, выполняемую с объектом или функцией справа от оператора. Однако в ряде случаев используются и операторы, которые действуют налево. Это специально оговаривается в дополнительных обозначениях. В общем случае предполагается, что оператор действует направо, что и использовано ниже.

Исходя из определения оператора ясно, что если для любых векторов $|x\rangle$ выполняется равенство $\hat{F}|x\rangle = \lambda|x\rangle$, где λ – число, то оператор яв-

ляется числом $\hat{F} = \lambda$. В общем случае оператор может быть равен нулю, единице, любому действительному или комплексному числу. Таким образом, в соответствии с (1.9) число является частным случаем оператора.

Для операторов вводится понятие равенства операторов. Два оператора \hat{A} и \hat{B} называются *равными*, если для произвольных векторов состояний $|x\rangle$ выполняется равенство $\hat{A}|x\rangle = \hat{B}|x\rangle$. Символически равенство операторов обозначается в виде $\hat{A} = \hat{B}$, которое подразумевает выполнение соотношения $\hat{A}|x\rangle = \hat{B}|x\rangle$. Понятие “больше” (“меньше”) для операторов не вводится и определено только по норме операторов. Норма оператора $\|\hat{F}\|$ является положительно определенным числом, которое может быть задано соотношением $\|\hat{F}\| = \sqrt{\langle b|b\rangle}$, где $|b\rangle = \hat{F}|a\rangle$, $|a\rangle$ – заданный вектор.

Для операторов вводятся обычные алгебраические операции [5], такие как сложение, умножение и т. п. Например, сложение (вычитание) операторов определено по правилу

$$\left(\hat{F}_1 \pm \hat{F}_2\right)|x\rangle = \hat{F}_1|x\rangle \pm \hat{F}_2|x\rangle. \quad (1.10)$$

Произведение двух операторов определяется как результат последовательного действия этих операторов на вектор состояния. Так, в произведении $\hat{A} \cdot \hat{B}$ сначала вычисляется действие оператора \hat{B} на вектор состояния $|x\rangle$, а затем действие оператора \hat{A} на вектор $\hat{B}|x\rangle$. Определение произведения двух операторов легко обобщается на случай произведения произвольного числа операторов в виде последовательного действия операторов справа налево на все, что находится справа от произведения операторов.

В общем случае $\hat{A} \cdot \hat{B}|x\rangle \neq \hat{B} \cdot \hat{A}|x\rangle$ при произвольных $|x\rangle$, т. е. операторы не коммутируют (не переставляются) в произведении. В силу произвольности вектора состояния $|x\rangle$ это соотношение можно записать в операторном виде: $\hat{A} \cdot \hat{B} \neq \hat{B} \cdot \hat{A}$. Чтобы определить возможность или правило перестановки операторов в произведении, вводится понятие коммутатора двух операторов.

Коммутатор двух операторов \hat{A} и \hat{B} обозначается символом $[\hat{A}, \hat{B}]$ и определяется равенством

$$[\hat{A}, \hat{B}] \equiv \hat{A} \cdot \hat{B} - \hat{B} \cdot \hat{A}. \quad (1.11)$$

Если коммутатор двух операторов равен нулю, то такие операторы называются коммутирующими $\hat{A} \cdot \hat{B} = \hat{B} \cdot \hat{A}$ и для них несуществен порядок

их действия при вычислении произведения. Если коммутатор операторов не равен нулю, то правило перестановки операторов определяется выражением (1.11), а именно:

$$\hat{A} \cdot \hat{B} = \hat{B} \cdot \hat{A} + [\hat{A}, \hat{B}]. \quad (1.12)$$

Из определения произведения операторов следует определение *целой положительной степени оператора*:

$$\hat{A}^n \equiv \underbrace{\hat{A} \cdot \hat{A} \cdot \hat{A} \dots \hat{A}}_n. \quad (1.13)$$

Обратный к \hat{A} оператор обозначается символом \hat{A}^{-1} . Обратный оператор определен только тогда, когда уравнение $\hat{A}|x\rangle = |y\rangle$ разрешимо относительно $|x\rangle$. В этом случае $|x\rangle = \hat{A}^{-1}|y\rangle$. По определению

$$\hat{A}^{-1} \cdot \hat{A} = \hat{A} \cdot \hat{A}^{-1} \equiv 1, \quad [\hat{A}, \hat{A}^{-1}] = 0. \quad (1.14)$$

Функция от оператора определяется по аналогии с разложением функции в ряд Тейлора (если такое разложение возможно):

$$\hat{F}(\hat{A}) \equiv \sum_{n=0}^{\infty} \frac{1}{n!} F^{(n)}(0) \cdot \hat{A}^{(n)}, \quad F^{(n)}(0) = \left. \frac{\partial^n F(x)}{\partial x^n} \right|_{x=0}. \quad (1.15)$$

В алгебре операторов вводится понятие линейного оператора. Оператор \hat{F} называется *линейным*, если для него выполняется следующее равенство:

$$\hat{F}(c_1|x_1\rangle + c_2|x_2\rangle) = c_1\hat{F}|x_1\rangle + c_2\hat{F}|x_2\rangle, \quad (1.16)$$

где c_1, c_2 — произвольные комплексные числа.

Ещё одним важным для квантовой теории классом операторов является класс самосопряжённых (эрмитовых) операторов. Оператор \hat{F} , удовлетворяющий условию

$$\langle F^\dagger b | a \rangle = \langle b | \hat{F}a \rangle; \quad \langle b | \hat{F}a \rangle \equiv \langle b | \hat{F} | a \rangle, \quad (1.17)$$

называется самосопряжённым (или эрмитовским) оператором, что символически выражается операторным равенством $F = F^\dagger$. Из определения самосопряжённого оператора следует, что если операторы \hat{A} и \hat{B} самосопряжённые, то и сумма операторов $\hat{A} + \hat{B}$ также является самосопряжённым оператором.

Рассмотрим соотношение (1.17) для произведения самосопряжённых операторов. По определению

$$\langle b | \hat{A} \cdot \hat{B} | a \rangle = \langle \hat{A}^\dagger b | \hat{B} | a \rangle = \langle \hat{B}^\dagger \hat{A}^\dagger b | a \rangle = \langle (\hat{A} \cdot \hat{B})^\dagger b | a \rangle. \quad (1.18)$$

Таким образом, $(\hat{A}\hat{B})^\dagger = \hat{B}^\dagger\hat{A}^\dagger$. В результате оператор $\hat{R} = \hat{A} \cdot \hat{B}$ самосопряжён, если $[\hat{A}, \hat{B}] = 0$.

Помимо внутреннего произведения бра- и кет-векторов можно рассмотреть их произведение следующего вида: $|a\rangle\langle b|$. Такое произведение векторов состояний называется прямым произведением. Нетрудно установить, что прямое произведение векторов состояний является оператором, который действует как на кет-векторы, так и на бра-векторы.

Составим, например, внутреннее произведение $|a\rangle\langle b|$ с кет-вектором $|x\rangle$. В результате получим $|a\rangle\langle b|x\rangle$. Но $\langle b|x\rangle$ – это по определению комплексное число $\langle b|x\rangle = c$. Следовательно, при действии $|a\rangle\langle b|$ на вектор $|x\rangle$ получился вектор $|y\rangle = c|a\rangle$. А это соответствует действию оператора на вектор $|x\rangle$, в результате которого данное состояние преобразовано в состояние $|y\rangle$. Таким образом, $|a\rangle\langle b|$ есть линейный оператор, который действует на кет-векторы. Составляя внутреннее произведение $|a\rangle\langle b|$ с бра-вектором $\langle x|$ слева, получим бра-вектор $\langle b|$, умноженный на число $\langle x|a\rangle$. То есть $|a\rangle\langle b|$ – оператор, действующий как на бра-, так и на кет-состояния, при этом

$$(|a\rangle\langle b|)^\dagger = |b\rangle\langle a|. \quad (1.19)$$

Введём в рассмотрение понятие “ортонормированный базис” пространства векторов состояний $E = \{|e_n\rangle\}$ как набор состояний, удовлетворяющих условиям

$$\langle e_n | e_m \rangle = 0 \quad \text{при} \quad n \neq m \quad \text{и} \quad \langle e_n | e_n \rangle = 1. \quad (1.20)$$

Размерность пространства определяется числом ортонормированных векторов, составляющих базис. В общем случае пространство может иметь конечную или бесконечную размерность.

При заданном ортонормированном базисе любой вектор (размерности базиса) может быть представлен в виде

$$|x\rangle = \sum_n \lambda_n |e_n\rangle, \quad \text{где} \quad \lambda_n = \langle e_n | x \rangle. \quad (1.21)$$

Соответственно, линейный оператор \hat{F} в пространстве векторов состояний имеет вид

$$\hat{F} = \sum_{n,m} f_{n,m} |e_n\rangle \langle e_m|, \quad \text{где} \quad f_{n,m} = \langle e_n | \hat{F} | e_m \rangle. \quad (1.22)$$

Отсюда вытекает, что для единичного оператора $\hat{F} = 1$, $f_{n,m} = 0$ при

$n \neq m$ и $f_{n,n} = 1$, и, следовательно, имеет место равенство

$$1 = \sum_n |e_n\rangle \langle e_n|. \quad (1.23)$$

Кроме представленных выше определений, в квантовой теории имеют важное значение унитарные операторы и операторы проектирования.

Оператор \hat{F} называется унитарным, если $\hat{F}^\dagger = \hat{F}^{-1}$.

Оператор \hat{F} называется оператором проектирования, если $\hat{F}^2 = \hat{F}$.

Для произвольного оператора вводится понятие собственного вектора оператора. *Вектор $|x\rangle$ называется собственным вектором оператора \hat{F} , если для некоторой константы f имеет место равенство $\hat{F}|x\rangle = f|x\rangle$.* При этом константа f называется собственным значением оператора, соответствующим вектору $|x\rangle$.

Упражнение 1.1. Вычислить коммутаторы операторов

$$\left[x, \frac{d}{dx} \right], \quad \left[\frac{d}{dx}, \frac{d}{dy} \right].$$

Упражнение 1.2. Определить, какие из перечисленных операторов линейны: оператор дифференцирования, оператор извлечения квадратного корня, оператор комплексного сопряжения, третья степень линейного оператора \hat{F} .

Упражнение 1.3. Доказать, что операторы

$$\hat{A} \cdot \hat{B} + \hat{B} \cdot \hat{A} \quad \text{и} \quad i(\hat{A} \cdot \hat{B} - \hat{B} \cdot \hat{A})$$

всегда самосопряжёны. Здесь i — мнимая единица.

1.3 Принцип суперпозиции состояний

Принцип суперпозиции квантовых состояний является одним из фундаментальных постулатов квантовой теории и утверждает, что между квантовыми состояниями существуют особые соотношения, которые проявляются нетривиальным способом. А именно, *если система находится в определённом состоянии, то можно одновременно считать, что она находится отчасти в двух или нескольких других состояниях, или в суперпозиции состояний.*

Суперпозиция квантовых состояний не имеет аналога в классической теории и является утверждением, которое формулирует принцип на основе специально разработанного математического аппарата и схемы его

применения. Схема является физической теорией, если устанавливаются законы, связывающие математический аппарат с физически наблюдаемыми процессами и явлениями. Именно эти законы и определяют квантовую теорию в целом.

По смыслу суперпозиция состояний оперирует с векторами состояний, которые можно “складывать”, получая величины того же рода. Кроме того, введённые векторы квантовых состояний можно умножать на комплексное число $c |a\rangle$ и складывать между собой, образуя новые векторы, например

$$|y\rangle = c_1 |a\rangle + c_2 |b\rangle, \quad (1.24)$$

где c_1 и c_2 — комплексные числа. В общем случае суперпозиция произвольного числа состояний имеет вид

$$|y\rangle = \sum_n c_n |x_n\rangle, \quad (1.25)$$

где c_n — комплексные числа.

В соответствии с принципом суперпозиции, если вектор $|a, d, x \dots\rangle$ зависит, например, от x , то в силу возможности сложения векторов можно проинтегрировать вектор по x и получить новый вектор:

$$|y\rangle = \int |a, d, x \dots\rangle dx. \quad (1.26)$$

В суперпозиции двух или большего числа состояний порядок, в котором выполняется суперпозиция состояний, несуществен. Кроме того, если коэффициенты суперпозиции не равны нулю, то соотношение суперпозиции между всеми состояниями симметрично. Так, в (1.24) вектор состояния $|a\rangle$ образован суперпозицией векторов состояний $|y\rangle$ и $|b\rangle$. Аналогично вектор состояния $|b\rangle$ может быть образован суперпозицией векторов состояний $|a\rangle$ и $|y\rangle$. Так как в квантовой теории постулируется, что умножение вектора состояния на любое не равное нулю комплексное число даёт вектор, соответствующий тому же квантовому состоянию, это утверждение определяет коренное различие между понятиями квантовой и классической суперпозиции. Соответственно, если равенство (1.24) умножить на комплексное число α , то, так как вектор $\alpha |y\rangle$ не меняет состояния $|y\rangle$, для определения состояния $|y\rangle$ в (1.24) существенно лишь отношение комплексных коэффициентов c_1 и c_2 . Или, другими словами, нормированная суперпозиция двух состояний определяется двумя вещественными параметрами, так как в соответствии с (1.8) общий фазовый множитель также не меняет исходного состояния.

Введённое ранее скалярное произведение бра- и кет-векторов обеспечивает выполнение принципа суперпозиции и является линейной функцией состояния $|a\rangle$, так как по определению имеет место равенство

$$\langle d| \{c_1|a\rangle + c_2|b\rangle\} = c_1\langle d|a\rangle + c_2\langle d|b\rangle, \quad (1.27)$$

где c_1 и c_2 — произвольные комплексные числа.

Так как бра-вектор определён полностью, если задано его скалярное произведение с любым кет-вектором, то *сумма бра-векторов* $\langle b| + \langle c|$ определяется из условия

$$\{\langle b| + \langle c|\}|a\rangle \equiv \langle b|a\rangle + \langle c|a\rangle. \quad (1.28)$$

Соответственно, произведение бра-вектора на комплексное число c определяется равенством

$$\{c\langle b|\}|a\rangle \equiv c\langle b|a\rangle. \quad (1.29)$$

На основании (1.27) и (1.28) ясно, что определённое выше скалярное произведение удовлетворяет дистрибутивному закону умножения, а из (1.27) и (1.29) вытекает, что умножение бра- и кет-векторов на число удовлетворяет обычной алгебре чисел.

Если в суперпозиции двух состояний (1.24) состояния $|a\rangle$ и $|b\rangle$ ортогональны и нормированы, то из условия нормировки состояния $|y\rangle$ следует

$$\langle y|y\rangle = |c_1|^2 + |c_2|^2 = 1. \quad (1.30)$$

В случае суперпозиции произвольного числа ортонормированных состояний имеем

$$\langle y|y\rangle = \sum_n |c_n|^2 = 1. \quad (1.31)$$

Упражнение 1.4. Доказать равенство (1.30).

Упражнение 1.5. Доказать равенство (1.31).

1.4 Постулат соответствия оператора физической величине

Физические величины, использующиеся при классическом описании системы, такие как координаты, скорости, импульсы, моменты импульсов, энергия, а также функции от этих величин называются *динамическими переменными*.

Утверждение рассматриваемого постулата квантовой теории состоит в том, что *динамическим переменным системы соответствуют линейные самосопряжённые операторы, определённые в тот же момент времени, что и векторы состояния*.

Другими словами, физической величине F ставится в соответствие линейный, самосопряжённый (эрмитовский) оператор $\hat{F}: F \Rightarrow \hat{F}$.

Уравнение на собственные векторы и собственные значения оператора \hat{F} имеет вид

$$\hat{F} |a\rangle = \alpha |a\rangle, \quad (1.32)$$

где α — число. Если уравнение (1.32) выполняется, то α называется собственным значением оператора \hat{F} , а вектор $|a\rangle$ — собственным вектором оператора \hat{F} .

Решение уравнения (1.32) может иметь место при различных значениях α , в том числе и образующих дискретный ряд чисел $\alpha \in \alpha_1 \alpha_2 \dots \alpha_n \dots$. В этом случае принято данное уравнение писать в виде

$$\hat{F} |a_n\rangle = \alpha_n |a_n\rangle. \quad (1.33)$$

В данном случае каждому собственному числу α_n соответствует собственный вектор $|a_n\rangle$. Совокупность всех собственных чисел α_n называется *спектром оператора*. Если спектр состоит из набора дискретных чисел, то спектр называется *дискретным*.

В случае если одному собственному числу соответствует несколько векторов состояний

$$\hat{F} |a_{nk}\rangle = \alpha_n |a_{nk}\rangle, \quad k \in 1, 2, \dots, f, \quad (1.34)$$

то спектр называется *вырожденным*, а число различных состояний f , соответствующих одному собственному значению, — *кратностью вырождения*.

Если решение уравнения (1.32) возможно при произвольном значении α , то спектр называется *непрерывным*.

В квантовой теории используются только линейные, самосопряжённые (эрмитовские) операторы. Линейность операторов квантовой теории обеспечивает выполнение принципа суперпозиции.

Для самосопряжённых операторов установлено несколько общих утверждений, вытекающих из (1.33) и (1.34), которые для систематизации изложим в виде следующих теорем [5].

Теорема 1.1. *Собственные значения самосопряжённого оператора — вещественные числа.*

Для доказательства рассмотрим систему двух уравнений, составленных из уравнения (1.33) и уравнения, сопряжённого с (1.33):

$$\hat{F} |a_n\rangle = \alpha_n |a_n\rangle; \quad \langle F^\dagger a_n | = \alpha_n^* \langle a_n|. \quad (1.35)$$

Образуем из данных уравнений скалярные произведения, “умножая” первое уравнение на бра-вектор $\langle a_n |$ слева, а второе – на кет-вектор $|a_n \rangle$ справа. В результате получим пару уравнений вида

$$\langle a_n | \hat{F} a_n \rangle = \alpha_n \langle a_n | a_n \rangle; \quad \langle F^\dagger a_n | a_n \rangle = \alpha_n^* \langle a_n | a_n \rangle. \quad (1.36)$$

Вычитая второе равенство из первого в (1.36), найдем:

$$\langle a_n | \hat{F} a_n \rangle - \langle F^\dagger a_n | a_n \rangle = (\alpha - \alpha_n^*) \langle a_n | a_n \rangle. \quad (1.37)$$

На основании определения (1.17) имеем $\langle a_n | \hat{F} a_n \rangle - \langle F^\dagger a_n | a_n \rangle = 0$ и, следовательно, $\alpha - \alpha_n^* = 0$, так как $\langle a_n | a_n \rangle > 0$. Таким образом, $\alpha = \alpha_n^*$, что и доказывает действительность собственного числа эрмитовского оператора с дискретным спектром. Случай оператора с непрерывным спектром рассматривается аналогично.

Теорема 1.2. Собственные значения, соответствующие сопряжённым бра- и кет-состояниям, совпадают.

Теорема 1.3. Бра-вектор, сопряжённый с кет-вектором, является собственным вектором, относящимся к тому же собственному значению, что и кет-вектор, и обратно.

Теорема 1.4. Собственные векторы самосопряжённого оператора ортонормированы (ортогональны и нормированы).

В случае если спектр оператора дискретный, условие ортонормировки состояний имеет вид

$$\langle a_n | a_m \rangle = \delta_{nm}, \quad (1.38)$$

где δ_{nm} – символ Кронекера.

В случае если спектр оператора непрерывен, уравнение (1.33) имеет следующий вид:

$$\hat{F} |x\rangle = \alpha |x\rangle, \quad (1.39)$$

где α – любое число на отрезке $\alpha_{min} \leq \alpha \leq \alpha_{max}$. Условие ортонормировки собственных векторов оператора с непрерывным спектром есть

$$\langle x | x' \rangle = \delta(x - x'). \quad (1.40)$$

Здесь $\delta(x)$ – дельта-функция Дирака.

Теорема 1.5. Набор собственных векторов эрмитовского оператора – полный.

Условие полноты векторов состояний означает, что произвольный вектор можно представить в виде разложения по полной системе собственных векторов оператора \hat{F} для дискретного или непрерывного спектра:

$$|A\rangle = \sum_n c_n |n\rangle; \quad |A\rangle = \int c_x |x\rangle dx. \quad (1.41)$$

Здесь коэффициенты разложения c_n и c_x равны соответственно

$$c_n = \langle n | A \rangle, \quad c_x = \langle x | A \rangle. \quad (1.42)$$

На языке операторов условие полноты можно записать в виде (1.23), которое часто называют дираковским разложением единицы:

$$\sum_n |n\rangle \langle n| = 1 \quad \text{или} \quad \int |x\rangle \langle x| dx = 1. \quad (1.43)$$

Динамические переменные, собственные состояния которых образуют полную систему, называются *наблюдаемыми*. Другими словами, свойство системы, которое может быть измерено, есть “наблюдаемая”.

Не всякая динамическая переменная в конкретной физической системе обладает достаточным количеством собственных состояний, чтобы образовать полную систему. Переменные, собственные состояния которых не образуют полной системы, не являются наблюдаемыми и не могут быть измерены.

В заключение подчеркнём, что центральным элементом данного постулата является утверждение теории о сопоставлении физической величине линейного, эрмитовского оператора. Вид операторов для конкретных физических величин зависит от способа представления состояний и будет рассмотрен в разделе “Теория представлений”.

Упражнение 1.6. Доказать **Теорему 1.2**.

Упражнение 1.7. Доказать **Теорему 1.3**.

Упражнение 1.8. Доказать **Теорему 1.4** на примере оператора, обладающего дискретным спектром.

Упражнение 1.9. Доказать равенства (1.42).

1.5 Постулат об измерении физической величины

В квантовой теории постулируется, что *результатом измерения динамической переменной (или физической величины) является число, принадлежащее спектру оператора этой физической величины*. Кроме того, *в результате процесса измерения вектор состояния системы изменяется и становится собственным для оператора этой физической величины*.

Таким образом, если до измерения квантовая система определялась вектором состояния $|\psi\rangle$ и в этой системе проводится измерение величины F , которой соответствует самосопряжённый оператор \hat{F} , то [11]:

- 1) необходимо определить собственные векторы и собственные значения оператора \hat{F} , например в случае дискретного невырожденного спектра из решения уравнения

$$\hat{F} |n\rangle = f_n |n\rangle, \quad n = 1, 2, \dots; \quad (1.44)$$

- 2) результатом измерения может быть только одно из чисел f_n ;
- 3) вероятность w измерения числа f_n определяется квадратом модуля коэффициента разложения состояния $|\psi\rangle$ по полному набору ортонормированных собственных состояний $|n\rangle$ оператора \hat{F} :

$$|\psi\rangle = \sum_n a_n |n\rangle; \quad a_n \equiv \langle n | \psi \rangle, \quad (1.45)$$

$$w(f_n) = |\langle n | \psi \rangle|^2 = \langle \psi | n \rangle \langle n | \psi \rangle \equiv \langle \psi | \hat{P}_n | \psi \rangle, \quad (1.46)$$

здесь введен оператор $\hat{P}_n \equiv |n\rangle \langle n|$, который является оператором проектирования на состояние $|n\rangle$, так как $P_n^2 = P_n$ и

$$\hat{P}_n \hat{P}_m = \delta_{nm} \hat{P}_n, \quad \hat{P}_n^\dagger = \hat{P}_n; \quad (1.47)$$

- 4) в результате измерения состояние системы $|\psi\rangle$ редуцируется в состояние $|\psi\rangle \Rightarrow |\Phi_n\rangle = N \hat{P}\psi$, которое является собственным для оператора \hat{F} . $\hat{F} |\Phi_n\rangle = f_n |\Phi_n\rangle$. Здесь N – нормировочная константа. Другими словами, любое последующее измерение физической величины F в заданной системе будет приводить к значению f_n с вероятностью, равной единице.

Нормированное состояние после измерения $|\Phi_n\rangle$ имеет вид

$$|\Phi_n\rangle = \frac{1}{\sqrt{\langle \psi | \hat{P} | \psi \rangle}} \cdot \hat{P}_n |\psi\rangle, \quad (1.48)$$

так как условие нормировки означает выполнение равенства

$$\langle \Phi_n | \Phi_n \rangle = N^2 \langle \hat{P}_n^\dagger \psi | \hat{P}_n \psi \rangle = N^2 \langle \psi | \hat{P}_n \hat{P}_n | \psi \rangle = N^2 \langle \psi | \hat{P}_n | \psi \rangle = 1. \quad (1.49)$$

Откуда и находим:

$$N = \frac{1}{\sqrt{\langle \psi | \hat{P}_n | \psi \rangle}}. \quad (1.50)$$

Как следует из постулата об измерении физической величины, процесс измерения в квантовой теории носит вероятностный характер. Теория предсказывает лишь вероятность измерения конкретного значения. Согласование теории с экспериментом осуществляется путём проведения много-кратных измерений. Многократное повторение измерения в системе предполагает наличие ансамбля систем в состоянии $|\psi\rangle$. В этом случае можно ввести понятие среднего значения физической величины, которое будет получено в результате многократных измерений в данном ансамбле состояний. Обозначим среднее значение величины F символом $\langle F \rangle$, тогда по определению теории вероятности с учетом соотношения (1.46) получим:

$$\langle F \rangle = \sum_n f_n w(f_n) = \sum_n f_n \cdot |\langle n | \psi \rangle|^2 = \sum_n f_n \langle \psi | n \rangle \langle n | \psi \rangle. \quad (1.51)$$

С учётом (1.44) и условия полноты (1.43) данное равенство можно преобразовать следующим образом:

$$\langle F \rangle = \sum_n \langle \psi | \hat{F} | n \rangle \langle n | \psi \rangle = \langle \psi | \hat{F} | \psi \rangle. \quad (1.52)$$

Выражение $\langle \psi | \hat{F} | \psi \rangle$ определяет правило вычисления среднего значения произвольной физической величины, полученной в результате многократного повторения процесса измерения F в ансамбле состояний $|\psi\rangle$.

Из постулата соответствия оператор – физическая величина и постулата об измерении вытекает теорема, которая устанавливает принцип неопределённости для физических величин и формулируется следующим образом.

Теорема 1.6. Если для произвольных линейных эрмитовских операторов \hat{F} и \hat{M} выполняется равенство

$$[\hat{F}, \hat{M}] = i\hat{K}, \quad (1.53)$$

где i – мнимая единица, \hat{K} – линейный эрмитовский оператор, то для операторов среднеквадратичных отклонений

$$\Delta \hat{F}^2 = (\hat{F} - \langle F \rangle)^2 \quad \text{и} \quad \Delta \hat{M}^2 = (\hat{M} - \langle M \rangle)^2$$

имеет место неравенство

$$\langle (\Delta \hat{F})^2 \rangle \langle (\Delta \hat{M})^2 \rangle \geq \frac{\langle \hat{K}^2 \rangle}{4}. \quad (1.54)$$

Содержательная часть данной теоремы состоит в том, что физические величины F и M могут быть измерены точно в одном состоянии только при условии, если их операторы коммутируют друг с другом.

Выражение (1.54) часто называют соотношением неопределённости для физических величин.

Упражнение 1.10. Доказать равенство (1.54) (см. [5]).

1.6 Постулат об эволюции квантовых состояний

Данный постулат утверждает, что *квантовое состояние реальной физической системы зависит от времени $|\psi(t)\rangle$ и развитие состояния во времени (эволюция) определяется уравнением*

$$i\hbar \frac{\partial}{\partial t} |\psi(t)\rangle = \hat{H} |\psi(t)\rangle. \quad (1.55)$$

Здесь i — мнимая единица, $\hbar \approx 1.06 \cdot 10^{-27}$ эрг · с — постоянная Планка; оператор \hat{H} — специальный линейный самосопряжённый оператор, который носит название оператора Гамильтона, или гамильтонiana системы, и определяется как сумма операторов кинетической энергии T и потенциальной функции U :

$$\hat{H} = \hat{T} + \hat{U}. \quad (1.56)$$

В случае когда потенциальная функция не зависит от времени, U совпадает с потенциальной энергией системы. Явный вид этих операторов устанавливается в теории представлений (см. ниже).

Если гамильтониан системы не зависит от времени, то состояние $|\psi(t)\rangle$ является собственным состоянием оператора Гамильтона:

$$\hat{H} |\psi(t, E_n)\rangle = E_n |\psi(t, E_n)\rangle, \quad (1.57)$$

и, как следует из (1.55), зависимость такого состояния от времени определяется выражением

$$|\psi(t, E_n)\rangle = \exp\left(-i\frac{E_n}{\hbar}t\right) |E_n\rangle. \quad (1.58)$$

Здесь E_n определяет энергию системы, как это следует из соображений размерности. В квантовой теории состояния типа (1.58) называются стационарными квантовыми состояниями.

Эволюция состояния $|\psi(t)\rangle$ во времени может быть описана на языке оператора эволюции, который связывает состояния в различные моменты времени. Так, если в начальный момент $t = 0$ исходное состояние обозначить $|\psi(0)\rangle$, то состояние в момент времени t определяется выражением

$$|\psi(t)\rangle = \hat{U}(t) |\psi(0)\rangle. \quad (1.59)$$

Здесь $\hat{U}(t)$ называется оператором эволюции.

Подставляя (1.59) в (1.55), нетрудно получить операторное уравнение для оператора эволюции:

$$i\hbar \frac{\partial}{\partial t} \hat{U} = \hat{H} \hat{U}. \quad (1.60)$$

Из последнего уравнения следует, что если \hat{H} не зависит от времени, то оператор эволюции равен

$$\hat{U}(t) = \exp\left(-\frac{i}{\hbar} \hat{H} \cdot t\right). \quad (1.61)$$

После изложения общих принципов квантовой теории, можно ещё раз вернуться к понятию состояния квантовой системы. В определении состояния утверждается, что состояние – это полный набор переменных, характеризующих систему. В общем случае этот набор переменных устанавливается как совокупность физических величин, операторы которых коммутируют друг с другом.

Упражнение 1.11. Доказать равенство (1.58).

Упражнение 1.12. Объяснить, почему E_n в (1.58) имеет размерность энергии.

Упражнение 1.13. Вывести равенство (1.61).

1.7 Представление квантовых состояний и операторов

Изложенная выше формальная аксиоматическая схема квантовой теории, построенная в воображаемом гильбертовом пространстве, не является физической теорией. Представленная схема не позволяет ответить на вопрос о том, как конкретно изложенные принципы связаны с физическими системами и наблюдаемыми, не устанавливает явного вида операторов физических величин и соответствия этих операторов известным математическим операторам. Физическое “оживление” квантовой теории осуществляется на основе так называемой теории представлений. Теория представлений устанавливает связь квантовых состояний с комплексными числами, а операторов с математическими операциями над полем комплексных чисел [6], [5].

Как следует из определения квантовых состояний, комплексные числа образуются при скалярном произведении векторов состояний. При этом не были сформулированы правила построения или нахождения скалярных произведений векторов состояний.

Для формулировки основных понятий теории представления состояний введём следующую терминологию. Пусть x означает координату, p — импульс, E — энергию. Будем называть векторы состояний физических величин следующим очевидным образом:

- $|x\rangle$ — состояние с определённым значением координаты;
- $|p\rangle$ — состояние с определённым значением импульса;
- $|E_n\rangle$ — состояние с определённым значением энергии;
- $|F_n\rangle$ — состояние с определённым значением физической величины F и т. д.

В теории представлений вводится основное понятие, которое определяется *функцией состояния* $|A\rangle$ в *F-представлении* по следующему определению:

$$\Psi_{\text{состояние } A} (\text{F-представление}) \equiv \langle \text{F-представление} | \text{состояние } A \rangle. \quad (1.62)$$

В соответствии с (1.62), например, следующие скалярные произведения будут именоваться:

- $\langle x | p \rangle$ — функция состояния с определённым значением импульса в координатном представлении;
- $\langle p | x \rangle$ — функция состояния с определённым значением координаты в импульсном представлении;
- $\langle x | E_n \rangle$ — функция состояния с определённым значением энергии в координатном представлении;
- $\langle F_n | A \rangle$ — функция состояния с определённым значением физической величины A в *F-представлении* и т. п.

По определению функция состояния в заданном представлении является в общем случае комплексной функцией своих переменных, для которой применимы стандартные правила теории функций комплексной переменной. На основании (1.3) видно, что имеется полная симметрия между переменными, определяющими состояния, и переменными, определяющими представление, так как

$$\Psi_{\text{состояние } A} (\text{F-представление}) \equiv \Psi^*_{\text{состояние } F} (A\text{-представление}). \quad (1.63)$$

Таким образом, если в качестве переменных представления используются координаты системы, то говорят о координатном представлении квантовой теории. Если в качестве переменных представления используются импульсы частиц, образующих систему, то говорят об импульсном представлении. Наконец, если в качестве переменных представления используется энергия, то говорят об энергетическом представлении теории.

По историческим причинам в квантовой теории координатное представление имеет в некотором смысле преимущественное значение. Такая квантовая теория построена Шрёдингером и приводит к хорошо разработанному способу описания системы, основанному на решении специального дифференциального уравнения. При этом решение уравнения Шрёдингера $\Psi(x, t)$ зависит от координат и времени и называется волновой функцией. Термин “волновая функция” закрепился за решением этого уравнения по историческим причинам. Реально данная функция не обязательно имеет вид решения волнового уравнения и не всегда имеет волновую структуру.

Энергетическое представление было использовано Гейзенбергом и привело к формулировке матричной квантовой механики. По сути, можно построить и другие представления квантовой теории, однако они не получили столь широкого применения, как координатное представление.

Аналогично способу задания соответствия состояний и комплексных функций необходимо ввести правила задания соответствия для операторов, действующих в формальном математическом гильбертовом пространстве, математическим операциям, определённым над полем комплексных чисел (функций) в заданном представлении.

Любое преобразование векторов состояний под действием оператора в общем случае имеет вид

$$|A\rangle = \hat{S} |B\rangle, \quad (1.64)$$

где \hat{S} – линейный, самосопряжённый оператор. Установим вид равенства (1.64) в произвольном F -представлении.

Пусть, например, физической величине F соответствует линейный эрмитовский оператор \hat{F} , собственные значения f_n которого образуют дискретный спектр:

$$\hat{F} |n\rangle = f_n |n\rangle, \quad n = 1, 2, \dots \quad (1.65)$$

Разложения состояний $|A\rangle$ и $|B\rangle$ из (1.64) по полному набору состояний $|n\rangle$ имеют вид

$$|A\rangle = \sum_n a_n |n\rangle = \sum_n |n\rangle \langle n |A\rangle, \quad (1.66)$$

$$|B\rangle = \sum_n b_n |n\rangle = \sum_n |n\rangle \langle n |B\rangle. \quad (1.67)$$

Подставляя (1.66) и (1.67) в (1.64) и умножая скалярно полученное равенство на $\langle m |$ слева, находим:

$$\langle m | A \rangle = \sum_n \langle m | \hat{S} | n \rangle \langle n | B \rangle, \quad m, n \in 1, 2, \dots \quad (1.68)$$

Если ввести для краткости обозначение $\langle m | \hat{S} | n \rangle \equiv S_{mn}$, то видно, что уравнение (1.68) является матричным уравнением, связывающим набор комплексных чисел (функций) $\langle m | A \rangle$ ($m = 1, 2, \dots$) с набором комплексных чисел (функций) $\langle n | B \rangle$ ($n = 1, 2, \dots$). Каждый из этих наборов образует функции состояния $|A\rangle$ или состояния $|B\rangle$ в F -представлении. В результате соотношение (1.68) можно переписать в матричном виде:

$$\begin{pmatrix} \langle 1 | A \rangle \\ \langle 2 | A \rangle \\ \vdots \\ \langle k | A \rangle \\ \vdots \end{pmatrix} = \begin{pmatrix} S_{11} & S_{12} & S_{13} & \dots \\ S_{21} & S_{22} & \dots & \dots \\ \dots & \dots & \dots & \dots \\ S_{k1} & S_{k2} & \dots & \dots \end{pmatrix} \begin{pmatrix} \langle 1 | B \rangle \\ \langle 2 | B \rangle \\ \vdots \\ \langle k | B \rangle \\ \vdots \end{pmatrix} \quad (1.69)$$

Таким образом, вектор состояния, определённый набором комплексных чисел $\langle n | A \rangle$, получается из вектора состояния, определённого набором комплексных чисел $\langle n | B \rangle$, путём действия оператора, имеющего вид матрицы S , элементы которой S_{nm} называются матричными элементами оператора \hat{S} . Фактически равенство (1.69) и определяет вид оператора \hat{S} в F -представлении.

Рассмотрим один тривиальный, но чрезвычайно важный пример. Пусть оператор \hat{S} совпадает с оператором \hat{F} , физическая величина которого выбрана в качестве переменной представления. В этом случае на основании (1.65) имеем

$$\langle m | \hat{S} | n \rangle \equiv \langle m | \hat{F} | n \rangle = f_n \langle m | n \rangle = f_n \delta_{nm}, \quad (1.70)$$

где δ_{nm} — символ Кронекера. Таким образом, *оператор в своем собственном представлении есть диагональная матрица, на главной диагонали которой стоят собственные числа оператора*

$$\hat{F} \rightarrow \begin{pmatrix} f_1 & 0 & 0 & \dots \\ 0 & f_2 & 0 & \dots \\ 0 & 0 & f_3 & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix} \quad (1.71)$$

Как следует из изложенного выше примера, размерность матрицы оператора определяется числом собственных состояний $|n\rangle$. Так, если оператор имеет только два собственных состояния, то операторы, действующие в пространстве этих двух состояний, являются квадратными матрицами размерности 2×2 . При числе состояний n образуются квадратные матрицы размерности $n \times n$. Для случая бесконечного числа состояний операторами являются квадратные матрицы бесконечной размерности.

Приведённые выше выражения справедливы для случая, когда оператор \hat{F} имеет дискретный спектр. Если спектр оператора \hat{F} непрерывный, то уравнение (1.65) есть

$$\hat{F}|F\rangle = f|F\rangle, \quad (1.72)$$

где f — собственное число, принимающее непрерывный ряд значений. В результате разложения векторов состояний $|A\rangle$ и $|B\rangle$ по полному набору состояний $|F\rangle$ принимает вид

$$|A\rangle = \int a_F |F\rangle dF = \int |F\rangle \langle F|A\rangle dF, \quad (1.73)$$

$$|B\rangle = \int b_F |F\rangle dF = \int |F\rangle \langle F|B\rangle dF. \quad (1.74)$$

Действуя далее аналогично выводу уравнения (1.68), получим интегральное равенство

$$\langle F|A\rangle = \int \langle F|\hat{S}|F'\rangle \langle F'|B\rangle dF'. \quad (1.75)$$

Таким образом, если спектр оператора физической величины, использующейся в качестве переменной представления, непрерывен, то оператор \hat{S} является ядром интегрального преобразования.

В случае если $\hat{S} \equiv \hat{F}$, т. е. оператор совпадает с оператором представления, ядро интегрального преобразования (1.75) существенно упрощается:

$$\langle F|\hat{S}|F'\rangle \equiv \langle F|\hat{F}|F'\rangle = S_{FF'} = f'\delta(F - F'), \quad (1.76)$$

где $\delta(F - F')$ — дельта-функция Дирака. Интегрирование в (1.68) снимается, и оператор в этом частном случае (оператор в своем собственном представлении) является бесконечно мерной непрерывной диагональной матрицей, на главной диагонали которой расположены собственные значения оператора:

$$\langle F|A\rangle = f\langle F|B\rangle.$$

Таким образом, оператор в своём собственном представлении (для случая непрерывного спектра) является просто умножением на данную физическую величину.

Например, координата (частицы) x принимает непрерывный ряд значений. Ядро интегрального преобразования (1.75) оператора координаты в координатном представлении в соответствии с (1.75) и (1.76) есть

$$\langle x|\hat{x}|x'\rangle = x'\langle x|x'\rangle = x'\delta(x - x'). \quad (1.77)$$

На основании (1.77) можно заключить, что оператор координаты в координатном представлении есть умножение на координату x ($\hat{x} \equiv x$), а уравнение (1.64) в координатном представлении имеет вид

$$\langle x | A \rangle = x \langle x | B \rangle. \quad (1.78)$$

Аналогично, если импульс частицы в системе принимает непрерывный ряд значений, получим, что оператор импульса \hat{p} в импульсном представлении есть умножение на импульс $\hat{p} = p$.

Как уже отмечалось выше, конкретный вид уравнений квантовой механики может быть получен в представлении различных физических величин или динамических переменных. Исторически первые уравнения квантовой теории были установлены независимо в координатном (Шредингер) и энергетическом (Гейзенберг) представлениях. Так, уравнение (1.55) в координатном представлении имеет вид

$$i\hbar \frac{\partial}{\partial t} \langle x | \psi \rangle = \hat{H} \langle x | \psi \rangle. \quad (1.79)$$

Здесь $\langle x | \psi \rangle \equiv \psi(x, t)$ – волновая функция в координатном представлении, а \hat{H} – оператор Гамильтона в координатном представлении.

Например, для одной частицы массы m , находящейся в потенциальном поле с потенциальной энергией $U(x)$ (одномерный случай), оператор \hat{H} есть

$$\hat{H} = \hat{T} + \hat{U} = \frac{\hat{p}^2}{2m} + U(x). \quad (1.80)$$

Для определения явного вида \hat{H} в координатном представлении необходимо установить вид оператора импульса в координатном представлении, так как вид оператора потенциальной энергии в координатном представлении в силу (1.77) и (1.78) просто совпадает с потенциальной функцией.

В силу того что оператор импульса в импульсном представлении известен (это есть умножение на импульс), возникает задача нахождения вида оператора импульса в координатном представлении. Решение этой задачи представлено ниже.

Так как собственные векторы оператора импульса являются собственными векторами эрмитовского оператора, то они ортонормированы (в соответствии с изложенными выше теоремами):

$$\langle p' | p \rangle = \delta(p - p'). \quad (1.81)$$

В силу условия полноты состояний с определённым значением координаты $|x\rangle$ выполняется тождество (Дираковское разложение единицы):

$$\int |x\rangle \langle x| dx = 1.$$

С учётом данного соотношения перепишем (1.81) в виде

$$\langle p' | p \rangle = \langle p' | 1 | p \rangle = \int_{-\infty}^{\infty} \langle p' | x \rangle \langle x | p \rangle dx = \delta(p - p'). \quad (1.82)$$

По определению $\langle x | p \rangle \equiv \psi_p(x)$ — функция состояния с определённым значением импульса в координатном представлении, а $\langle p' | x \rangle = \langle x | p' \rangle^* = \psi_{p'}^*(x)$ — комплексно сопряжённая функция состояния с определённым значением импульса в координатном представлении, т. е. (1.82) имеет вид

$$\int_{-\infty}^{\infty} \psi_{p'}^*(x) \cdot \psi_p(x) dx = \delta(p - p'). \quad (1.83)$$

Так как для δ -функции Дирака известно следующее интегральное определение [5] (i — мнимая единица):

$$\int_{-\infty}^{\infty} \exp [ix(k - k')] dx = 2\pi \delta(k - k'), \quad (1.84)$$

то из сравнения (1.83) и (1.84) можно найти явный вид $\psi_p(x)$. Из (1.84) ясно, что если x — координата, то размерность k совпадает с обратной размерностью координаты x . В теории волновых процессов k является волновым числом. Нетрудно заметить, что волновое число связано с импульсом p следующим соотношением: $k = p/\hbar$. Здесь \hbar — постоянная Планка. Кроме того, известно, что $\delta(ax) = \delta(x)/|a|$, где a — константа. То есть $\delta(k - k') = \hbar\delta(p - p')$. Таким образом, нормированная собственная функция оператора импульса в координатном представлении имеет вид

$$\langle x | p \rangle \equiv \psi_p(x) = \frac{1}{\sqrt{2\pi\hbar}} \exp \left(i \frac{p}{\hbar} x \right). \quad (1.85)$$

Так как спектр оператора не зависит от типа представления, а уравнение на собственные функции оператора импульса в координатном представлении \hat{p}_x имеет вид

$$\hat{p}_x \langle x | p \rangle = p \langle x | p \rangle, \quad (1.86)$$

то на основании (1.85) можно установить, что оператор импульса в координатном представлении есть

$$\hat{p}_x \equiv -i\hbar \frac{\partial}{\partial x}. \quad (1.87)$$

В результате одномерное уравнение Шрёдингера для частицы в поле $U(x)$ в координатном представлении имеет следующий вид уравнения в частных производных:

$$i\hbar \frac{\partial \psi(x, t)}{\partial t} = \left[-\frac{\hbar^2}{2m} \frac{\partial^2}{\partial x^2} + U(x) \right] \psi(x, t). \quad (1.88)$$

Здесь учтено, что $\hat{p}_x^2 = -\hbar^2 \frac{\partial^2}{\partial x^2}$.

Решение уравнения Шрёдингера называется волновой функцией. Волновая функция (в одномерном случае) удовлетворяет следующей *статистической интерпретации*: $|\psi(x, t)|^2 dx$ есть вероятность обнаружить частицу в интервале $x \div x+dx$ в момент времени t . Другими словами, квадрат модуля функции равен плотности вероятности нахождения частицы в точке с координатой x .

При решении уравнения Шрёдингера на волновую функцию всегда накладываются три условия, которые называются *стандартными*. А именно: волновая функция должна быть *ограниченной, непрерывной и однозначной* функцией своих переменных.

Предыдущее изложение для определения вида уравнения Шрёдингера тривиальным образом обобщается на случай одной частицы в трёхмерном пространстве:

$$i\hbar \frac{\partial \psi(\mathbf{r}, t)}{\partial t} = \left[-\frac{\hbar^2}{2m} \nabla^2 + U(\mathbf{r}, t) \right] \psi(\mathbf{r}, t). \quad (1.89)$$

Здесь учтено, что оператор импульса \mathbf{p} в пространстве трёх измерений есть $\mathbf{p} = -i\hbar \vec{\nabla}$. При этом статистическая интерпретация решения уравнения Шрёдингера означает, что $|\psi(\mathbf{r}, t)|^2 dV$ есть вероятность найти частицу в момент времени t внутри бесконечно малого объема dV , положение которого определяется радиусом-вектором \mathbf{r} .

Соответственно, в случае n частиц уравнение Шрёдингера имеет вид

$$i\hbar \frac{\partial \psi}{\partial t} = \left[-\sum_{i=1}^n \frac{\hbar^2}{2m_i} \nabla_i^2 + U(\mathbf{r}_1, \mathbf{r}_2, \dots, \mathbf{r}_n, t) \right] \psi, \quad (1.90)$$

где волновая функция ψ зависит уже от $3n$ пространственных переменных системы частиц и времени $\psi = \psi(\mathbf{r}_1, \mathbf{r}_2, \dots, \mathbf{r}_n, t)$. При этом

$$|\psi(\mathbf{r}_1, \mathbf{r}_2, \dots, \mathbf{r}_n, t)|^2 dV_1 dV_2, \dots, dV_n$$

определяет вероятность обнаружить в момент времени t частицы системы находящимися внутри бесконечно малых объемов $dV_1 dV_2, \dots, dV_n$, положение которых в пространстве определяется векторами $\mathbf{r}_1, \mathbf{r}_2, \dots, \mathbf{r}_n$.

При решении уравнения Шрёдингера (при заданной U) будет найдена функция $\psi_A(x) = \langle x | A \rangle$, в которой появится набор переменных A , характеризующих состояние системы. Другими словами, уравнение Шрёдингера — это способ вычисления скалярного произведения вектора состояния A и вектора с определенным значением координаты, т. е. проекция вектора состояния на вектор координаты. Это и есть координатное представление состояния A .

Вектор A может быть спроектирован на состояние произвольной физической величины $F - \langle F | A \rangle$. Для определения явного вида такого скалярного произведения необходимо либо найти и решить уравнение в этом F -представлении, либо исходя из координатного представления перейти в представление величины F . Пусть, например, имеется оператор физической величины F , обладающий дискретным спектром $\hat{F} | n \rangle = f_n | n \rangle$. В координатном представлении это уравнение имеет вид

$$\hat{F} \varphi_n(x) = f_n \varphi_n(x), \quad \text{или} \quad \hat{F} \langle x | n \rangle = f_n \langle x | n \rangle.$$

В силу полноты собственных функций эрмитовского оператора \hat{F} представим волновую функцию $\psi_A(x) = \langle x | A \rangle$ следующим образом:

$$\psi_A(x) = \langle x | A \rangle = \langle x | 1 | A \rangle = \sum_n \langle x | n \rangle \langle n | A \rangle = \sum_n \langle n | A \rangle \varphi_n(x).$$

В последнем соотношении коэффициенты ряда $\langle n | A \rangle$ и дают набор чисел, определяющих состояние A в F -представлении. Таким образом, существует простое правило перехода от координатного к F -представлению: *для определения вида состояния A в F -представлении из вида этого состояния в координатном представлении необходимо разложить функцию состояния A в координатном представлении по собственным функциям оператора \hat{F} в координатном представлении. Коэффициенты разложения и определяют функцию заданного состояния в искомом представлении.*

Статистическая интерпретация функции состояния в выбранном представлении отражает вероятностный характер принципов квантовой механики и имеет смысл, вытекающий из принципа суперпозиции и постулата об измерении физической величины.

Упражнение 1.14. Вывести равенство (1.68).

Упражнение 1.15. Вывести равенство (1.75).

Упражнение 1.16. Показать, что нормированная собственная функция оператора импульса в координатном представлении имеет вид (1.85).

1.8 Кубит

Квантовая теория имеет очень широкий спектр приложений в атомной, молекулярной физике, физике элементарных частиц и т. д., которые сами формируют целые направления в науке. Для приложений квантовой теории в области информационных систем имеет исключительно важное значение исследование суперпозиции двух квантовых состояний. Общее рассмотрение такой суперпозиции приведено ниже.

С точки зрения теории векторных пространств суперпозиция двух квантовых состояний есть гильбертово пространство \mathbf{H}_2 . Ортонормированный базис такого пространства можно обозначить двумя ортонормированными векторами, например: $|e_1\rangle$ и $|e_2\rangle$ или $|a\rangle$ и $|b\rangle$ и т. п. Однако для дальнейшего приложения ортонормированного базиса к информационным системам обозначим эти базисные состояния через $|0\rangle$ и $|1\rangle$. Удобство такого выбора определяется тем, что информационные технологии используют (в основном) бинарную арифметику. По этой причине ортонормированный базис $|0\rangle$ и $|1\rangle$ часто называют вычислительным базисом. Ортонормировка базиса означает выполнение равенств $\{|i\rangle\}$ $i = 0, 1$; $\langle i | j \rangle = \delta_{ij}$, $ij \in 0, 1$, где δ_{ij} — символ Кронекера.

В соответствии с принципом суперпозиции наиболее общее нормированное состояние в \mathbf{H}_2 может быть представлено в виде

$$|\psi\rangle = a|0\rangle + b|1\rangle, \quad (1.91)$$

где a и b — комплексные числа, а $|0\rangle$ и $|1\rangle$ — базисные векторы. Условие нормировки состояния $|\psi\rangle$: $\langle \psi | \psi \rangle = 1$ означает, что комплексные числа a и b удовлетворяют соотношению

$$\langle \psi | \psi \rangle = |a|^2 + |b|^2 = 1. \quad (1.92)$$

Состояние, определённое равенством (1.91), в теории квантовых вычислений называется кубитом (quantum bit=qubit).

Проектируя состояние кубита на вычислительный базис $\{|i\rangle\}$, $i = 0, 1$, т. е. составляя скалярные произведения вида $\langle i | \psi \rangle$, получим

$$\langle 0 | \psi \rangle = a, \quad \langle 1 | \psi \rangle = b, \quad (1.93)$$

где $|a|^2$ — вероятность обнаружить в суперпозиции $|\psi\rangle$ состояние $|0\rangle$, а $|b|^2$ — вероятность обнаружить в суперпозиции $|\psi\rangle$ состояние $|1\rangle$. Отметим, что на основании постулата об измерении после проектирования на ортонормированный вычислительный базис состояние кубита $|\psi\rangle$ переходит или в состояние $|0\rangle$ ($|\psi\rangle \rightarrow |0\rangle$), или в состояние $|1\rangle$ ($|\psi\rangle \rightarrow |1\rangle$).

В соответствии с принципами квантовой теории общая фаза кубита физического смысла не имеет, так как состояния $|\psi\rangle$ и $\exp(i\alpha)|\psi\rangle$ тождественны (см. (1.8)).

$$|\psi\rangle \equiv \exp(i\alpha)|\psi\rangle, \quad \alpha = \text{Re}. \quad (1.94)$$

Таким образом, можно заключить, что состояние кубита определяется двумя действительными параметрами. Чтобы показать это, представим комплексные константы a и b из (1.91) в тригонометрической форме:

$$|\psi\rangle = \varrho_a \exp(i\varphi_a)|0\rangle + \varrho_b \exp(i\varphi_b)|1\rangle. \quad (1.95)$$

Если вынести фазовый множитель $\exp(i\varphi_a)$ за скобку и опустить в соответствии с (1.94), то кубит можно представить в форме

$$|\psi\rangle = \varrho_a|0\rangle + \varrho_b \exp(i\varphi)|1\rangle, \quad (1.96)$$

где $\varphi = \varphi_b - \varphi_a$. Так как в силу условия нормировки должно выполняться равенство $\varrho_a^2 + \varrho_b^2 = 1$, то можно положить $\varrho_a = \cos(\theta/2)$ и $\varrho_b = \sin(\theta/2)$. В результате кубит определён с использованием только двух действительных параметров θ и φ в виде

$$|\psi\rangle = \cos \frac{\theta}{2}|0\rangle + e^{i\varphi} \sin \frac{\theta}{2}|1\rangle. \quad (1.97)$$

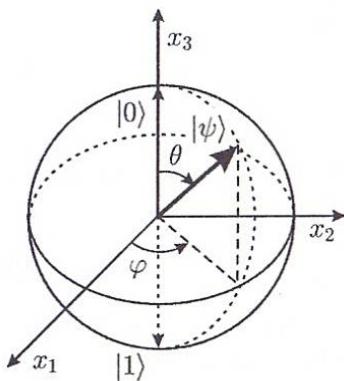


Рис. 1.1. Сфера Блоха

Если рассматривать параметры θ и φ как углы в некотором воображаемом трёхмерном пространстве, то понятию “кубит” можно придать формально простую “геометрическую” интерпретацию. Два действительных параметра θ и φ определяют точку на сфере, как показано на рис. 1.1. Вектор, соединяющий начало координат этого воображаемого пространства с точкой на сфере, задаёт геометрическую интерпретацию вектора состояния $|\psi\rangle$, или кубита. Геометрическое место точек “конца” вектора состояния образует сферу единичного радиуса в силу нормировки ψ .

Эта сфера часто называется сферой Блоха. Как видно из рисунка, при $\varphi = 0$ и $\theta = 0$ вектор $|\psi\rangle$ совпадает с базисным вектором $|0\rangle$ и направлен по оси x_3 . Соответственно, при $\theta = \pi$ вектор $|\psi\rangle$ совпадает с базисным вектором $|1\rangle$ и направлен против оси x_3 . То есть при такой геометрической интерпретации векторов состояний ортогональными являются векторы противоположного направления.

В квантовой теории информации кубит определяется как единица квантовой информации, аналогично тому, как бит (0 или 1) определяется как единица классической теории информации. Однако в отличие от понятия “бит информации” в классической теории, который может быть считан (измерен) без разрушения состояния бита, кубит при считывании (измерении) переходит в одно из двух своих базисных состояний: $|0\rangle$ или $|1\rangle$.

Ещё одной особенностью кубита является неограниченный объём информации, который формально может быть в него записан. Действительно, если на сфере Блоха за точками сферы закрепить какую-то определённую информацию, то, как это ни парадоксально, в кубит можно записать бесконечный объём информации! Однако считать из кубита можно только или состояние $|0\rangle$, или $|1\rangle$, т. е. только один бит из двух возможных единиц классической информации. В этом смысле кубит рассматривается как объект, который хранит два бита классической информации. Совокупность кубит образует квантовый регистр.

Упражнение 1.17. Какое число классических бит можно записать в регистр из n кубит?

1.9 Трансформационные свойства квантовых состояний

В настоящем разделе рассматриваются некоторые операции над квантовыми состояниями, которые играют важную роль при исследовании возможности управления квантовыми состояниями.

Известно, что понятие симметрии физической системы тесно связано с законами сохранения. Наличие симметрии в физической системе выражается в сохранении некоторых физических свойств при определённых преобразованиях. В квантовой теории преобразования связаны с унитарными операторами, действующими на векторы состояний. Как отмечалось ранее, оператор называется унитарным, если для него выполняется равенство $\hat{U}^\dagger = \hat{U}^{-1}$.

Рассмотрим действие линейного унитарного оператора \hat{U} на векторы

состояний системы $\{|\psi_n\rangle\}$, приводящее к новым состояниям $\{|\psi'_n\rangle\}$:

$$|\psi'_n\rangle = \hat{U} |\psi_n\rangle. \quad (1.98)$$

Конкретным унитарным преобразованием может быть, например, сдвиг во времени, сдвиг в пространстве, вращение системы координат относительно начала координат и т. п.

Рассматривая скалярное произведение состояний $|\psi'_n\rangle$ (1.98)

$$\langle \psi'_n | \psi'_m \rangle = \langle \psi_n | U^\dagger U | \psi_m \rangle = \langle \psi_n | \psi_m \rangle, \quad (1.99)$$

видим, что при унитарных преобразованиях длина вектора состояний в пространстве состояний $\{|\psi'_n\rangle\}$ сохраняется. Определяя некоторое унитарное преобразование над вектором состояний (1.98), необходимо установить, как меняются операторы наблюдаемых при таких преобразованиях. Для этого рассмотрим матричный элемент произвольного оператора \hat{Q} . Так как $\hat{U}^\dagger U = 1$, получим

$$\langle \psi_n | \hat{Q} | \psi_m \rangle = \langle \psi_n | \hat{U}^\dagger \hat{U} \hat{Q} \hat{U}^\dagger \hat{U} | \psi_m \rangle = \langle \psi'_n | \hat{U} \hat{Q} \hat{U}^\dagger | \psi_m \rangle' \equiv \langle \psi'_n | \hat{Q}' | \psi_m \rangle'. \quad (1.100)$$

Таким образом, при унитарных преобразованиях оператор Q изменяется по закону

$$\hat{Q}' = \hat{U} \hat{Q} \hat{U}^\dagger = \hat{U} \hat{Q} \hat{U}^{-1}. \quad (1.101)$$

Заметим, что оператор \hat{U} , определяющий унитарное преобразование, переходит в единичную матрицу I , если вызванное преобразованием изменение ε некоторой переменной стремится к нулю. В этом случае для малых ε оператор \hat{U} можно представить в виде

$$\hat{U} \approx I + i\varepsilon \hat{T} + o(\varepsilon^2), \quad (1.102)$$

где ε – бесконечное малое число. Оператор \hat{T} определяет бесконечно малое преобразование и называется *генератором бесконечно малого преобразования*. Для того чтобы выполнилось условие $\hat{U}^\dagger \hat{U} = I$ с точностью до бесконечно малого порядка ε , необходимо, чтобы $\hat{T} = \hat{T}^\dagger$, так как в этом случае

$$\hat{U}^\dagger \hat{U} \approx (1 - i\varepsilon \hat{T}^\dagger)(1 + i\varepsilon \hat{T}) \approx 1 + i\varepsilon(\hat{T} - \hat{T}^\dagger) + o(\varepsilon^2) \approx 1 + o(\varepsilon^2).$$

Таким образом, *генератор бесконечно малого преобразования* является *эрмитовским оператором*, а следовательно, связан с наблюдаемой.

Два последовательных унитарных преобразования также дают унитарное преобразование. В связи с этим n -последовательных бесконечно малых преобразований, каждое из которых вызывает изменение $\Delta = \varepsilon/n$, определяется оператором

$$\hat{U} = [I + i\Delta\hat{T}]^n. \quad (1.103)$$

Предел при $n \rightarrow \infty$ приводит к понятию оператора конечного преобразования:

$$\hat{U} = \lim_{n \rightarrow \infty} [I + i\frac{\varepsilon}{n}\hat{T}]^n = \exp(i\varepsilon\hat{T}) = \sum_{k=0}^{\infty} \frac{(i\varepsilon)^k}{k!} \hat{T}^k. \quad (1.104)$$

Так как оператор конечного унитарного преобразования (1.104) определяется оператором \hat{T} , то очевидно, что коммутатор $[\hat{U}, \hat{T}] = 0$. Это означает, что собственные состояния оператора \hat{T} являются одновременно и собственными состояниями для оператора \hat{U} , а собственные значения оператора \hat{T} не изменяются (сохраняются) при действии оператора \hat{U} .

Инвариантность системы по отношению к унитарному преобразованию определяет закон сохранения собственных значений эрмитовского оператора \hat{T} , что соответствует определённому закону сохранения физической величины T .

Пример 1.1. Сдвиг во времени

Рассмотрим преобразование $\hat{T}(\tau)$, которое переносит физическую систему во времени или меняет временную координату с t на $t' = t + \tau$:

$$\hat{T}(\tau)|t\rangle = |t'\rangle = |t + \tau\rangle. \quad (1.105)$$

Если изменение времени τ мало, то формальное разложение состояния $|t'\rangle$ в ряд Тейлора по параметру τ приводит к выражению

$$|t'\rangle = |t\rangle + \tau \frac{\partial}{\partial t} |t\rangle + \frac{1}{2!} \tau^2 \frac{\partial^2}{\partial t^2} |t\rangle + \dots \equiv \exp\left(\tau \frac{\partial}{\partial t}\right) |t\rangle. \quad (1.106)$$

Сравнивая (1.105) с (1.106), находим, что оператор сдвига по времени на произвольную величину τ имеет вид

$$\hat{T}(\tau) = \exp\left(\tau \frac{\partial}{\partial t}\right). \quad (1.107)$$

С учётом постулата об эволюции квантовых состояний ($i\hbar \frac{\partial}{\partial t} |\psi\rangle = \hat{H} |\psi\rangle$) находим, что оператор сдвига во времени можно записать в виде

$$\hat{T}(t) = \exp\left(-\frac{i}{\hbar} t \hat{H}\right), \quad (1.108)$$

где \hat{H} – оператор Гамильтона системы. Если оператор Гамильтона не зависит от времени, то его собственные векторы удовлетворяют соотношению (в момент времени 0)

$$\hat{H} |\psi_n(0)\rangle = E_n |\psi_n(0)\rangle \quad (1.109)$$

и к моменту времени t эти собственные векторы эволюционируют к состоянию $|\psi_n(t)\rangle$:

$$|\psi_n(t)\rangle = \hat{T}(t) |\psi_n(0)\rangle = \exp\left(-\frac{i}{\hbar}t\hat{H}\right) |\psi_n(0)\rangle = \exp\left(-\frac{i}{\hbar}tE_n\right) |\psi_n(0)\rangle. \quad (1.110)$$

Здесь E_n – энергия состояния системы в начальный момент времени.

Оператор (1.108) является оператором сдвига во времени для состояний, в которых \hat{H} сам явно не зависит от времени. То есть симметрия системы, связанная с однородностью времени, приводит к закону сохранения энергии, так как собственными числами оператора Гамильтона являются энергии $\hat{H} |\psi_n(0)\rangle = E_n |\psi_n(0)\rangle$. Изменение квантовых состояний во времени определяется в этом случае выражением

$$|\psi(t)\rangle = \exp\left(-\frac{i}{\hbar}tE_n\right) |\psi(0)\rangle. \quad (1.111)$$

Такие состояния в квантовой теории называются *стационарными*.

Пример 1.2. Сдвиг в пространстве

Одномерный оператор сдвига $D(x_0)$, перемещающий начало координат системы в точку x_0 и, следовательно, меняющий координату на $x' = x - x_0$, определяется равенством

$$\hat{D}(x_0) |x\rangle = |x'\rangle = |x - x_0\rangle. \quad (1.112)$$

Аналогично предыдущему случаю, разлагая состояние $|x'\rangle = |x - x_0\rangle$ по переменной x_0 , получим:

$$|x'\rangle = |x\rangle + (-x_0) \frac{\partial}{\partial x} |x\rangle + \frac{1}{2!} (-x_0)^2 \frac{\partial^2}{\partial x^2} |x\rangle + \dots \equiv \exp\left(-x_0 \frac{\partial}{\partial x}\right) |x\rangle. \quad (1.113)$$

Таким образом, оператор сдвига имеет вид

$$\hat{D}(x_0) = \exp\left(-x_0 \frac{\partial}{\partial x}\right). \quad (1.114)$$

Данное выражение можно переписать с учётом определения проекции оператора импульса на ось x : $\hat{p}_x = -i\hbar \frac{\partial}{\partial x}$ в следующем виде:

$$\hat{D}(x_0) = \exp\left(-ix_0 \frac{\hat{p}_x}{\hbar}\right). \quad (1.115)$$

Для трёхмерного сдвига на вектор \mathbf{r}_0 обобщением (1.115) является

$$\hat{D}(\mathbf{r}) = \exp\left(-i\frac{1}{\hbar}\mathbf{r} \cdot \hat{\mathbf{p}}\right), \quad (1.116)$$

где $\hat{\mathbf{p}} = -i\hbar\vec{\nabla}$ – оператор импульса в координатном представлении.

Естественно, что найденные выше операторы сдвига могут быть использованы и в пространстве обычных функций. Пусть, например, есть функция вида $f(x) = ax^2$, где a – константа. Вычисление действия оператора $\hat{D}(x_0)$ приводит к следующему очевидному результату:

$$\begin{aligned} \hat{D}(x_0)f(x) &= ax^2 - \frac{1}{1!}x_0 2ax + \frac{1}{2!}x_0^2 a + 0 + 0 + \dots = \\ &= a(x^2 - 2x_0 x + x_0^2) = a(x - x_0)^2 = f(x - x_0). \end{aligned} \quad (1.117)$$

Пример 1.3. Вращение в пространстве

Оператор поворота вокруг оси z на угол φ_0 определяется равенством

$$\hat{R}_z(\varphi_0)|\varphi\rangle = |\varphi'\rangle = |\varphi - \varphi_0\rangle. \quad (1.118)$$

Аналогично предыдущим случаям находим, что

$$|\varphi'\rangle = \exp\left(-\varphi_0 \frac{\partial}{\partial \varphi}\right) |\varphi\rangle = \exp\left(-i\frac{\hat{L}_z}{\hbar} \varphi_0\right) |\varphi\rangle, \quad (1.119)$$

где $\hat{L}_z = -i\hbar \frac{\partial}{\partial \varphi}$ – оператор проекции момента импульса $\mathbf{L} = [\mathbf{r} \times \mathbf{p}]$ на ось z в сферической системе координат. Декартовы компоненты оператора момента импульса $\hat{L}_x, \hat{L}_y, \hat{L}_z$ удобнее обозначить в виде $\hat{L}_x = \hat{L}_1, \hat{L}_y = \hat{L}_2, \hat{L}_z = \hat{L}_3$. В этом случае коммутатор пары этих операторов можно записать следующим одним соотношением [5]:

$$[\hat{L}_i, \hat{L}_j] = i\varepsilon_{ijk} \hat{L}_k, \quad (1.120)$$

где ε_{ijk} – полностью антисимметричный, единичный тензор третьего ранга (или символ Леви – Чивита), равный +1, если последовательность индексов i, j, k образует чётную перестановку с последовательностью 1, 2, 3; равный минус 1, если последовательность индексов i, j, k образует нечётную перестановку с последовательностью 1, 2, 3; и равный 0, если хотя бы пара индексов из набора i, j, k совпадает.

Так как коммутационным соотношениям типа (1.120) удовлетворяют ряд физически важных операторов, в квантовой теории вводится формальное определение оператора углового момента $\hat{\mathbf{J}}$. *Оператором углового момента называется любой векторный оператор $\hat{\mathbf{J}}$, для декартовых компонент которого выполняются коммутационные соотношения:*

$$[\hat{J}_i, \hat{J}_j] = i\varepsilon_{ijk} \hat{J}_k. \quad (1.121)$$

Соответственно, для произвольного вращения вокруг оси \mathbf{n} на угол α обобщение (1.119) есть

$$\hat{R}_{\mathbf{n}}(\alpha) = \exp\left(-\frac{i}{\hbar}\alpha(\mathbf{J} \cdot \mathbf{n})\right), \quad (1.122)$$

где $\hat{\mathbf{J}}$ – оператор углового момента системы [4].

Упражнение 1.18. Доказать, что оператор проекции момента импульса на ось z в сферической системе координат равен $\hat{L}_z = -i\hbar \frac{\partial}{\partial \varphi}$.

Упражнение 1.19. Вывести равенство (1.119).

Упражнение 1.20. Доказать равенство (1.120).

1.10 Квантовая теория на основе уравнения Шрёдингера

Основным уравнением квантовой теории в координатном представлении является уравнение Шрёдингера, определяющее изменение состояния A системы, заданного в координатном представлении волновой функцией $\psi \equiv \psi_A(x, t) = \langle x | A \rangle$ с течением времени:

$$i\hbar \frac{\partial}{\partial t} \psi = \hat{H} \psi. \quad (1.123)$$

Здесь \hat{H} – оператор Гамильтона системы, который в нерелятивистском случае представляет собой сумму операторов кинетической \hat{T} и потенциальной энергии \hat{U} . Оператор Гамильтона – эрмитовский оператор. Уравнение (1.123) при заданном виде оператора Гамильтона позволяет найти волновую функцию системы в последующий момент времени, если волновая функция в начальный момент времени известна.

Из (1.123) следует условие сохранения нормировки волновой функции с течением времени:

$$\frac{d}{dt} \int \psi^* \psi dx = 0. \quad (1.124)$$

Здесь интегрирование выполняется по всей области всех переменных представления x , от которых зависит волновая функция. Для доказательства умножим слева от операторов уравнение (1.123) на ψ^* , а уравнение, комплексно сопряжённое с (1.123), на функцию ψ . Составив разность этих уравнений, найдём:

$$i\hbar \frac{\partial}{\partial t} (\psi^* \psi) = \psi^* \hat{H} \psi - \psi \hat{H}^* \psi^*. \quad (1.125)$$

Проинтегрировав данное равенство по всей области всех переменных представления x , с учётом определения самосопряжённости оператора получим соотношение (1.124). Самосопряжённость оператора Гамильтона в координатном представлении означает выполнение следующего равенства:

$$\int \psi_1^* \hat{H} \psi_2 dx = \int \psi_2 \hat{H}^* \psi_1^* dx. \quad (1.126)$$

Здесь интегрирование осуществляется по всей области изменения всех пространственных переменных x .

По определению в квантовой теории $\varrho \equiv \psi^* \psi$ — это плотность вероятности найти систему с координатами x в момент времени t . Вычисляя действие оператора Гамильтона в правой части соотношения (1.125), данное равенство можно представить в виде уравнения непрерывности [5]

$$\frac{\partial \varrho}{\partial t} + \operatorname{div} \mathbf{j} = 0, \quad (1.127)$$

где \mathbf{j} — вектор плотности тока вероятности:

$$\mathbf{j} = -\frac{i}{\hbar} [\psi^* \hat{H} \psi - \psi \hat{H}^* \psi^*].$$

Например, для одной частицы массы m в трёхмерном пространстве, находящейся в поле U , оператор Гамильтона имеет вид: $\hat{H} = \hat{\mathbf{p}}^2/2m + U$, где $\hat{\mathbf{p}}$ — оператор импульса в координатном представлении $\hat{\mathbf{p}} = -i\hbar \nabla$. В этом случае вектор плотности тока вероятности \mathbf{j} будет иметь вид

$$\mathbf{j} = i \frac{\hbar}{2m} (\psi \nabla \psi^* - \psi^* \nabla \psi). \quad (1.128)$$

Волновая функция ψ в общем случае является комплексной функцией, которую всегда можно представить в виде $\psi = f(x, t) \exp(i\phi(x, t))$, где $f(x, t)$ и $\phi(x, t)$ — действительные функции. В результате плотность тока вероятности можно представить следующим выражением:

$$\mathbf{j} = \frac{\hbar}{m} \varrho \nabla \phi. \quad (1.129)$$

Последнее равенство означает, что $\mathbf{j} = 0$ для волновых функций, у которых ϕ не зависит от координат, и для всех действительных волновых функций.

В случае когда оператор Гамильтона не зависит от времени, в решении уравнения (1.123) можно отделить пространственные переменные от времени. Волновая функция любой системы в этом случае имеет вид

$$\psi(x, t) = \varphi_E(x) \exp\left(-i \frac{E}{\hbar} t\right) \quad (1.130)$$

и называется волновой функцией стационарного состояния. E – энергия системы, а $\varphi_E(x)$ – решение так называемого стационарного уравнения Шредингера, удовлетворяющее стандартным условиям (непрерывность, однозначность и ограниченность) и физическим условиям конкретной задачи:

$$\hat{H}\varphi_E(x) = E\varphi_E(x). \quad (1.131)$$

Среднее значение физической величины \hat{F} у системы с волновой функцией $\psi_a(x, t)$ в координатном представлении вычисляется на основании выражения [5]

$$\langle F \rangle = \langle a | \hat{F} | a \rangle = \int \psi_a^*(x, t) \hat{F} \psi_a(x, t) dx. \quad (1.132)$$

В стационарных состояниях плотность вероятности, плотность тока вероятности, среднее значение физической величины не зависят от времени. Кроме того, в стационарных состояниях физические величины могут иметь определённое значение, только если оператор этих величин коммутирует с оператором Гамильтона. Например, координата не может иметь определённого значения в стационарном состоянии, так как оператор координаты \hat{x} не коммутирует с оператором Гамильтона. В этом смысле набор физических величин, определяющих квантовое состояние, состоит из физических величин, операторы которых коммутируют друг с другом и оператором Гамильтона.

Соответственно, на основании постулата об измерении физической величины F вероятность измерения данной физической величины в произвольном состоянии системы $\psi_a(x, t)$ определяется разложением $\psi_a(x, t)$ по полному набору собственных функций оператора $\hat{F}\varphi(x) = F\varphi(x)$ данной физической величины:

$$\psi_a(x, t) = \int c_F(a, t)\varphi_F(x) dF, \quad \text{где} \quad c_F(a, t) = \int \varphi_F^*(x)\psi_a(x, t) dx. \quad (1.133)$$

Квадрат модуля коэффициентов разложения $|c_F(a, t)|^2$ и определяет плотность вероятности измерения величины F . Соответственно, $|c_F(a, t)|^2 dF$ – вероятность измерения величины F внутри бесконечно малого интервала dF в системе в момент времени t . Формула (1.133) справедлива в случае, когда спектр оператора \hat{F} непрерывный. Если спектр оператора \hat{F} дискретный, т. е. $\hat{F}\varphi_n(x) = F_n\varphi_n(x)$, вероятность измерения физической

величины F определяется из разложения вида

$$\psi_a(x, t) = \sum c_n(a, t) \varphi_n(x), \quad \text{где} \quad c_n(a, t) = \int \varphi_n^*(x) \psi_a(x, t) dx. \quad (1.134)$$

При этом вероятность измерения физической величины F равна квадрату модуля коэффициента разложения $|c_n(a, t)|^2$.

В стационарных состояниях вероятность обнаружить определённое значение физической величины, по определению (1.133), (1.134), не зависит от времени.

Уравнение Шрёдингера в предельном случае, когда действие системы $S \gg \hbar$ содержит частным случаем уравнение классической механики. Таким образом квантовая теория не отвергает уравнения классической теории, а только устанавливает область применимости классической теории.

Упражнение 1.21. Вывести равенство (1.128).

Упражнение 1.22. Доказать соотношение (1.129).

Упражнение 1.23. Вывести правило вычисления среднего значения физической величины (1.132).

Упражнение 1.24. Доказать, что если действие системы S удовлетворяет неравенству $S \gg \hbar$, то уравнение Шрёдингера с точностью до отношения \hbar/S совпадает с уравнением классической механики (\hbar — постоянная Планка).

1.11 Простые примеры решения уравнения Шрёдингера

Достаточно краткое изложение принципов квантовой теории не даёт ясного представления о смысле принципов и многочисленных следствиях, вытекающих из этих принципов. Однако некоторые простые примеры хорошо демонстрируют положения теории, которые оставались непрояснёнными при аксиоматическом изложении. Ниже рассмотрены примеры, относительно наглядно раскрывающие некоторые положения теории.

Пример 1.4. Частица в одномерной потенциальной яме с двумя "бесконечно высокими стенками".

Свободная частица массы m находится в одномерном пространстве в интервале $0 \leq x \leq a$. Определить квантово-механическое описание такой системы.

Классическое представление такой задачи можно определить как движение без трения частицы на нитке между двумя упруго отражающими стенками. Решение классической задачи тривиально. Частица либо поко-

ится, либо, если ей придали в начальный момент времени скорость v , движется от стенки к стенке с заданной скоростью. При этом можно сообщить частице любую начальную скорость.

С точки зрения квантовой теории описание такой системы опирается на решение уравнения Шрёдингера с гамильтонианом следующего вида:

$$\hat{H} = \hat{T} + U(x) = \frac{\hat{p}_x^2}{2m} + U(x) = -\frac{\hbar^2}{2m} \frac{\partial^2}{\partial x^2} + U(x), \quad (1.135)$$

где $U(x)$ – потенциальная энергия частицы. По условию задачи $U(x)$ может быть задана соотношениями: $U(x) = \infty$ при $x \leq 0$ и $x \geq a$; $U(x) = 0$ при $0 \leq x \leq a$. Бесконечные значения потенциальной энергии формально обеспечивают невозможность попадания частицы в области $x < 0$ и $x > a$. Невозможность обнаружить частицу “за стенками” на языке квантовой теории означает, что волновая функция в этих областях равна нулю. Таким образом, нужно найти решение уравнения Шрёдингера только в области $0 \leq x \leq a$, в которой $U(x) = 0$.

$$i\hbar \frac{\partial}{\partial t} \Psi(x, t) = \hat{H} \Psi(x, t) = -\frac{\hbar^2}{2m} \frac{\partial^2}{\partial x^2} \Psi(x, t). \quad (1.136)$$

Так как гамильтониан не зависит от времени t , волновая функция имеет вид функции стационарного состояния

$$\Psi(x, t) = \Phi_E(x) \exp\left(-i\frac{E}{\hbar}t\right). \quad (1.137)$$

Здесь E – энергия частицы, а $\Phi_E(x)$ – пространственная часть волновой функции, удовлетворяющая уравнению

$$-\frac{\hbar^2}{2m} \frac{\partial^2}{\partial x^2} \Phi_E(x) = E \Phi_E(x). \quad (1.138)$$

Нормированное решение данного стационарного уравнения, удовлетворяющее физическим условиям задачи ($\Psi(x = 0, t) = \Psi(x = a, t) = 0$) и стандартным условиям (непрерывность, ограниченность, однозначность), возможно только при строго определенных значениях энергии E . Соответственно, пространственная часть волновой функции и дискретный спектр энергий есть

$$\Phi_{E_n}(x) \equiv \Phi_n(x) = \sqrt{\frac{2}{a}} \sin\left(\frac{n\pi x}{a}\right), \quad \text{где} \quad E_n = \frac{n^2\pi^2\hbar^2}{2ma^2}, \quad n = 1, 2, 3, \dots \quad (1.139)$$

Найденные решения ортонормированы, так как гамильтониан системы — эрмитовский:

$$\int_0^a \Phi_n(x) \Phi_m(x) dx = \delta_{n,m}. \quad (1.140)$$

Здесь $\delta_{n,m}$ — символ Кронекера.

Что же получено из квантовой теории и как это решение соотносится с классической теорией?

- У частицы имеется не равное нулю минимально разрешённое ей значение энергии E_1 . То есть частица не может находиться в состоянии покоя. На первый взгляд данное утверждение противоречит наблюдению из области окружающего мира. Однако оценим скорость частицы (например, массой в 1 г, ограниченной в пространстве в 10 м) в состоянии с наименьшей энергией:

$$v = \sqrt{\frac{2E}{m}} = \sqrt{\frac{2\pi^2(1,05 \cdot 10^{-27} \text{ эрг} \cdot \text{с})^2}{1 \text{ г} (10^4 \text{ см})^2}} \approx 10^{-30} \frac{\text{см}}{\text{с}}. \quad (1.141)$$

Нетрудно оценить далее, через какое время можно заметить перемещение такой частицы на расстояние l , например, 0,1 мм:

$$\tau = \frac{l}{v} \approx \frac{10^{-2} \text{ см}}{10^{-30} \text{ см/с}} = 10^{28} \text{ с} \approx 10^{21} \text{ лет.} \quad (1.142)$$

Это число на 7–8 порядков больше возраста Вселенной. Другими словами, в макромире мы просто не можем зарегистрировать такие маленькие скорости и принимаем их за состояние покоя.

- Наличие дискретного спектра у частицы, с точки зрения классической теории, означает, что мы не можем сообщить частице произвольную скорость. Но и этот вывод не противоречит наблюдениям для объектов макромира, так как расстояние между соседними уровнями энергий (т. е. различными значениями скоростей) настолько мало, что мы не можем зарегистрировать их разницу. Например, скорость в состоянии E_2 отличается от скорости в состоянии E_1 на величину порядка 10^{-30} см/с , что не представляется возможным зафиксировать. В этом смысле для макроскопических объектов дискретный спектр энергий или скоростей сливается, образуя непрерывный ряд значений с указанной выше точностью. Однако, если данной задачей моделировать атом водорода (электрон $m \approx 9,1 \cdot 10^{-28} \text{ г}$ локализован вблизи ядра на расстоянии порядка $a \approx 10^{-8} \text{ см}$), то эта

модель качественно объясняет наличие дискретных состояний у атома водорода и предсказывает расстояние между соседними уровнями, равными

$$\Delta \approx \frac{\hbar^2}{ma^2} = \frac{(1,05 \cdot 10^{-27} \text{ эрг} \cdot \text{с})^2}{9,1 \cdot 10^{-28} \text{ г} \cdot (10^{-8} \text{ см})^2} \approx 10^{-11} \text{ эрг} = 6,24 \text{ эВ}, \quad (1.143)$$

что соответствует по порядку величины экспериментально измеряемому значению разности энергий в атоме водорода. Таким образом, при переходе к объектам микромира (атомы, молекулы, элементарные частицы) получаем разумные результаты, доступные для измерения.

- Из решения уравнения Шредингера найдено, что энергия частицы есть физическая величина, определяющая её состояние. То есть волновая функция в дираковских обозначениях есть скалярное произведение вида $\Psi(x, t) = \langle x | E_n \rangle$. В этом смысле решение уравнения Шредингера есть правило вычисления проекции вектора состояния на вектор с определённым значением координаты.
- Из решения уравнения вытекает, что координата не имеет определённого значения. Частица не локализована в какой-то точке. Имеется ненулевая вероятность найти частицу в произвольной точке внутри отрезка $0 - a$. Вероятность обнаружить частицу в интервале $x \div x + dx$ не зависит от времени и определяется выражением

$$|\Psi_{E_n}(x, t)|^2 dx = |\Phi_{E_n}(x)|^2 dx = \frac{2}{a} \sin^2\left(\frac{n\pi}{a}x\right) dx. \quad (1.144)$$

- Среднее значение координаты $\langle \hat{x} \rangle$ рассматриваемой частицы в любом состоянии не зависит от времени и равно $a/2$, так как по определению среднего значения имеем

$$\langle \hat{x} \rangle = \int_0^a \sqrt{\frac{2}{a}} \sin\left(\frac{n\pi}{a}x\right) e^{iE_n t/\hbar} (\hat{x}) \sqrt{\frac{2}{a}} \sin\left(\frac{n\pi}{a}x\right) e^{-iE_n t/\hbar} dx = \frac{a}{2}. \quad (1.145)$$

Если ввести в рассмотрение вспомогательный оператор отклонения от среднего значения координаты $\Delta_x = \hat{x} - \langle \hat{x} \rangle$, то среднее значение квадрата отклонения координаты от среднего значения равно в настоящем примере

$$\langle (\Delta_x)^2 \rangle = \frac{2}{a} \int_0^a \sin^2\left(\frac{n\pi}{a}x\right) \left(x - \frac{a}{2}\right)^2 dx = \frac{a^2}{12} \frac{n^2 \pi^2 - 6}{n^2 \pi^2}. \quad (1.146)$$

Соответственно, среднее значение импульса $\langle \hat{p}_x \rangle = 0$. Если ввести оператор отклонения импульса от среднего значения $\Delta_p = \hat{p} - \langle \hat{p}_x \rangle$, то среднее значение квадрата отклонения импульса от среднего значения определяется выражением

$$\langle (\Delta_p)^2 \rangle = \frac{2}{a} \int_0^a \sin\left(\frac{n\pi}{a}x\right) \left(-i\hbar \frac{\partial}{\partial x}\right)^2 \sin\left(\frac{n\pi}{a}x\right) dx = \frac{\hbar^2}{2a^2} n^2 \pi^2. \quad (1.147)$$

И вычисленные данные согласуются с общим соотношением неопределённости (1.54):

$$\langle (\Delta_x)^2 \rangle \langle (\Delta_p)^2 \rangle = \frac{\hbar^2}{4} \frac{n^2 \pi^2 - 6}{6} \geq \frac{\hbar^2}{4}. \quad (1.148)$$

- Плотность вероятности измерения значения импульса не зависит от времени и определяется квадратом модуля коэффициента разложения функции $\Psi_E(x, t)$ по собственным функциям $\psi_p(x)$ (1.85) оператора импульса $\hat{p}_x = -i\hbar \nabla_x$:

$$\begin{aligned} |c_n(p)|^2 &= \left| \int_0^a \psi_p^*(x) \Psi_{E_n}(x, t) dx \right|^2 = \\ &= \left(\frac{a}{\hbar} \right) \frac{4n^2 \pi}{(n\pi)^2 - 4\kappa^2} \left\{ \begin{array}{ll} \sin^2(\kappa), & n - \text{чет.} \\ \cos^2(\kappa), & n - \text{неч.} \end{array} \right\}. \end{aligned} \quad (1.149)$$

Здесь $\kappa \equiv pa/2\hbar$. Соответственно, вероятность w измерения импульса в интервале $p \div p + dp$ равна $w = |c_n(p)|^2 dp$.

Пример 1.5. Частица в поле тяжести

Частица массой m находится в однородном гравитационном поле (ускорение свободного падения — g) над абсолютно упругой отражающей плоскостью.

Решение классической задачи состоит в том, что поднятое на произвольную высоту z тело падает вниз с ускорением g , упруго отражается вверх от плоскости $z = 0$ и поднимается на исходную высоту. Далее этот процесс циклически повторяется. Квантово-механическое описание такой системы основано на решении стационарного уравнения Шрёдингера следующего вида:

$$\left[-\frac{\hbar^2}{2m} \frac{d^2}{dz^2} + mgz \right] \Phi_E(z) = E \Phi_E(z). \quad (1.150)$$

Решение данного уравнения должно удовлетворять стандартным условиям (непрерывность, ограниченность и однозначность) и физическим условиям задачи (в данном примере $\Phi_E(0) = 0$, что означает невозможность обнаружения частицы в точках $z < 0$). При этом волновая функция частицы имеет вид функции стационарного состояния (1.130).

Для упрощения записи уравнения введём новые переменные x и ε по определению $z = ax$ и $E = \lambda\varepsilon$. Выбор констант a и λ основан на максимальном упрощении записи. Так, если положить $a = 2^{-1/3}\hbar^{2/3}m^{-2/3}g^{-1/3}$ и $\lambda = 2^{-1/3}\hbar^{2/3}m^{1/3}g^{2/3}$, то уравнение (1.150) будет иметь вид

$$\left[\frac{d^2}{dx^2} - (x - \varepsilon) \right] \Phi_E(x) = 0. \quad (1.151)$$

Решение данного уравнения выражается через функцию Эйри $Ai(\xi)$, где $\xi \equiv x - \varepsilon$. При положительных значениях ξ (что соответствует условию $mgz - E > 0$, т. е. полная энергия частицы меньше потенциальной энергии – неклассический случай) функция Эйри выражается через модифицированную функцию Ханкеля $K_\nu(x)$ [1]:

$$\Phi_E(x) = N Ai(\xi) = N \frac{1}{\pi} \sqrt{\frac{\xi}{3}} K_{1/3} \left(\frac{2}{3} \xi^{3/2} \right), \quad \xi = x - \varepsilon > 0. \quad (1.152)$$

Здесь N – нормировочная константа. Учитывая асимптотическое поведение функции Ханкеля при больших аргументах $K_\nu(\xi) \rightarrow \xi^{-1/2} \exp(-\xi)$, видно, что найденное решение в этом случае ограничено при любых z и экспоненциально мало (область за классической точкой поворота).

В случае если $mgz - E < 0$ (классический случай) или $\xi < 0$, функция Эйри выражается через линейную комбинацию функций Бесселя $J_\nu(x)$ [1] и решение уравнения имеет вид

$$\Phi_E(x) = N Ai(\xi) = N \frac{\sqrt{|\xi|}}{3} \left[J_{1/3} \left(\frac{2}{3} |\xi|^{3/2} \right) + J_{-1/3} \left(\frac{2}{3} |\xi|^{3/2} \right) \right], \quad (1.153)$$

где $\xi = x - \varepsilon < 0$. То есть функция осциллирует и многократно проходит через ноль. По этой причине условие $\Phi_E(x = 0) = 0 \rightarrow Ai(-\varepsilon) = 0$ означает, что имеется бесконечное число дискретных (разрешённых) значений энергии ε , при которых $\Phi_E(x = 0) = 0$. В общем случае эти значения можно рассчитать численными методами. Для упрощения результата рассмотрим случай больших значений $\xi < 0$. Известное асимптотическое поведение функций Бесселя [1] приводит к следующему результату:

$$\Phi_E(x) = N Ai(\xi) \rightarrow N \frac{1}{\pi} |\xi|^{-1/4} \cos \left(\frac{2}{3} |\xi|^{3/2} - \frac{\pi}{4} \right), \quad \xi = x - \varepsilon < 0. \quad (1.154)$$

Следовательно, при больших n спектр разрешённых уровней энергии есть

$$E_n = \lambda \varepsilon_n = \lambda \left[\frac{3}{4} \left(2n - \frac{1}{2} \right) \right]^{2/3}, \quad n \gg 1. \quad (1.155)$$

Как видно, квантовое решение существенно более сложное в сравнении с классическим решением даже для такой относительно простой системы. Согласование результатов квантовой теории и классической аналогично предыдущему случаю и далее не приводится.

Пример 1.6. Линейный гармонический осциллятор.

Частица в одномерном потенциальном поле вида $U(x) = kx^2/2$, где k – константа, является примером линейного гармонического осциллятора. Определить квантово-механическое описание такой системы.

В классической теории осциллятор можно представить в виде частицы массы m на пружине с жёсткостью k . Классическое уравнение для определения траектории движения $x(t)$ (x – смещение от положения равновесия, t – время) такой частицы и его решение имеет вид

$$m \frac{d^2x}{dt^2} = -kx; \quad x(t) = \frac{v_0}{\omega} \sin(\omega t); \quad \omega = \sqrt{\frac{k}{m}}. \quad (1.156)$$

Представленное решение соответствует условию, когда частица в начальный момент времени находилась в начале координат и имела начальную скорость v_0 . При этом начало координатной оси x совпадает с положением равновесия пружины. Фактически имеется большое число систем, описание которых эквивалентно уравнению (1.156), поэтому решение этой задачи представляет разнообразные приложения.

С точки зрения квантовой теории, описание линейного осциллятора основано на решении стационарного уравнения Шрёдингера:

$$\left[-\frac{\hbar^2}{2m} \frac{d^2}{dx^2} + \frac{kx^2}{2} \right] \Phi_E(x) = E\Phi_E(x). \quad (1.157)$$

Решение данного уравнения, удовлетворяющее стандартным условиям, возможно только при строго определённых значениях энергии [5], равных

$$E_n = \hbar\omega \left(n + \frac{1}{2} \right), \quad \text{где} \quad n = 0, 1, 2, \dots, \quad \omega = \sqrt{\frac{k}{m}}. \quad (1.158)$$

При этом пространственная часть волновой функции, соответствующая

энергии частицы E_n , имеет вид [5]

$$\Phi_{E_n}(x) \equiv \Phi_n(x) = \frac{1}{\sqrt{\sqrt{\pi} n! 2^n}} \exp\left(-\frac{x^2}{2a^2}\right) H_n\left(\frac{x}{a}\right); \quad a \equiv \sqrt{\frac{\hbar}{m\omega}}. \quad (1.159)$$

Здесь $H_n(\xi)$ – полином Эрмита [1]

$$H_n(\xi) = (-1)^n \exp(\xi^2) \frac{d^n}{d\xi^n} \exp(-\xi^2). \quad (1.160)$$

При частных значениях индекса n полиномы Эрмита имеют достаточно простой вид:

$$H_0(\xi) = 1; \quad H_1(\xi) = 2\xi; \quad H_2(\xi) = 4\xi^2 - 2; \quad \dots \quad (1.161)$$

Функции $\Phi_n(x)$ ортонормированы:

$$\int_{-\infty}^{\infty} \Phi_n(x) \Phi_m(x) dx = \delta_{n,m}. \quad (1.162)$$

Очевидно, что квантовое решение имеет ряд фундаментальных отличий от классического решения. Так, если классический осциллятор означает движение частицы внутри ограниченного интервала $-A \leq x \leq +A$, где A – амплитуда колебаний, квантовую частицу можно обнаружить в любой точке одномерного пространства $-\infty \leq x \leq \infty$. В этом смысле говорят, что есть ненулевая вероятность обнаружить частицу за “классическими точками поворота”. Классические точки поворота определяются из условия $E = U(x)$. Для осциллятора $x_{1,2} = \pm\sqrt{2E/k}$. Квантовый осциллятор имеет отличную от нуля наименьшую энергию (отсутствие состояния покоя). Квантование энергии означает невозможность передать осциллятору произвольную энергию. Все эти особенности аналогичны тем, которые подробно рассматривались для частицы в яме с двумя бесконечно высокими стенками.

Пример 1.7. Атом водорода

Примером решения уравнения Шрёдингера в трёхмерном пространстве является задача об электроне, локализованном около положительно заряженного ядра. Известно, что атом водорода – это система, состоящая из протона и электрона, которая является простейшей атомарной структурой. Так как масса протона на три порядка больше массы электрона, а размеры протона много меньше характерных размеров атома, в первом приближении можно пренебречь движением протона и рассматривать атом

водорода как электрон массы μ и заряда $-|e|$, локализованный у точечного бесконечно тяжелого положительно заряженного центра $+|e|$. В этом случае потенциальная энергия электрона равна $U(r) = -e^2/r$, где r — расстояние от заряженного центра до электрона. Стационарное уравнение Шрёдингера для такой системы в сферической системе координат, связанной с положительным зарядом, имеет вид

$$\left[-\frac{\hbar^2}{2\mu} \nabla^2 - \frac{e^2}{r} \right] \Phi(r, \theta, \varphi) = E\Phi(r, \theta, \varphi). \quad (1.163)$$

Здесь r, θ, φ — переменные сферической системы координат. Решение данного уравнения, удовлетворяющее стандартным условиям, у рассматриваемой связанной системы существует только при дискретных значениях энергии E [5]:

$$E = E_n = -\frac{1}{2n^2} \frac{e^2}{a_0}, \quad \text{где } n = 1, 2, 3, \dots, \quad a_0 = \frac{\hbar^2}{mc^2} \approx 0,5 \cdot 10^{-8} \text{ см.} \quad (1.164)$$

При этом каждому значению E_n соответствует n^2 различных состояний, ортонормированные пространственные части волновой функции которых имеют вид

$$\Phi(r, \theta, \varphi) = \Phi_{nlm}(r, \theta, \varphi) = R_{nl}(r)Y_{lm}(\theta, \varphi). \quad (1.165)$$

Здесь n, l, m — квантовые числа: $n = 1, 2, 3, \dots$ — главное квантовое число (определяющее энергию системы (1.164)); l — орбитальное квантовое число (определяющее момент импульса электрона $\hbar\sqrt{l(l+1)}$), которое при фиксированном n принимает ряд значений $l = 0, 1, 2, \dots, n-1$; наконец, m — магнитное квантовое число, которое при фиксированном значении l принимает следующий ряд значений: $0, \pm 1, \pm 2, \dots, \pm l$ (всего $2l+1$ значений). $R_{nl}(r)$ — радиальная часть волновой функции (т. е. функция, зависящая только от радиальной пространственной переменной r), а $Y_{lm}(\theta, \varphi)$ — сферическая функция, зависящая от угловых пространственных переменных θ, φ , явный вид которой хорошо известен [4]. Радиальная часть функции может быть представлена в виде [5]

$$R_{nl}(r) = N_{nl} \left(\frac{2r}{na_0} \right)^l F \left(-n + l + 1; 2l + 2; \frac{2r}{na_0} \right) \exp \left(-\frac{r}{na_0} \right), \quad (1.166)$$

где N_{nl} — нормировочная константа:

$$N_{nl} = \frac{1}{(2l+1)!} \sqrt{\frac{(n+l)!}{2n(n-l-1)!}} \left(\frac{2}{na_0} \right), \quad (1.167)$$

а $F(a; b; x)$ – вырожденная гипергеометрическая функция [1]:

$$F(a; b; x) = \sum_{n=0}^{\infty} \frac{(a)_n}{n!(b)_n} x^n = 1 + \frac{a}{1!b} x + \frac{a(a+1)}{2!b(b+1)} x^2 \dots, \quad (1.168)$$

где $(a)_n = \Gamma(a+n)/\Gamma(a)$ – символ Похгаммера. $\Gamma(x)$ – Гамма-функция [1].

Согласно квантовой теории переходов [5] разности энергетических состояний определяют частоты электромагнитных волн, излучаемых (или поглощаемых) квантовой системой $\hbar\omega = E_n - E_m$. Например, для атома водорода частота излучения $\nu = \omega/(2\pi)$ определяется выражением

$$\nu = \omega/(2\pi) = R \left(\frac{1}{n^2} - \frac{1}{m} \right), \quad m > n, \quad R = \frac{e^4 \mu}{4\pi \hbar^3}.$$

Здесь $R = 3,27 \cdot 10^{15} \text{с}^{-1}$ – постоянная Ридберга.

Состояние электрона в атоме водорода с наимизшей энергией описывается волновой функцией $\Phi_{100}(r, \theta, \varphi) = R_{10}(r)Y_{00}(\theta, \varphi)$. Угловая часть волновой функции $Y_{00}(\theta, \varphi) = 1/\sqrt{4\pi}$, т. е. состояние сферически симметрично. Вероятность dW обнаружить электрон на заданном расстоянии от ядра внутри шарового слоя dr радиуса r определяется выражением

$$dW = |\Phi_{100}|^2 4\pi r^2 dr = \frac{4}{a_0^3} \exp\left(-\frac{2r}{a_0}\right) r^2 dr, \quad a_0 = \frac{\hbar^2}{\mu e^2}. \quad (1.169)$$

Здесь $a_0 \approx 0,529 \cdot 10^{-8} \text{см}$ – Боровский радиус. Из (1.169) видно, что эта вероятность отлична от нуля во всем пространстве, хотя и экспоненциально затухает с ростом r . Вычисление максимума функции плотности вероятности dW/dr показывает, что наибольшее значение достигается при $r = a_0$. Таким образом, электрон с наибольшей вероятностью находится на расстоянии a_0 от ядра, что качественно определяет “размеры” атома.

Глава 2

Спин

2.1 Спин электрона

Квантовая теория, основанная на решении уравнения Шрёдингера, не объяснила всей известной совокупности явлений в теории атомов. Так, например, эффект расщепления спектральных линий в магнитном поле (эффект Зеемана) оказался объяснённым только частично. Объяснение такого рода явлений стало возможным после установления специального свойства у ряда элементарных частиц. Это свойство получило наименование спин.

Спин – векторное свойство ряда частиц (в дополнение к заряду и массе), которое проявляется во внешнем поле. Это внутренний (т. е. неотъемлемый от частицы) механический момент, который ориентируется в пространстве дискретно по отношению к выделенному направлению (пространственное квантование).

Первоначально спин был открыт у электрона в опытах Штерна – Герлаха. Спин электрона – вектор, стандартное обозначение которого – s . Вектор спина s ориентируется в пространстве двояко, так что проекция спина на направление поля (например, ось z) принимает одно из двух значений $\pm \hbar/2$, где \hbar – постоянная Планка. Впоследствии спин с аналогичными свойствами был обнаружен и у ряда других частиц: протона, нейтрона и т. п. В дальнейшем было установлено, что существуют частицы, проекция внутреннего момента которых на выделенное направление принимает значения $0, \pm \hbar$ или $\pm 1/2\hbar, \pm 3/2\hbar$.

В то же время экспериментально установлено, что у ряда частиц данное свойство отсутствует. В этом смысле частицы делятся на спиновые (обладающие спином) и бесспиновые. В свою очередь, частицы, обладающие спином, делятся на частицы с целой (в единицах \hbar) проекцией спина (бозоны) и полуцелой проекцией (фермионы). Принято говорить о величине

спина, связывая его с максимально возможной проекцией на выделенное направление (в единицах \hbar). То есть частицы со спином $1/2; 1; 3/2; 2; \dots$

Совокупность частиц, в которую входят электрон, протон, нейтрон и ряд других, образует группу частиц со спином $1/2$.

Квантово-механическое описание частиц со спином $1/2$ основано на использовании оператора спина электрона \hat{s} . Декартовы проекции оператора спина обозначаются \hat{s}_x, \hat{s}_y и \hat{s}_z . Или альтернативно в виде $\hat{s}_x = \hat{s}_1, \hat{s}_y = \hat{s}_2$ и $\hat{s}_z = \hat{s}_3$. Так как спин является внутренним механическим моментом, декартовы компоненты его оператора удовлетворяют тем же коммутационным соотношениям, что и компоненты оператора момента импульса (1.120) или в общем случае оператора углового момента (1.121):

$$[\hat{s}_j, \hat{s}_k] = i\hbar\epsilon_{jkl}\hat{s}_l, \quad j, k, l = 1, 2, 3. \quad (2.1)$$

Здесь ϵ_{jkl} — символ Леви — Чивита (см. (1.120)), i — мнимая единица.

В классической электродинамике установлено, что для заряженной, точечной частицы с зарядом e и массой m связь между механическим \mathbf{L} и магнитным моментом \mathbf{m}_l имеет вид

$$\mathbf{m}_l \equiv \frac{1}{2c} \int [\mathbf{r} \times \mathbf{j}] dv = \frac{e}{2mc} \mathbf{L} = \frac{e}{2mc} [\mathbf{r} \times \mathbf{p}]. \quad (2.2)$$

Здесь c — скорость света, $\mathbf{p} = mv$ — импульс частицы, \mathbf{v} — скорость, \mathbf{j} — плотность тока, $\mathbf{j} = \varrho\mathbf{v}$, ϱ — плотность заряда. Для точечной частицы $\varrho(\mathbf{r}) = e\delta(\mathbf{r} - \mathbf{r}_e)$, \mathbf{r}_e — радиус-вектор заряда в пространстве.

В квантовой теории с внутренним механическим моментом (спином) s связан магнитный спиновый момент \mathbf{m}_s . Связь между этими векторами была установлена экспериментально в опытах Эйнштейна — де Газа и имеет вид

$$\mathbf{m}_s = \frac{e}{mc} \mathbf{s}. \quad (2.3)$$

Выражение (2.3) отличается от (2.2) множителем 2, что подчеркивает неклассические свойства спина. И спин, и магнитный спиновый момент частиц играют существенную роль как в области микромира, так и в поведении макротел. Поэтому исследование этого свойства является важной задачей квантовой теории.

Для построения вида оператора спина $1/2$ (или спина электрона) можно опереться на основное его свойство — наличие только двух значений проекций спина s_z , которые могут быть экспериментально измерены. Так как в своем собственном представлении оператор физической величины

есть диагональная матрица размерности, равной числу собственных значений, на главной диагонали которой стоят собственные числа, то в s_z -представлении (представлении, когда ось квантования спина есть ось z) оператор \hat{s}_z равен

$$\hat{s}_z = \begin{pmatrix} \hbar/2 & 0 \\ 0 & -\hbar/2 \end{pmatrix} = \frac{\hbar}{2} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (2.4)$$

Для определения вида операторов \hat{s}_x и \hat{s}_y в s_z -представлении зададим их в виде матриц размерности 2×2 :

$$\hat{s}_x = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}; \quad \hat{s}_y = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}, \quad (2.5)$$

где a_{ij} и b_{ij} — произвольные комплексные числа, которые необходимо определить. Используя коммутационные соотношения (2.1) и условие эрмитовости оператора s , можно установить, что явный вид матриц \hat{s}_x и \hat{s}_y в s_z -представлении есть

$$\hat{s}_x = \frac{\hbar}{2} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \quad \hat{s}_y = \frac{\hbar}{2} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \quad (2.6)$$

Вместо матриц операторов проекций спина удобно ввести безразмерные матрицы $\hat{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$, которые называются матрицами Паули, по определению $s = \hbar/2 \hat{\sigma}$. Таким образом, декартовы компоненты введённых матриц Паули имеют вид

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (2.7)$$

Ниже тождественно используются и алгебраические обозначения для декартовых компонент матриц Паули: $\sigma_x \equiv \sigma_1$, $\sigma_y \equiv \sigma_2$, $\sigma_z \equiv \sigma_3$.

Упражнение 2.1. Показать, что проекции оператора спина удовлетворяют коммутационным соотношениям (2.1).

2.2 Свойства матриц Паули

Из определения (2.7) следует:

— матрицы Паули эрмитовы:

$$\sigma_j = \sigma_j^\dagger, \quad j = 1, 2, 3; \quad (2.8)$$

— матрицы Паули унитарны:

$$\sigma_j^{-1} = \sigma_j^\dagger, \quad j = 1, 2, 3; \quad (2.9)$$

— сумма диагональных элементов матриц Паули равна нулю:

$$Sp \sigma_j = 0, \quad j = 1, 2, 3; \quad (2.10)$$

— определитель матриц Паули равен -1 :

$$det\|\sigma_j\| = -1, \quad j = 1, 2, 3; \quad (2.11)$$

— матрицы Паули удовлетворяют перестановочным соотношениям:

$$\sigma_j \sigma_k - \sigma_k \sigma_j = 2i\sigma_\ell \varepsilon_{jkl}, \quad j, k, \ell = 1, 2, 3; \quad (2.12)$$

— матрицы Паули антикоммутативны:

$$\sigma_j \sigma_k = -\sigma_k \sigma_j, \quad j \neq k; \quad (2.13)$$

— квадрат каждой матрицы Паули равен единичной матрице:

$$\sigma_j^2 = I, \quad j = 1, 2, 3; \quad (2.14)$$

— вместе с единичной двумерной матрицей I матрицы σ_j , $j = 1, 2, 3$ образуют полный набор в пространстве матриц размерности 2×2 , т. е. любая двумерная эрмитовская матрица A может быть представлена в виде

$$A = \lambda_0 I + \sum_{k=1}^3 \lambda_k \sigma_k, \quad (2.15)$$

где λ_k — числа ($k = 0, 1, 2, 3$);

— произведение всех трёх матриц Паули образует мнимую единичную матрицу

$$\sigma_x \sigma_y \sigma_z = i I, \quad (2.16)$$

где i — мнимая единица, а I — единичная матрица размерности 2×2 .

Объединяя перечисленные выше свойства, можно записать таблицу умножения, которой удовлетворяют матрицы Паули:

$1 \setminus 2$	1	σ_x	σ_y	σ_z
1	1	σ_x	σ_y	σ_z
σ_x	σ_x	1	$i\sigma_z$	$-i\sigma_y$
σ_y	σ_y	$-i\sigma_z$	1	$i\sigma_x$
σ_z	σ_z	$i\sigma_y$	$-i\sigma_x$	1

Помимо декартовых компонент матриц Паули $\sigma_j, j = 1, 2, 3$, в физических приложениях используются их комбинации, которые называются *циклическими компонентами* матриц Паули:

$$\sigma_+ = \sigma_x + i\sigma_y = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}; \quad \sigma_- = \sigma_x - i\sigma_y = \begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix}. \quad (2.17)$$

Циклические компоненты σ_{\pm} не имеют собственных значений, так как не существует обратных к σ_{\pm} матриц и эти матрицы не являются эрмитовскими.

Квадрат циклических компонент матриц Паули удовлетворяет соотношению

$$\sigma_{\pm}^2 = (\sigma_x \pm i\sigma_y)^2 = \sigma_x^2 - \sigma_y^2 \pm i(\sigma_x\sigma_y + \sigma_y\sigma_x) = 0.$$

Таким образом, σ_{\pm} образуют объекты, которые дают пример, когда квадрат ненулевого элемента равен нулю.

Комбинации вида $(1 \pm \sigma_j)/2$, где $j \in x, y, z$, образуют идемпотентные матрицы, так как

$$\left[\frac{1}{2}(1 \pm \sigma_j) \right]^2 = \frac{1}{4}(1 \pm 2\sigma_j + 1) = \frac{1}{2}(1 \pm \sigma_j). \quad (2.18)$$

Идемпотентные матрицы удовлетворяют соотношению $N = N^2$. В квантовой теории такие матрицы называются операторами проектирования:

$$P_+ = \frac{1}{2}(1 + \sigma_z) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}; \quad P_- = \frac{1}{2}(1 - \sigma_z) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}. \quad (2.19)$$

Отметим ещё одно техническое равенство, справедливое для произвольных векторов \vec{A} и \vec{B} , которое можно установить непосредственно с учётом свойств матриц Паули:

$$(\vec{\sigma} \cdot \vec{A})(\vec{\sigma} \cdot \vec{B}) = (\vec{A} \cdot \vec{B}) + i\vec{\sigma} \cdot [\vec{A} \times \vec{B}]. \quad (2.20)$$

Упражнение 2.2. Доказать равенство (2.20).

2.3 Собственные векторы оператора спина

По определению в пространстве векторов состояний собственные векторы матриц Паули удовлетворяют соотношению

$$\sigma_k |\gamma_k\rangle = \gamma_k |\gamma_k\rangle, \quad k = 1, 2, 3. \quad (2.21)$$

В силу (2.14) собственные числа матриц Паули γ_k принимают два значения: $\gamma_k = \pm 1$. Так как оператор спина $\hat{s} = \hbar\vec{\sigma}/2$, то собственные векторы операторов проекции спина электрона в пространстве векторов состояний являются векторами в гильбертовом пространстве состояний. Для сопоставления компонентам этих векторов набора комплексных чисел воспользуемся вектором состояния с определённой проекцией спина на ось z : $|s'_z\rangle$. Здесь s'_z – спиновая переменная, принимающая только два значения, равные $\pm\hbar/2$. Данный вектор позволяет определить спиновые "функции" в s'_z -представлении: $\langle s'_z | s_x \rangle$, $\langle s'_z | s_y \rangle$ и $\langle s'_z | s_z \rangle$. В результате на основе общей теории представлений в s'_z -представлении (в котором оператор \hat{s}_z диагонален) уравнение на собственные функции и собственные значения, например для оператора $\hat{s}_z = \hbar\sigma_z/2$, имеет вид

$$\frac{\hbar}{2}\sigma_z\langle s_z | \lambda \rangle = \lambda\langle s_z | \lambda \rangle \quad \text{или} \quad \frac{\hbar}{2}\sigma_z\psi_\lambda(s_z) = \lambda\psi_\lambda(s_z). \quad (2.22)$$

В матричном изображении данное соотношение есть

$$\frac{\hbar}{2} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}_\lambda = \lambda \begin{pmatrix} a \\ b \end{pmatrix}_\lambda, \quad (2.23)$$

где для сокращения записи использовано следующее обозначение:

$$\langle s_z | \lambda \rangle \equiv \psi_\lambda(s_z) \equiv \begin{pmatrix} a \\ b \end{pmatrix}_\lambda = \begin{pmatrix} \langle s_z = +\hbar/2 | \lambda \rangle \\ \langle s_z = -\hbar/2 | \lambda \rangle \end{pmatrix}.$$

Так как $\lambda = \pm\hbar/2$, возникает два ортонормированных решения уравнения (2.3):

$$\begin{pmatrix} a \\ b \end{pmatrix}_{\lambda=+\hbar/2} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} a \\ b \end{pmatrix}_{\lambda=-\hbar/2} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \quad (2.24)$$

С учётом ортогональности векторов состояний условие нормировки для собственной функции оператора спина выглядит следующим образом:

$$\langle s_z | s_z \rangle = 1 = \sum_{\lambda=\pm\hbar/2} \langle s_z | \lambda \rangle \langle \lambda | s_z \rangle \equiv (a^*, b^*) \begin{pmatrix} a \\ b \end{pmatrix} = |a|^2 + |b|^2 = 1. \quad (2.25)$$

В обозначениях, принятых в квантовой теории представлений, собственные функции оператора проекции спина на ось z должны записываться в форме

$$\begin{pmatrix} a \\ b \end{pmatrix}_{\lambda=+\hbar/2} \equiv \begin{pmatrix} \langle \hbar/2 | \hbar/2 \rangle \\ \langle -\hbar/2 | \hbar/2 \rangle \end{pmatrix}; \quad \begin{pmatrix} a \\ b \end{pmatrix}_{\lambda=-\hbar/2} \equiv \begin{pmatrix} \langle \hbar/2 | -\hbar/2 \rangle \\ \langle -\hbar/2 | -\hbar/2 \rangle \end{pmatrix}. \quad (2.26)$$

Однако такая система обозначений достаточно громоздка. По этой причине собственные “функции” оператора σ_z для наглядности обозначают в виде, формально совпадающем с обозначением вектора в гильбертовом пространстве парой значков $|0\rangle, |1\rangle$, либо $|\uparrow\rangle, |\downarrow\rangle$ либо просто символами α, β :

$$|0\rangle \equiv |\uparrow\rangle \equiv \alpha \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}; \quad |1\rangle \equiv |\downarrow\rangle \equiv \beta \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \quad (2.27)$$

Следует подчеркнуть, что приведённое символическое обозначение собственных “функций” двух возможных спиновых состояний в форме $|0\rangle, |1\rangle$, либо $|\uparrow\rangle, |\downarrow\rangle$ по сути некорректно. Но в силу тривиального характера спиновой переменной s_z такая условность не мешает пониманию. Более корректное обозначение этих “функций” таково:

$$|0\rangle \rightarrow \alpha \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}; \quad |1\rangle \rightarrow \beta \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad (2.28)$$

где используется такая терминология: α – собственная “функция” состояния спина “вверх”, а β – собственная “функция” состояния спина “вниз”.

Учитывая явный вид матриц Паули σ_k и вид собственных функций (2.28), или (2.24), или (2.26), нетрудно установить следующие равенства:

$$\begin{aligned} \sigma_x |\uparrow\rangle &= |\downarrow\rangle; & \sigma_y |\uparrow\rangle &= i |\downarrow\rangle; & \sigma_z |\uparrow\rangle &= |\uparrow\rangle; \\ \sigma_x |\downarrow\rangle &= |\uparrow\rangle; & \sigma_y |\downarrow\rangle &= -i |\uparrow\rangle; & \sigma_z |\downarrow\rangle &= - |\downarrow\rangle. \end{aligned} \quad (2.29)$$

Для справки приведём также действие матриц σ_{\pm} и их произведений на спиновые функции α и β :

$$\sigma_+ |\uparrow\rangle = 0; \quad \sigma_- |\uparrow\rangle = 2 |\downarrow\rangle; \quad \sigma_+ |\downarrow\rangle = 2 |\uparrow\rangle; \quad \sigma_- |\downarrow\rangle = 0. \quad (2.30)$$

$$\sigma_+ \sigma_- |\uparrow\rangle = 4 |\uparrow\rangle; \quad \sigma_- \sigma_+ |\uparrow\rangle = 0; \quad \sigma_+ \sigma_- |\downarrow\rangle = 0; \quad \sigma_- \sigma_+ |\downarrow\rangle = 4 |\downarrow\rangle. \quad (2.31)$$

С учётом определения оператора спина ясно, что его собственные функции совпадают с собственными функциями безразмерных матриц Паули.

Аналогично решению уравнений (2.3), (2.22) могут быть найдены собственные “функции” операторов σ_x и σ_y (или \hat{s}_x, \hat{s}_y) в s_z -представлении. С учётом (2.7) для собственной функции σ_x имеем уравнение вида

$$\hat{s}_x \psi_{\lambda}(s_z) = \lambda \psi_{\lambda}(s_z), \quad \text{где} \quad \lambda = \pm \frac{\hbar}{2}. \quad (2.32)$$

Нормированные решения этого уравнения в s_z -представлении есть

$$|\uparrow_x\rangle \equiv \psi_{\lambda=+\hbar/2} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}; \quad |\downarrow_x\rangle \equiv \psi_{\lambda=-\hbar/2} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \quad (2.33)$$

где $|\uparrow_x\rangle$ – функция состояния с проекцией спина на ось x , направленной вдоль оси x , а $|\downarrow_x\rangle$ – функция состояния с проекцией спина на ось x , направленной против положительного направления оси x соответственно.

Уравнение на собственные функции оператора \hat{s}_y в s_z -представлении имеет вид

$$\hat{s}_y \Phi_\lambda(s_z) = \lambda \Phi_\lambda(s_z); \quad \lambda = \pm \frac{\hbar}{2}. \quad (2.34)$$

Нормированные решения данного уравнения есть

$$|\uparrow_y\rangle = \Phi_{\lambda=+\hbar/2} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}; \quad |\downarrow_y\rangle = \Phi_{\lambda=-\hbar/2} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}. \quad (2.35)$$

Здесь $|\uparrow_y\rangle$ – функция состояния с проекцией спина на ось y , направленной вдоль оси y , а $|\downarrow_y\rangle$ – функция состояния с проекцией спина на ось y , направленной против положительного направления оси y соответственно.

Представленные выше решения записаны в s_z -представлении.

Упражнение 2.3. Доказать равенства (2.29).

Упражнение 2.4. Доказать равенства (2.30), (2.31).

Упражнение 2.5. Показать, что собственные функции операторов проекции спина на оси x и y в s_z -представлении имеют вид (2.33) и (2.35) соответственно.

2.4 Вращение собственных векторов матриц Паули

В соответствии с (1.122) оператор поворота спинового состояния на угол ϕ вокруг оси \mathbf{n} равен

$$\hat{R}_{\mathbf{n}}(\phi) = \exp \left[-i \frac{\phi}{\hbar} (\hat{\mathbf{s}} \cdot \mathbf{n}) \right] = \exp \left[-i \frac{\phi}{2} (\vec{\sigma} \cdot \mathbf{n}) \right] = \sum_{k=0}^{\infty} \frac{1}{k!} \left[-i \frac{\phi}{2} (\vec{\sigma} \cdot \mathbf{n}) \right]^k, \quad (2.36)$$

так как в этом случае оператором углового момента является оператор спина $\hat{\mathbf{s}} = \hbar \vec{\sigma}/2$. Для удобного представления данного оператора поворота спинового состояния выделим суммы чётных и нечётных слагаемых в разложении (2.36). После тривиальной замены индексов суммирования в выделенных суммах оператор поворота можно записать в виде

$$\hat{R}_{\mathbf{n}}(\phi) = \sum_{k=0}^{\infty} \frac{1}{(2k)!} \left[-i \frac{\phi}{2} (\vec{\sigma} \cdot \mathbf{n}) \right]^{2k} + \sum_{k=0}^{\infty} \frac{1}{(2k+1)!} \left[-i \frac{\phi}{2} (\vec{\sigma} \cdot \mathbf{n}) \right]^{2k+1}. \quad (2.37)$$

На основании свойств матриц Паули прямыми вычислениями можно установить, что $(\vec{\sigma} \cdot \vec{n})^2 = 1$ (см. также равенство (2.20)). В результате оператор поворота из (2.37) представим следующим образом:

$$\hat{R}_n(\phi) = \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k)!} \left[\frac{\phi}{2} \right]^{2k} - i(\vec{\sigma} \cdot \vec{n}) \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k+1)!} \left[\frac{\phi}{2} \right]^{2k+1}, \quad (2.38)$$

что эквивалентно выражению

$$\hat{R}_n(\phi) = \cos \frac{\phi}{2} - i(\vec{\sigma} \cdot \vec{n}) \sin \frac{\phi}{2}. \quad (2.39)$$

В частном случае оператор поворота вокруг оси z на угол ϕ имеет вид

$$\hat{R}_z(\phi) = \cos \frac{\phi}{2} - i \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \sin \frac{\phi}{2} = \begin{pmatrix} \exp(-i\phi/2) & 0 \\ 0 & \exp(i\phi/2) \end{pmatrix}. \quad (2.40)$$

Действуя, например, оператором (2.40) на функцию состояния со спином “вверх” $|\uparrow\rangle$ по оси z , получим исходную функцию

$$\hat{R}_z |\uparrow\rangle = \hat{R}_z \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \exp(-i\phi/2) \\ 0 \end{pmatrix} = \exp(-i\phi/2) \begin{pmatrix} 1 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix} \equiv |\uparrow\rangle, \quad (2.41)$$

так как общий фазовый множитель у “функции” не имеет физического смысла и может быть опущен.

Но если осуществить поворот состояния со спином “вверх” $|\uparrow\rangle$ по оси z на угол $\phi = \pi/2$ вокруг оси y , то получим собственную функцию оператора \hat{s}_x в состоянии, когда проекция спина направлена по оси x (2.33) в исходном s_z -представлении:

$$\hat{R}_y |\uparrow\rangle = \left[\frac{1}{\sqrt{2}} - i\sigma_y \frac{1}{\sqrt{2}} \right] \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \psi_{\lambda=+\hbar/2}. \quad (2.42)$$

Из (2.33), (2.27) следует, что спиновое состояние, соответствующее проекции спина, направленного по оси x $|\uparrow_x\rangle$, может быть представлено в виде суперпозиции состояний: проекция спина по оси z (спин-вверх $|\uparrow_z\rangle$) и проекция спина против положительного направления оси z (спин-вниз $|\downarrow_z\rangle$):

$$|\uparrow_x\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right] = \frac{1}{\sqrt{2}} (|\uparrow_z\rangle + |\downarrow_z\rangle). \quad (2.43)$$

Аналогично состоянию с проекцией спина против положительного направления оси x есть суперпозиция вида

$$|\downarrow_x\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}} (|\uparrow_z\rangle - |\downarrow_z\rangle). \quad (2.44)$$

В обоих представленных случаях суперпозиции состояний (2.43), (2.44) при измерении проекции спина вдоль оси z с равной вероятностью $1/2$ получится значение спина “вверх” или значение спина “вниз” относительно оси z .

Однако если рассмотреть состояние $|a\rangle$, являющееся суперпозицией следующего вида:

$$|a\rangle = \frac{1}{\sqrt{2}} (|\uparrow_x\rangle + |\downarrow_x\rangle), \quad (2.45)$$

то при измерении спина с вероятностью, равной единице, получится значение спина “вверх” относительно оси z и никогда не будет обнаружено состояние спина “вниз”, так как

$$|a\rangle = \frac{1}{2} (|\uparrow_z\rangle + |\downarrow_z\rangle + |\uparrow_z\rangle - |\downarrow_z\rangle) = |\uparrow_z\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Суперпозиция состояний спина $1/2$ является физической моделью понятия кубита, введённого в предыдущей главе. Используя определение кубита и определение среднего значения физической величины, можно вычислить средние значения проекций спина в заданном произвольном однокубитовом состоянии $|q\rangle = a_0|0\rangle + a_1|1\rangle$, $\langle q|q\rangle = 1$. Так, для среднего значения проекции спина на ось x получим

$$\langle \hat{s}_x \rangle = \langle q| s_x |q\rangle = \frac{\hbar}{2} (a_0^*, a_1^*) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} = \frac{\hbar}{2} (a_0 a_1^* + a_0^* a_1). \quad (2.46)$$

Аналогичные вычисления для средних значений проекции спина на оси y и z приводят к следующим результатам:

$$\langle \hat{s}_y \rangle = \frac{\hbar}{2} (i a_0 a_1^* - i a_0^* a_1); \quad \langle \hat{s}_z \rangle = \frac{\hbar}{2} (a_0 a_0^* - a_1^* a_1). \quad (2.47)$$

Используя параметры, определяющие кубит через параметры на сфере Блоха, для средних значений проекций спина (2.46), (2.47) получим общие выражения в виде

$$\langle \hat{s}_x \rangle = \frac{\hbar}{2} \sin(\theta) \cos(\varphi); \quad \langle \hat{s}_y \rangle = \frac{\hbar}{2} \sin(\theta) \sin(\varphi); \quad \langle \hat{s}_z \rangle = \frac{\hbar}{2} \cos(\theta). \quad (2.48)$$

Упражнение 2.6. Вычислить результат действия оператора поворота на состояние $|\downarrow_x\rangle$ вокруг оси y на углы $\phi = \pm\pi/2$.

Упражнение 2.7. Вывести равенства (2.47).

Упражнение 2.8. Вывести равенства (2.48).

2.5 Уравнение Паули

Обобщение принципов квантовой теории, предложенной Шрёдингером, на случай когда учитывается спин частиц, образующих систему, выполнено Паули. Технический смысл обобщения сводится к тому, что вместо оператора Гамильтона уравнения Шрёдингера при описании системы используется оператор Гамильтона — Паули ($\hat{H}_{\text{Паули}}$), включающий помимо кинетической и потенциальной энергий энергию взаимодействия спинов с внешним полем. При этом гамильтониан Паули становится матрицей размерности 2×2 . Так, если спин частицы находится во внешнем магнитном поле с индукцией $\mathbf{B} = \text{rot} \mathbf{A}$, где \mathbf{A} — векторный потенциал, энергия взаимодействия спина с внешним полем определяется как скалярное произведение магнитного спинового момента \mathbf{m}_s и индукции магнитного поля $V = -(\mathbf{m}_s \cdot \mathbf{B})$ или

$$V = -(\mathbf{m}_s \cdot \mathbf{B}) = -\frac{e}{mc}(\hat{\mathbf{s}} \cdot \mathbf{B}) = -\frac{e\hbar}{2mc}(\vec{\sigma} \cdot \mathbf{B}). \quad (2.49)$$

Здесь e — заряд, m — масса частицы, c — скорость света. Соответственно, для описания системы вводится двухкомпонентная функция (столбец) $\Psi_{\text{Паули}}$, и обобщение квантового уравнения Шрёдингера, предложенное Паули, имеет вид

$$i\hbar \frac{\partial}{\partial t} \Psi_{\text{Паули}}(q, t) = \hat{H}_{\text{Паули}} \Psi_{\text{Паули}}(q, t), \quad \text{где} \quad \Psi_{\text{Паули}}(q, t) = \begin{pmatrix} \psi_1(q, t) \\ \psi_2(q, t) \end{pmatrix}. \quad (2.50)$$

Здесь q — пространственные и спиновые переменные, t — время.

Оператор Гамильтона — Паули для одной частицы имеет вид

$$\hat{H}_{\text{Паули}} = \frac{1}{2m} \left(\mathbf{p} - \frac{e}{c} \mathbf{A} \right)^2 + e\varphi_0 - \frac{e\hbar}{2mc}(\vec{\sigma} \cdot \mathbf{B}), \quad (2.51)$$

где φ_0 и \mathbf{A} — скалярный и векторный потенциалы соответственно. Таким образом, уравнение Паули — это система двух уравнений для определения функций $\psi_1(q, t)$ и $\psi_2(q, t)$.

Если оператор Гамильтона — Паули не зависит от времени, то

$$\Psi_{\text{Паули}}(q, t) = \Phi_{\text{Паули}}(q) \exp \left(-i \frac{E}{\hbar} t \right) = \begin{pmatrix} \varphi_1(q) \\ \varphi_2(q) \end{pmatrix} \exp \left(-i \frac{E}{\hbar} t \right). \quad (2.52)$$

Здесь E — энергия системы, а функция (столбец) $\Phi_{\text{Паули}}(q)$ удовлетворяет матричному 2×2 уравнению на собственные функции оператора $\hat{H}_{\text{Паули}}$:

$$\hat{H}_{\text{Паули}} \Phi_{\text{Паули}}(q) = E \Phi_{\text{Паули}}(q). \quad (2.53)$$

Упражнение 2.9. Записать уравнение Паули для свободного электрона, находящегося в магнитном поле, заданном векторным потенциалом \mathbf{A} .

Упражнение 2.10. Найти решение уравнения Паули для покоящегося электрона в постоянном магнитном поле с индукцией \mathbf{B} .

2.6 Спиновый резонанс для свободного электрона

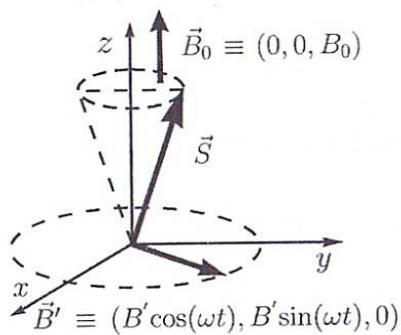


Рис. 2.1. Спин в магнитном поле

решение задачи, которая демонстрирует возможность управления кубитом посредством взаимодействия спина электрона с внешним магнитным полем.

В качестве примера рассмотрим поведение спина, находящегося в магнитном поле с индукцией $\vec{B}_0 \equiv (0, 0, B_0)$, направленной по оси z . Пусть в момент времени $t = 0$ дополнительно включается переменное магнитное поле с индукцией $\vec{B}' \equiv (B' \cos(\omega t), B' \sin(\omega t), 0)$, вектор которой лежит в плоскости x и y . Положим, что в начальный момент времени спин находится в состоянии “спин-вверх” (рис. 2.1). Найдём изменение состояния спина в такой системе с течением времени [12].

Описание поведения спина электрона (заряд e , масса m) основывается на решении уравнения Паули. В координатном представлении оператор Гамильтона – Паули такой системы совпадает с потенциальной энергией взаимодействия спинового магнитного момента $\vec{\mu}_s$ с внешним полем $\vec{B} = \vec{B}_0 + \vec{B}'$,

$$\hat{H} = -(\vec{\mu} \cdot \vec{B}) = -\frac{e\hbar}{2mc} (\vec{\sigma} \cdot \vec{B}) = \mu_0 (\vec{\sigma} \cdot \vec{B}), \quad \mu_0 \equiv \frac{|e|\hbar}{2mc}. \quad (2.54)$$

Здесь параметр μ_0 определяется фундаментальными константами и называется магнетоном Бора. С учетом выбранной геометрии и определения

циклических компонент матриц Паули (2.17) гамильтониан имеет вид

$$\hat{H} = \mu_0(\sigma_z B_0 + \sigma_x B'_x + \sigma_y B'_y) = \mu_0 \left[\sigma_z B_0 + \frac{1}{2} B' (\sigma_+ e^{-i\omega t} + \sigma_- e^{i\omega t}) \right]. \quad (2.55)$$

Уравнение Паули в этом случае есть

$$i\hbar \frac{\partial \Psi}{\partial t} = \mu_0 \left\{ B_0 \sigma_z + \frac{1}{2} B' (\sigma_+ e^{-i\omega t} + \sigma_- e^{i\omega t}) \right\} \Psi. \quad (2.56)$$

Решение уравнения (2.56) можно представить в виде суперпозиции двух возможных спиновых состояний $-|0\rangle \equiv \alpha$ и $|1\rangle \equiv \beta$:

$$\Psi(t) = u(t)|0\rangle + v(t)|1\rangle = u(t) \begin{pmatrix} 1 \\ 0 \end{pmatrix} + v(t) \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} u(t) \\ v(t) \end{pmatrix}, \quad (2.57)$$

где коэффициенты разложения являются функциями времени и подлежат определению. Подставляя (2.57) в (2.56) с учётом соотношений (2.30) и (2.29), получим систему уравнений

$$\begin{cases} i\dot{u} = -\omega_0 u + \omega' e^{-i\omega t} v \\ i\dot{v} = -\omega_0 v + \omega' e^{i\omega t} u \end{cases}, \quad (2.58)$$

где введены следующие обозначения: $\omega_0 \equiv \mu_0 B_0 / \hbar$; $\omega' \equiv \mu_0 B' / \hbar$. Кроме того, точка над функцией означает первую производную по времени. Для решения данной системы уравнений выполним замену функций по определению $u(t) \equiv \exp(-it\omega/2) U(t)$, $v(t) \equiv \exp(+it\omega/2) V(t)$. В результате систему уравнений (2.58) перепишем в виде

$$\begin{cases} i \left(\dot{U} - i \frac{\omega}{2} U \right) = -\omega_0 U + \omega' V \\ i \left(\dot{V} + i \frac{\omega}{2} V \right) = -\omega_0 V + \omega' U \end{cases}. \quad (2.59)$$

Умножим первое из уравнений системы (2.59) на $-i$ и запишем систему следующим образом:

$$\begin{cases} \dot{U} = -i\alpha U - i\omega' V \\ i\dot{V} = -\alpha V + \omega' U \end{cases}. \quad (2.60)$$

Здесь $\alpha \equiv \omega_0 - \omega/2$. Складывая и вычитая уравнения в полученной системе, можно найти систему уравнений для функций $\Phi = U + iV$ и $\Upsilon = U - iV$:

$$\begin{cases} \dot{\Phi} = (\omega' - i\alpha) \Upsilon \\ \dot{\Upsilon} = -(\omega' + i\alpha) \Phi \end{cases}. \quad (2.61)$$

Дифференцируя первое из уравнений (2.61) по времени с учётом второго уравнения, находим, что уравнение для Φ есть уравнение второго порядка с постоянными коэффициентами вида $\ddot{\Phi} + \Omega^2 \Phi = 0$, где $\Omega = \sqrt{\omega'^2 + \alpha^2} = \sqrt{\omega'^2 + (\omega_0 - \omega/2)^2}$. Полностью аналогичному уравнению удовлетворяет функция Υ .

Окончательно нормированное решение системы (2.58), удовлетворяющее начальному условию $\Psi(0) = |0\rangle$, равно

$$\Psi(t) = \left[\cos(\Omega t) - \frac{\omega_0 - \omega/2}{\Omega} \sin(\Omega t) \right] e^{-i\omega t/2} |0\rangle - \frac{\omega'}{\Omega} \sin(\Omega t) e^{i\omega t/2} |1\rangle. \quad (2.62)$$

Как следует из (2.62), например, вероятность измерения состояния “спин-вниз” с течением времени осциллирует и определяется выражением

$$P(t) = |v(t)|^2 = \left(\frac{\omega'}{\Omega} \right)^2 \sin^2(\Omega t). \quad (2.63)$$

Усреднённая за период $T = 2\pi/\Omega$ вероятность в этом случае есть

$$\langle P(t) \rangle = \frac{1}{T} \int_0^T P(t) dt = \frac{1}{2} \frac{\omega'^2}{\Omega^2} = \frac{\omega'^2}{(\omega_0 - \frac{1}{2}\omega)^2 + \omega'^2}. \quad (2.64)$$

Таким образом, можно сделать вывод о том, что если медленно менять B_0 , то для $\omega_0 = \omega/2$ (или $B_0 = \hbar\omega/2\mu_0$) вероятность окажется максимальной, равной $\langle P \rangle_{max} = 1/2$, независимо от вращающегося поля. Такое поле B_0 называется *резонансным*, а явление переворачивания спина — *спин-флип*.

Кроме того, теоретически, в соответствии с (2.62), управляя магнитными полями, можно получить суперпозицию состояний с требуемыми значениями u и v (т. е. приготовить кубит в определённой суперпозиции).

Упражнение 2.11. Вывести вид оператора Гамильтона — Паули в форме (2.55).

Упражнение 2.12. Вывести вид системы уравнений Паули (2.58).

Упражнение 2.13. Найти явный вид решения системы уравнений Паули (2.62).

2.7 Двухуровневая система

В общем случае имеются и другие физические системы, которые удовлетворяют определению кубита. Так, любая двухуровневая квантовая си-

стема или два различных состояния поляризации электромагнитного излучения также могут привести к физической реализации кубита.

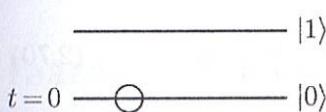


Рис. 2.2. Двухуровневая система

Рассмотрим в качестве примера произвольную двухуровневую систему (рис. 2.2) [12]. Пусть до момента $t = 0$ система определялась гамильтонианом H_0 , имеющим только два стационарных состояния, которые для краткости обозначим $|0\rangle$ и $|1\rangle$:

$$\hat{H}_0 |k\rangle = E_k |k\rangle, \quad k = 0, 1. \quad (2.65)$$

Здесь использованы обозначения $|0\rangle = \phi_0$ и $|1\rangle = \phi_1$. В момент времени $t = 0$ система находилась в состоянии ϕ_0 . В момент времени $t = 0$ на систему накладывается не зависящее от времени взаимодействие \hat{W} (например, постоянное поле). Дальнейшая эволюция системы удовлетворяет уравнению Шрёдингера:

$$i\hbar \frac{\partial \Psi}{\partial t} = (\hat{H}_0 + \hat{W})\Psi. \quad (2.66)$$

Решение уравнения (2.66) можно представить в виде

$$\Psi(t) = c_0(t) \exp(-i\omega_0 t)\phi_0 + c_1(t) \exp(-i\omega_1 t)\phi_1, \quad \hat{H}_0 \phi_k = E_k \phi_k, \quad (2.67)$$

где $\omega_k = E_k/\hbar$; $k \in 0, 1$ с начальным условием $c_0(0) = 1$; $c_1(0) = 0$.

Подставляя (2.67) в (2.66) и проектируя уравнение один раз на состояние ϕ_0 , а второй — на состояние ϕ_1 , получим систему уравнений для c_0 и c_1 , решение которой имеет вид

$$\begin{aligned} c_0(t) &= \left[\cos(\sigma t) + i \frac{\gamma}{2\sigma} \sin(\sigma t) \right] \exp(-i\lambda t), \\ c_1(t) &= -i \frac{\langle 0 | \hat{W} | 1 \rangle}{\hbar\sigma} \sin(\sigma t) \exp[-i(\lambda - \omega_{10})t], \end{aligned} \quad (2.68)$$

где $\hbar\sigma \equiv \sqrt{\gamma^2\hbar^2/4 + |W_{01}|^2}$, $\hbar\gamma \equiv W_{11} - W_{00} + \hbar\omega$, $\omega_{10} \equiv \omega_1 - \omega_0$, $\lambda \equiv W_{11}/\hbar + \gamma/2$,

$$W_{ij} \equiv \langle i | W | j \rangle \equiv \int \phi_i^* \hat{W} \phi_j dv \quad i, j \in 0, 1.$$

В результате вероятность найти систему в состоянии ϕ_1 (если в начальный момент времени система находилась в состоянии ϕ_0) есть

$$|c_1(t)|^2 = \frac{4 |W_{01}|^2}{(\hbar\gamma)^2 + 4 |W_{01}|^2} \sin^2(\sigma t). \quad (2.69)$$

Усреднённая за период $T = 2\pi/\sigma$ вероятность найти систему в возбуждённом состоянии ϕ_1 равна

$$\langle |c_1(t)|^2 \rangle = \frac{1}{T} \int_0^T |c_1(t)|^2 dt = \frac{2|W_{01}|^2}{(\hbar\gamma)^2 + 4|W_{01}|^2}. \quad (2.70)$$

В реальном случае выполняется неравенство $\hbar\gamma \gg W_{01}$, и, таким образом, вероятность найти систему в возбуждённом состоянии в данном примере — достаточно маленькая величина.

Вероятность обнаружить систему в исходном состоянии определяется выражением

$$|c_0(t)|^2 = 1 - |c_1(t)|^2 = 1 - \frac{4|W_{01}|^2}{(\hbar\gamma)^2 + 4|W_{01}|^2} \sin^2(\sigma t) \quad (2.71)$$

и близка к единице.

Но если та же самая система находится под влиянием возмущения, периодически зависящего от времени $\hat{W} = \hat{W}_0 \cos(\omega t)$, и при этом частота поля такова, что практически совпадает с частотой $\omega_{10} = \omega_1 - \omega_0$, то вероятность обнаружить систему в возбуждённом состоянии определяется выражением

$$|c_1(t)|^2 = \frac{\Gamma}{\sqrt{\Gamma^2 + (\Delta\omega)^2}} \sin^2\left(\frac{1}{2}\Omega t\right). \quad (2.72)$$

Здесь $\hbar\Gamma \equiv W_{01} = \langle 0 | \hat{W}_0 | 1 \rangle$, $\Delta\omega \equiv \omega - \omega_{10}$, $\Omega \equiv \sqrt{\Gamma^2 + (\Delta\omega)^2}$. Как видно, переход системы в возбуждённое состояние представляет собой ясно выраженный резонансный процесс, так как вероятность процесса быстро падает по мере роста величины $|\Delta\omega|$. Соответственно, при $\Delta\omega = 0$ вероятности $|c_1|^2$ и $|c_0|^2$ определяются выражениями

$$|c_1(t)|^2 = \sin^2\left(\frac{1}{2}\Omega t\right), \quad |c_0(t)|^2 = \cos^2\left(\frac{1}{2}\Omega t\right). \quad (2.73)$$

Таким образом, двухуровневая система, находящаяся под влиянием возмущения, периодически зависящего от времени, также попадет под определение кубита как система, осциллирующая между двумя стационарными состояниями.

Упражнение 2.14. Найти явный вид системы уравнений для рассматриваемой двухуровневой системы и решение системы уравнений в форме (2.68).

Глава 3

Матрица плотности

3.1 Чистые и смешанные состояния

Описание системы опирается в квантовой теории на вектор состояния. Однако при рассмотрении совокупности систем (например, ансамбля одинаковых систем) использование принципов квантовой теории требует уточнений и введения правил вычисления наблюдаемых величин в ансамбле систем. Чтобы подчеркнуть возникающее различие, напомним результаты эксперимента Штерна — Герлаха для частиц со спином 1/2.

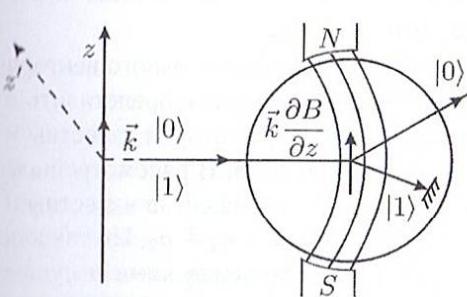


Рис. 3.1. Схема опыта Штерна — Герлаха

спина: $|0\rangle$ или $|1\rangle$. Если один из прошедших пучков удалить, например пучок частиц в состоянии $|1\rangle$, то оставшиеся частицы будут находиться в состоянии, соответствующем лишь состоянию $|0\rangle$ (рис. 3.1).

Очевидно, что если падающий пучок содержит только частицы, спины которых ориентированы вдоль оси z , т. е. частицы находятся в состоянии $|0\rangle$, то весь пучок частиц пройдет сквозь установку без потери интенсивности. Если ось установки наклонить, т. е. изменить направление градиента поля, то только часть пучка пройдет через установку и прошедший пучок

В данном эксперименте рассматривается пучок частиц со спином 1/2, проходящий через неоднородное магнитное поле, градиент которого направлен вдоль оси z . До попадания в поле частицы находятся в суперпозиции вида $a|0\rangle + b|1\rangle$. После прохождения области магнитного поля пучок расщепляется на два, каждый из которых соответствует одному из двух возможных состояний

будет менее интенсивный, чем падающий.

В общем случае, если падающий пучок содержит спины, ориентированные вдоль некоторой произвольной оси z' , то путём поворота установки можно найти такую её ориентацию, при которой пропускается весь пучок.

Если в опыте Штерна — Герлаха можно найти ориентацию установки, при которой падающий пучок полностью пропускается, то говорят о *чистом спиновом состоянии* пучка. В чистом состоянии совместное состояние всех частиц представляется с помощью одного вектора состояния. Изображённую на рис. 3.1 установку можно рассматривать как способ приготовления пучка частиц в чистом состоянии.

Чистые спиновые состояния не являются наиболее общими состояниями, в которых может находиться ансамбль частиц. Пусть два пучка частиц приготовлены в чистых состояниях $|0\rangle$ и $|1\rangle$ независимо. Положим, что пучок состоит из n_1 частиц в состоянии $|0\rangle$ и из n_2 частиц в состоянии $|1\rangle$. Направим объединённый пучок этих частиц на фильтр Штерна — Герлаха, у которого будем менять направление градиента магнитного поля. Опыт показывает, что невозможно найти такую ориентацию фильтра, при которой через него проходит весь пучок полностью. Таким образом, объединённый пучок по определению не является чистым спиновым состоянием. Такие состояния называются *смешанными состояниями*.

Смешанное состояние невозможно описать с помощью одного вектора состояний. Другими словами, смешанное состояние нельзя представить в виде линейной суперпозиции состояний $a|0\rangle + b|1\rangle$, в которой известны и модули коэффициентов a и b , и их относительная фаза. В рассмотренном выше случае смеси спинов квадраты модулей коэффициентов известны и равны соответственно $|a|^2 = n_1/n$; $|b|^2 = n_2/n$, где $n = n_1 + n_2$. Но так как оба пучка приготовлены независимо друг от друга, то между ними не существует определённого фазового соотношения, а без значения фазы нельзя построить суперпозицию чистого состояния. В связи с этим возникает вопрос о способе описания смешанных состояний ансамбля частиц.

Прежде чем перейти непосредственно к смешанным состояниям, рассмотрим способы вычисления среднего значения величины F в произвольном чистом состоянии вида

$$|\Psi\rangle = \sum_n c_n |n\rangle, \quad c_n = \langle n | \Psi \rangle, \quad (3.1)$$

где $|n\rangle$ — ортонормированный базис. В соответствии с общей теорией среднее значение физической величины F в представленном чистом состоянии

$|\Psi\rangle$ определяется выражением

$$\langle F \rangle = \langle \Psi | \hat{F} | \Psi \rangle = \sum_{m,n} c_m^* c_n \langle m | F | n \rangle = \sum_{m,n} F_{mn} c_m^* c_n. \quad (3.2)$$

В данном выражении произведение комплексных коэффициентов $c_m^* c_n$ можно рассматривать как матрицу, для которой введём следующее обозначение:

$$\varrho_{nm} = c_n c_m^*. \quad (3.3)$$

В результате правило вычисления среднего значения можно переписать в эквивалентном виде:

$$\langle F \rangle = \sum_{mn} F_{mn} \varrho_{nm} = \sum_{n,m} \varrho_{nm} F_{mn}. \quad (3.4)$$

Матрицу ϱ_{nm} можно рассматривать как матричный элемент от некоторого оператора $\hat{\varrho}$, т. е. $\varrho_{nm} \equiv \langle n | \hat{\varrho} | m \rangle$. В результате среднее значение оператора \hat{F} можно переписать следующим образом:

$$\begin{aligned} \langle F \rangle &= \sum_{n,m} \varrho_{nm} F_{mn} = \sum_{n,m} \langle n | \hat{\varrho} | m \rangle \langle m | \hat{F} | n \rangle = \\ &= \sum_n \langle n | \hat{\varrho} \hat{F} | n \rangle = Sp(\hat{\varrho} \hat{F}). \end{aligned} \quad (3.5)$$

Здесь $Sp(A) \equiv Tr(A)$ — след оператора. В данном случае оператор $\hat{A} = \hat{\varrho} \hat{F}$ есть произведение операторов $\hat{\varrho}$ и \hat{F} , матричные элементы которых можно записать в виде $\varrho_{nm} = \langle n | \hat{\varrho} | m \rangle$ и $F_{mn} = \langle m | \hat{F} | n \rangle$ соответственно. Таким образом вводится оператор $\hat{\varrho}$, получивший название *оператор плотности*, а матрица ϱ (3.3) называется *матрицей плотности*. След произведения операторов, как следует из (3.4), можно переписать, используя свойство следа оператора $Sp(\hat{A} \hat{B}) = Sp(\hat{B} \hat{A})$. Таким образом, эквивалентные формулы для вычисления среднего значения $\langle F \rangle$ для чистых состояний с использованием оператора плотности могут быть представлены выражениями:

$$\langle F \rangle = Sp(\hat{\varrho} \hat{F}) = \sum_{n,m} \varrho_{nm} F_{mn} = \sum_{m,n} F_{mn} \varrho_{nm} = Sp(\hat{F} \hat{\varrho}). \quad (3.6)$$

Так как в соответствии с (3.3) $\varrho_{nm} = c_n c_m^*$, то с учётом $c_n = \langle n | \Psi \rangle$ и $c_m^* = \langle \Psi | m \rangle$ получим

$$\varrho_{nm} = c_n c_m^* = \langle n | \Psi \rangle \langle \Psi | m \rangle = \langle n | |\Psi\rangle \langle \Psi| |m\rangle = \langle n | \hat{\varrho} | m \rangle. \quad (3.7)$$

Таким образом, явный вид оператора плотности для чистого состояния Ψ имеет вид

$$\hat{\rho} = |\Psi\rangle \langle \Psi|. \quad (3.8)$$

Естественно, что результат вычисления среднего значения оператора в чистом состоянии с использованием матрицы плотности ничем не отличается от выражения (3.2), в котором используется вектор состояния Ψ . Для чистого состояния $\hat{\rho}$ несёт ту же информацию о системе, что и вектор состояния Ψ .

Однако введение матрицы плотности даёт регулярное правило вычисления среднего значения для смешанных состояний, при описании которых используется данный формализм. В смешанном состоянии оператор плотности $\hat{\rho}$ определяется выражением

$$\hat{\rho} = \sum_n p_n |\Psi_n\rangle \langle \Psi_n| = \sum_n p_n \hat{P}_n. \quad (3.9)$$

Здесь p_n — вероятность чистого состояния Ψ_n в смеси состояний ансамбля систем, $P_n = |\Psi_n\rangle \langle \Psi_n|$ — оператор проектирования, $\sum_n p_n = 1$. В частном случае одного чистого состояния Ψ_0 вероятность $p_n = \delta_{n0}$, где δ_{n0} — символ Кронекера. Постулатом квантовой теории при описании смешанных состояний является правило вычисления среднего значения оператора в соответствии с равенством

$$\langle F \rangle = Sp(\hat{\rho}F). \quad (3.10)$$

В общем случае для оператора плотности смешанного состояния из его определения можно установить, что оператор плотности — эрмитовский $\hat{\rho} = \hat{\rho}^\dagger$. След от оператора плотности равен $Sp(\hat{\rho}) = 1$, так как на основании (3.10) выполняются соотношения $1 = \langle 1 \rangle = Sp(\hat{\rho}1) = Sp(\hat{\rho})$. Наконец, $Sp(\hat{\rho}^2) \leq 1$ и при этом равенство единице возникает только для чистого состояния.

Описание квантовых систем с использованием матрицы плотности возникает не только для смешанных состояний, но и при описании так называемых “запутанных” состояний, образующихся при специальных преобразованиях, в том числе и чистых состояний. Так, в соответствии с общей идеологией квантовой теории свойства любой системы определяются вектором состояния в гильбертовом пространстве, при этом необходимо учесть все взаимодействия, которым подвержена рассматриваемая система. В этом смысле требуется построить и использовать вектор состояния всей Вселенной. Конечно, реальное описание систем ограничивается и

пространственными рамками, и выделением только части взаимодействий, существенных с физической точки зрения. Другими словами, из всей Вселенной “вырезается” небольшая часть, которая и подвергается изучению. Большая часть опускается в соответствии с определёнными модельными предположениями. Однако при рассмотрении части большой системы необходимо иметь в виду, что: *состояния подсистем не являются лучами в гильбертовом пространстве; измерения в подсистеме не являются ортогональным проектированием; эволюция подсистемы не определяется унитарными преобразованиями.*

Рассмотрим для примера две бесконечно удалённые, невзаимодействующие системы, свойства которых задаются векторами состояний $|A_n(x)\rangle$ и $|B_m(y)\rangle$. Состояние объединённой системы, включающей как первую, так и вторую системы, хорошо определяется в объединённом гильбертовом пространстве вектором состояния $|\Psi_{in}\rangle = |A_n\rangle \otimes |B_m\rangle$. Сведём рассматриваемые системы воедино, в результате чего они могут взаимодействовать друг с другом, изменяя свои состояния. Таким образом начальное состояние $|\Psi_{in}\rangle$ перейдет к моменту времени t в состояние, которое обозначим через $|\Psi(t)\rangle$.

Разведём далее системы снова на бесконечные расстояния и прекратим их взаимодействие. В целом, объединённая система будет определяться вектором состояния $|\Psi_{out}(x, y)\rangle$, который зависит от переменных обеих систем. Учитывая, что набор начальных состояний $|A_n\rangle \otimes |B_m\rangle$ в объединённом гильбертовом пространстве полный, состояние $|\Psi_{out}\rangle$ можно представить в виде

$$|\Psi_{out}\rangle = \sum_{n,m} c_{nm}(x, y) |A_n(x)\rangle \otimes |B_m(y)\rangle. \quad (3.11)$$

В соответствии с принципом суперпозиции $|c_{nm}|^2$ даёт вероятность нахождения системы A в состоянии $|A_n\rangle$ и одновременно системы B в состоянии $|B_m\rangle$ после их взаимодействия. Другими словами, конкретное конечное состояние системы A , например $|A_k\rangle$, связано с набором конечных состояний системы B . Это означает, что невозможно записать конечное состояние в виде прямого произведения состояний системы $|A\rangle$ и $|B\rangle$, которые зависели бы только от переменных каждой системы, т. е. $|\Psi_{out}\rangle \neq |A\rangle \otimes |B\rangle$.

Таким образом, формулируется утверждение, которое иногда называют *принципом несепарабельности: если две системы взаимодействовали в прошлом, то в общем случае невозможно присвоить один вектор состояния любой из двух подсистем.*

Пусть, например, система A подвергается процессу измерения после взаимодействия. В результате измерения система A будет обнаружена в состоянии, которое не является *чистым* состоянием. В этом случае говорят, что неподверженная процессу измерения система B приводит к потере когерентности в системе A .

Рассмотрим для примера систему из двух кубитов A и B , находящихся в некотором квантовом состоянии. Ортонормированный базис для кубита A и B обозначим соответственно $\{|0\rangle_A, |1\rangle_A\}$ и $\{|0\rangle_B, |1\rangle_B\}$. При этом над кубитом A производятся измерения, а кубит B недоступен. Необходимо сформулировать принципы, которые позволяют характеризовать результаты наблюдения кубита A . Пусть двухкубитовое состояние имеет следующий вид:

$$|\Psi\rangle_{AB} = a|0\rangle_A \otimes |0\rangle_B + b|1\rangle_A \otimes |1\rangle_B. \quad (3.12)$$

Это означает, что кубиты были подвержены некоторому воздействию, приведшему к образованию состояния (3.12), и, следовательно, они скоррелированы. Так, если спроектировать состояние (3.12) на базис кубита A , то с вероятностью $|a|^2$ будет получен результат $|0\rangle_A$ и измерение приведёт к редукции состояния $|\Psi\rangle_{AB}$ к состоянию $|\Psi\rangle_{AB} \rightarrow |0\rangle_A \otimes |0\rangle_B$ из (3.12), а с вероятностью $|b|^2$ будет получен результат $|1\rangle_A$ с редукцией (3.12) в состояние $|\Psi\rangle_{AB} \rightarrow |1\rangle_A \otimes |1\rangle_B$. Другими словами, измерение состояния кубита A привело кубит B в определённое базисное состояние. При этом кубиты могли до измерения находиться в разных точках пространства.

В общем случае, действие самосопряжённого оператора \hat{F} только на кубит A в состоянии (3.12) определяется оператором $\hat{F}_A \otimes \hat{I}_B$, где \hat{I}_B – единичный оператор, действующий на кубит B . Среднее значение наблюдаемой \hat{F} в состоянии (3.12) есть

$$\langle F \rangle = {}_{AB}\langle \Psi | \hat{F}_A \otimes \hat{I}_B | \Psi \rangle_{AB} = |a|^2 \langle 0 | F | 0 \rangle_A + |b|^2 \langle 1 | F | 1 \rangle_A. \quad (3.13)$$

Как видно, это выражение соответствует вычислению среднего значения с использованием оператора плотности:

$$\langle F \rangle_A = Sp(\hat{\rho}_A \cdot \hat{F}_A), \quad (3.14)$$

где оператор $\hat{\rho}_A$ определён соотношением

$$\hat{\rho}_A = |a|^2 |0\rangle \langle 0|_A + |b|^2 |1\rangle \langle 1|_A \quad (3.15)$$

и является оператором плотности для кубита. Введённый способ описания части системы существенно отличается от описания когерентной суперпозиции состояний $|0\rangle$ и $|1\rangle$ для изолированного кубита и опирается на понятие ансамбля состояний.

Существенное отличие чистых и смешанных состояний можно продемонстрировать и на ранее приведённом примере, в котором показано, что при измерении σ_x в однокубитовом состоянии $(|\uparrow_z\rangle + |\downarrow_z\rangle)/\sqrt{2}$ с вероятностью, равной единице, следует результат $|\uparrow_x\rangle$. Но ансамбль спинов, в котором состояния $|\uparrow_z\rangle$ и $|\downarrow_z\rangle$ присутствуют с равной вероятностью $1/2$, представляется уже оператором матрицы плотности вида (см. (3.15))

$$\varrho = \frac{1}{2} |\uparrow_z\rangle \langle \uparrow_z| + \frac{1}{2} |\downarrow_z\rangle \langle \downarrow_z| = \frac{1}{2} \begin{pmatrix} 1 \\ 0 \end{pmatrix} (1, 0) + \frac{1}{2} \begin{pmatrix} 0 \\ 1 \end{pmatrix} (0, 1) = \frac{1}{2} I. \quad (3.16)$$

А так как оператор проектирования \hat{P}_n на состояние $|n\rangle$ определён равенством $|n\rangle \langle n|$, то проекция на состояние спина $|\uparrow_x\rangle$ в этом случае с учётом соотношения (2.33) есть

$$\begin{aligned} \langle |\uparrow_x\rangle \langle \uparrow_x| \rangle &= Sp\left\{(|\uparrow_x\rangle \langle \uparrow_x| \varrho)\right\} = Sp\left\{\frac{1}{2} \begin{pmatrix} 1 \\ 1 \end{pmatrix} (1, 1) \frac{1}{2} I\right\} = \\ &= Sp\left\{\frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \frac{1}{2} I\right\} = \frac{2}{4} = \frac{1}{2}, \end{aligned} \quad (3.17)$$

что отличается от чистого состояния, в котором такая вероятность, как отмечено выше, равна 1.

Обсуждение коррелиированного двухкубитового состояния $|\Psi\rangle_{AB}$ (3.12) тривиально обобщается на произвольное состояние любой системы, состоящей из двух подсистем A и B . Гильбертово пространство объединённых A и B состояний есть $H_A \otimes H_B$, где H_k — гильбертовы пространства частей A и B соответственно с ортонормированными базисами $|n\rangle_A$ и $|m\rangle_B$. Таким образом, произвольное нормированное чистое состояние в пространстве $H_A \otimes H_B$ может быть представлено в виде

$$|\Psi\rangle_{AB} = \sum_{n,m} a_{nm} |n\rangle_A \otimes |m\rangle_B, \quad (3.18)$$

$$\langle \Psi | \Psi \rangle_{AB} = \sum_{n,m} |a_{nm}|^2 = 1. \quad (3.19)$$

Среднее значение наблюдаемой $\hat{F}_A \otimes \hat{I}_B$, оператор которой действует только на подсистему A , определяется равенством

$$\langle \hat{F} \rangle_A = \langle \Psi | \hat{F}_A \otimes \hat{I}_B | \Psi \rangle_{AB} = \sum_{k,n,m} a_{km}^* a_{nm} \langle k | \hat{F} | n \rangle_A = Sp(\hat{F}_A \hat{\varrho}_A), \quad (3.20)$$

где

$$\hat{\varrho}_A \equiv Sp_B (|\Psi\rangle_{AB} \langle \Psi|_{AB}) = \sum_{n,m,k} a_{nm} a_{km}^* |n\rangle_A \langle k|_A. \quad (3.21)$$

Определённый в (3.21) оператор называется оператором плотности подсистемы или редуцированным оператором матрицы плотности. Таким образом, если даже состояние целой системы является лучом в гильбертовом пространстве, то состояние подсистемы в общем случае не является лучом в гильбертовом пространстве, а является смесью состояний. В частном случае состояние подсистемы может оказаться лучом и в этом случае являться чистым состоянием. Если состояние подсистемы является чистым состоянием $|\Psi\rangle_A$, тогда оператор матрицы плотности $\hat{\varrho}_A = |\Psi\rangle_A \langle \Psi|_A$ является оператором проектирования. Матрица плотности чистого состояния является идемпотентным оператором, т. е. $\hat{\varrho}^2 = \hat{\varrho}$.

Так как оператор $\hat{\varrho}_A$ подсистемы самосопряжённый, то он может быть приведён к диагональному виду

$$\hat{\varrho}_A = \sum_n p_n |n\rangle \langle n|, \quad (3.22)$$

где $0 < p_n \leq 1$ и $\sum_n p_n = 1$.

В общем случае (в смешанном состоянии) $\hat{\varrho}_A^2 \neq \hat{\varrho}_A$ и

$$Sp \hat{\varrho}_A^2 = \sum_n p_n^2 < \sum_n p_n = 1. \quad (3.23)$$

Принято говорить, что $\hat{\varrho}_A$ есть некогерентная суперпозиция состояний $|n\rangle$. При этом некогерентность означает, что относительные фазы набора состояний $|n\rangle$ экспериментально неизвестны.

В базисе состояний, в котором $\hat{\varrho}_A$ диагональна, среднее значение любой наблюдаемой \hat{F} может быть определено соотношением

$$\langle \hat{F} \rangle = Sp (\hat{F} \cdot \hat{\varrho}) = \sum_n p_n \langle n | \hat{F} | n \rangle. \quad (3.24)$$

Таким образом, как и прежде, можно интерпретировать оператор $\hat{\varrho}$ как описание ансамбля чистых квантовых состояний, в которых состояние $|n\rangle$ присутствует с вероятностью p_n .

В общем случае состояния A и B подсистем целой системы коррелированы и называются *запутанными* (entangled) состояниями.

В квантовой теории для характеристики вероятности перехода между состояниями системы $|\psi_1\rangle$ и $|\psi_2\rangle$ определяется величина $\langle \psi_1 | \psi_2 \rangle$, которая характеризует амплитуду вероятности перехода между этими состояниями. Соответственно, вероятность перехода ω в этом случае равна

$$\omega(\psi_1 \rightarrow \psi_2) = |\langle \psi_1 | \psi_2 \rangle|^2.$$

Для чистых состояний данное выражение можно переписать с использованием определения матрицы плотности:

$$\begin{aligned}\omega(\psi_1 \rightarrow \psi_2) &= \langle \psi_1 | \psi_2 \rangle \langle \psi_1 | \psi_2 \rangle^* = \langle \psi_1 | (|\psi_2\rangle \langle \psi_2|) | \psi_1 \rangle = \\ &= Sp(|\psi_2\rangle \langle \psi_2| |\psi_1\rangle \langle \psi_1|).\end{aligned}$$

Другими словами, для вероятности перехода имеем

$$\omega(\psi_1 \rightarrow \psi_2) = Sp(\hat{\varrho}_{\psi_2} \hat{\varrho}_{\psi_1}). \quad (3.25)$$

Упражнение 3.1. Найти вид оператора матрицы плотности для кубита $|q\rangle = \alpha|0\rangle + \beta|1\rangle$.

Упражнение 3.2. Построить оператор матрицы плотности для пучка частиц, находящихся в двух чистых состояниях $|\psi_1\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $|\psi_2\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Вероятность состояния $|\psi_1\rangle$ в смеси равна $1/3$, а состояния $|\psi_2\rangle - 2/3$.

Упражнение 3.3. Определить вероятность перехода кубита из состояния $|\psi_1\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ в $|\psi_2\rangle = (|0\rangle + \sqrt{3}|1\rangle)/2$.

3.2 Эволюция оператора плотности

По определению оператор матрицы плотности зависит от времени. Эволюция оператора матрицы плотности с течением времени может быть получена путём дифференцирования по времени выражения (3.9). Для выполнения такого дифференцирования представим эволюцию зависящих от времени t состояний $|\Psi_n(t)\rangle$ с использованием определения оператора эволюции, а именно:

$$|\Psi_n(t)\rangle = \hat{U}(t)|\Psi_n(0)\rangle.$$

Здесь $|\Psi_n\rangle(0)$ – состояние системы в начальный момент времени $t = 0$. В результате оператор матрицы плотности можно записать в виде

$$\hat{\varrho}(t) = \sum_n \omega_n \hat{U}(t) |\Psi_n(0)\rangle \langle \Psi_n(0)| \hat{U}^\dagger(t) \quad (3.26)$$

или эквивалентно следующим образом:

$$\hat{\varrho}(t) = \hat{U}(t) \left(\sum_n \omega_n |\Psi_n(0)\rangle \langle \Psi_n(0)| \right) \hat{U}^\dagger(t) = \hat{U}(t) \varrho(0) \hat{U}^\dagger(t). \quad (3.27)$$

Если оператор Гамильтона \hat{H} системы не зависит от времени, то с учётом равенства (1.61) выражение (3.27) может быть представлено в виде

$$\hat{\varrho}(t) = \exp\left(-\frac{i}{\hbar} \hat{H} t\right) \hat{\varrho}(0) \exp\left(\frac{i}{\hbar} \hat{H} t\right), \quad (3.28)$$

из которого следует уравнение

$$i\hbar \frac{\partial \hat{\varrho}}{\partial t} = [\hat{H}, \hat{\varrho}]. \quad (3.29)$$

Данное уравнение часто называют уравнением Лиувилля, так как оно имеет вид, совпадающий с уравнением движения в фазовом пространстве для функции распределения вероятности в классической механике. Операторное уравнение (3.29) в произвольном дискретном базисе $|n\rangle$ является системой дифференциальных уравнений вида

$$i\hbar \frac{\partial \varrho_{nm}}{\partial t} = \sum_k (H_{nk}\varrho_{km} - \varrho_{nk}H_{km}). \quad (3.30)$$

Число уравнений системы определяется размерностью базиса.

Если базис состояний является собственным базисом гамильтониана с определённой энергией E_n , то матричные элементы оператора плотности можно представить в виде

$$\varrho_{nm}(t) = \varrho_{nm}(0) \exp\left(i\frac{E_m - E_n}{\hbar}t\right). \quad (3.31)$$

Данное соотношение показывает, что диагональные матричные элементы матрицы плотности от времени не зависят, а недиагональные осциллируют с частотой, равной $\omega_{mn} = (E_m - E_n)/\hbar$. В этом случае среднее значение произвольной величины F представляется выражением

$$\langle \hat{F} \rangle = \sum_{nm} \langle n | \hat{F} | m \rangle \varrho_{mn}(0) \exp(i\omega_{mn}t). \quad (3.32)$$

Для составной системы эволюция оператора плотности легко определяется в случае, когда две подсистемы A и B не связаны друг с другом. Гамильтониан в этом случае имеет вид

$$\hat{H}_{AB} = \hat{H}_A \otimes \hat{I}_B + \hat{I}_A \otimes \hat{H}_B, \quad (3.33)$$

где \hat{H}_A и \hat{H}_B – операторы, действующие в пространстве векторов состояний A и B соответственно.

Оператор эволюции для объединённой системы в этом случае есть прямое произведение операторов эволюции векторов состояний систем A и B :

$$\hat{U}_{AB}(t) = U_A(t) \otimes U_B(t). \quad (3.34)$$

Вектор состояния объединённой системы в произвольный момент времени может быть представлен в виде

$$|\Psi(t)\rangle_{AB} = \sum_{n,m} a_{nm} |n(t)\rangle_A \otimes |m(t)\rangle_B, \quad (3.35)$$

где векторы состояний

$$|n(t)\rangle_A = U_A(t) |n(0)\rangle_A, \quad |m(t)\rangle_B = U_B(t) |m(0)\rangle_B \quad (3.36)$$

определяют новый ортогональный базис, так как $U_A(t)$ и $U_B(t)$ – унитарные операторы. Таким образом, оператор матрицы плотности подсистемы A есть

$$\hat{\varrho}_A(t) = \sum_{n,m,k} a_{nm} a_{km}^* |n(t)\rangle_A \langle m(t)|_A = U_A(t) \varrho_A(0) U_A^\dagger(t). \quad (3.37)$$

В частном случае в базисе состояний, в котором $\hat{\varrho}_A(0)$ диагональна, получим

$$\hat{\varrho}_A(t) = \sum_n p_n U_A(t) |n(0)\rangle_A \langle n(0)|_A U_A^\dagger(t). \quad (3.38)$$

Уравнение (3.38) справедливо только при выполнении условия (3.33).

3.3 Вектор поляризации. Спиновая матрица плотности

В качестве примера ниже рассмотрено применение матрицы плотности при прохождении частиц через фильтр Штерна – Герлаха.

Известно, что для описания чистых спиновых состояний может быть введён *вектор поляризации* \vec{P} , компоненты которого определяются как средние значения матриц Паули:

$$P_i \equiv \langle \sigma_i \rangle; \quad i = x, y, z \text{ или } 1, 2, 3. \quad (3.39)$$

В σ_x -представлении с учётом явного вида матриц Паули получим для пучка частиц, находящихся в чистом состоянии $|0\rangle$, следующие значения проекций вектора поляризации:

$$P_x = \langle 0 | \sigma_x | 0 \rangle = (1, 0) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 0; \quad (3.40)$$

$$P_y = \langle 0 | \sigma_y | 0 \rangle = (1, 0) \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 0;$$

$$P_z = \langle 0 | \sigma_z | 0 \rangle = (1, 0) \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1.$$

Аналогично для частиц, находящихся в чистом состоянии $|1\rangle$, проекции вектора поляризации имеют вид

$$P_x = \langle 1 | \sigma_x | 1 \rangle = 0; \quad P_y = \langle 1 | \sigma_y | 1 \rangle = 0; \quad P_z = \langle 1 | \sigma_z | 1 \rangle = -1. \quad (3.41)$$

В рассмотренных случаях векторы поляризации имеют единичную длину, но направлены противоположно.

Рассмотрим далее чистое нормированное однокубитовое состояние, являющееся суперпозицией состояний $|0\rangle$ и $|1\rangle$:

$$|\Psi\rangle = a_1|0\rangle + a_2|1\rangle \equiv \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle = \begin{pmatrix} \cos(\theta/2) \\ e^{i\phi}\sin(\theta/2) \end{pmatrix}. \quad (3.42)$$

В этом случае для компонент вектора поляризации получим следующие выражения:

$$\begin{aligned} P_x &= \langle\Psi|\sigma_x|\Psi\rangle = \sin\theta\cos\phi, \\ P_y &= \langle\Psi|\sigma_y|\Psi\rangle = \sin\theta\sin\phi, \\ P_z &= \langle\Psi|\sigma_z|\Psi\rangle = \cos\theta. \end{aligned} \quad (3.43)$$

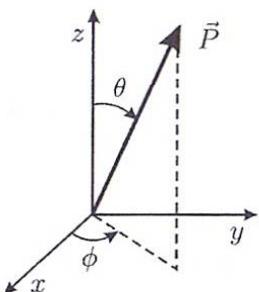


Рис. 3.2. Направление вектора поляризации с использованием переменных сферической системы координат

Вектор поляризации, компоненты которого определяются выражениями (3.43), также имеет единичную длину, а параметры θ и ϕ являются углами сферической системы координат, определяющими направление вектора \vec{P} (рис. 3.2). Если выбрать новую систему координат (x', y', z') так, чтобы ось z' была параллельна \vec{P} , то в новой системе координат проекции вектора поляризации равны: $P_{x'} = 0$, $P_{y'} = 0$, $P_{z'} = 1$. По определению, если направить пучок через фильтр Штерна – Герлаха, расположенный параллельно вектору \vec{P} , то весь пучок пройдёт через фильтр полностью.

Рассмотрим теперь вектор поляризации пучка спинов, приготовленного из двух пучков независимо друг от друга, в которых n_1 частиц находится в состоянии $|0\rangle$, а n_2 в состоянии $|1\rangle$. В соответствии с (3.24)

$$P_i = \langle\sigma_i\rangle = Sp(\hat{F}\hat{\varrho}) = p_1\langle 0|\sigma_i|0\rangle + p_2\langle 1|\sigma_i|1\rangle, \quad (3.44)$$

где $p_1 = n_1/n$, $p_2 = n_2/n$, $n = n_1 + n_2$. Вычисления P_i по формуле (3.44) приводят к следующему результату:

$$P_x = 0, \quad P_y = 0, \quad P_z = p_1 - p_2 = (n_1 - n_2)/n. \quad (3.45)$$

Как видно, длина вектора поляризации в данном случае меньше единицы и пропорциональна разности числа спинов в состояниях $|0\rangle$ и $|1\rangle$.

В общем случае, когда пучок приготовлен путём смешивания n_A частиц в чистом состоянии $|\Psi_A\rangle$ и n_B частиц в чистом состоянии $|\Psi_B\rangle$, компоненты

вектора поляризации равны:

$$\begin{aligned} P_i &= p_A \langle \Psi_A | \sigma_i | \Psi_A \rangle + p_B \langle \Psi_B | \sigma_i | \Psi_B \rangle = \\ &= p_A P_i^A + p_B P_i^B, \quad i = 1, 2, 3. \end{aligned} \quad (3.46)$$

Здесь $p_A = n_A/n$; $p_B = n_B/n$; $n = n_A + n_B$, а $P_i^A = \langle \Psi_A | \sigma_i | \Psi_A \rangle$ и $P_i^B = \langle \Psi_B | \sigma_i | \Psi_B \rangle$. Соотношение (3.46) можно переписать в векторном виде:

$$\vec{P} = p_A \vec{P}^A + p_B \vec{P}^B, \quad (3.47)$$

при этом $|\vec{P}^A| = |\vec{P}^B| = 1$. Модуль вектора \vec{P} в (3.47) определяется соотношением

$$\begin{aligned} |\vec{P}| &= \sqrt{\vec{P}^2} = \sqrt{p_A^2 + 2p_A p_B (\vec{P}^A \cdot \vec{P}^B) + p_B^2} \leqslant \\ &\leqslant \sqrt{p_A^2 + 2p_A p_B + p_B^2} = \sqrt{(p_A + p_B)^2} = \sqrt{1} = 1. \end{aligned} \quad (3.48)$$

Таким образом, длина вектора поляризации системы частиц, находящихся в смешанном состоянии, удовлетворяет условию

$$0 \leq |\vec{P}| \leq 1. \quad (3.49)$$

При этом максимально возможное значение $|\vec{P}| = 1$ достигается, только когда пучок находится в чистом состоянии, а для смешанных состояний $|\vec{P}| < 1$.

Спиновая матрица плотности является двумерной эрмитовской матрицей, которую можно представить в виде линейной комбинации единичной 2×2 матрицы и матриц Паули σ_i :

$$\hat{\varrho} = aI + \sum_{k=1}^3 b_k \sigma_k. \quad (3.50)$$

В этом выражении коэффициенты a, b_1, b_2, b_3 подлежат определению. Учитывая, что $Sp \varrho = 1$, получим $a = 1/2$. Умножая (3.50) на σ_i и вычисляя $Sp(\hat{\varrho}\sigma_i)$, получим:

$$\begin{aligned} Sp(\hat{\varrho}\sigma_i) &\equiv \langle \sigma_i \rangle \equiv P_i = \sum_{k=1}^3 b_k Sp(\sigma_i \sigma_k) = \\ &= \sum_{k=1}^3 b_k \cdot 2\delta_{ik} = 2b_i, \quad i = 1, 2, 3, \end{aligned} \quad (3.51)$$

так как с учётом свойств матриц Паули $Sp(\sigma_i \sigma_k) = 2\delta_{ik}$. Таким образом, $b_i = P_i/2$. В результате вид спиновой матрицы плотности можно представить в виде

$$\varrho = \frac{1}{2} (I + \vec{\sigma} \cdot \vec{P}) = \frac{1}{2} \begin{pmatrix} 1 + P_z & P_x - iP_y \\ P_x + iP_y & 1 - P_z \end{pmatrix}. \quad (3.52)$$

Исходя из полученного выражения, следует, что определитель спиновой матрицы плотности равен $\det \varrho = (1 - P^2)/4$. Таким образом, условие положительности собственных значений ϱ есть $\det \varrho \geq 0$ или $P^2 \leq 1$.

В случае чистого состояния $|A\rangle$ оператор матрицы плотности есть оператор проектирования $\varrho_A = |A\rangle \langle A|$. Введём вектор поляризации состояния $|A\rangle$ и обозначим его через $\vec{P}^{(A)}$. На основании (3.52) находим

$$\varrho_A = |A\rangle \langle A| \equiv \frac{1}{2} \left(1 + \vec{\sigma} \cdot \vec{P}^{(A)} \right). \quad (3.53)$$

В результате вычисление среднего значения в состоянии $|A\rangle$ можно переписать в виде

$$\begin{aligned} \langle A | \hat{\varrho} | A \rangle &= Sp(|A\rangle \langle A| \hat{\varrho}) = \\ &= \frac{1}{4} Sp \left[(1 + \vec{\sigma} \cdot \vec{P}^{(A)}) (1 + \vec{\sigma} \cdot \vec{P}) \right] = \\ &= \frac{1}{2} (1 + \vec{P}^{(A)} \cdot \vec{P}). \end{aligned} \quad (3.54)$$

Здесь учтено, что $(\vec{\sigma} \cdot \vec{A})(\vec{\sigma} \cdot \vec{B}) = (\vec{A} \cdot \vec{B}) + i\vec{\sigma}[\vec{A} \times \vec{B}]$, а также что след от матрицы Паули равен нулю. Приведённый в (3.54) результат можно интерпретировать следующим образом: если пучок частиц определяется матрицей плотности ϱ , то этот пучок может проходить через фильтр Штерна – Герлаха без потерь, лишь находясь в чистом состоянии $|A\rangle$. Другими словами, если фильтр ориентирован параллельно вектору $\vec{P}^{(A)}$, то вероятность того, что частица пучка пройдёт через фильтр, определяется скалярным произведением $\vec{P}^{(A)} \cdot \vec{P}$. Вероятность прохождения пучка максимальна, если \vec{P} ориентирован параллельно градиенту поля $\vec{P}^{(A)}$, и минимальна в случае его антипараллельной ориентации. В частности, если пучок не поляризован ($\vec{P} = 0$), то для любого фильтра

$$\langle A | \hat{\varrho} | A \rangle = 1/2. \quad (3.55)$$

В соответствии с (3.52) P_x, P_y, P_z представляют собой минимальный набор данных, который необходим для определения матрицы плотности спина 1/2. Таким образом, информацией о пучке является задание трёх

компонент вектора \vec{P} . Если вектор \vec{P} известен, то (3.52) содержит всю информацию о пучке.

Если $|\vec{P}| = 1$, то система (пучок) находится в чистом спиновом состоянии. В этом случае достаточно двух параметров для описания системы (например, углы θ и ϕ вектора \vec{P}). Если $|\vec{P}| < 1$, то пучок находится в смешанном состоянии. Такие состояния характеризуются тремя параметрами ($|\vec{P}|, \theta, \phi$).

Упражнение 3.4. Найти вероятность того, что частица, находящаяся в чистом состоянии $|q\rangle = (\sqrt{3}|0\rangle + |1\rangle)/2$ пройдёт через фильтр Штерна – Герлаха, ориентированный под углом 30° .

Упражнение 3.5. На пути пучка кубит в состоянии $|q\rangle = \alpha|0\rangle + \beta|1\rangle$ установлены два фильтра Штерна – Герлаха, ориентированные под углом 0° и 90° соответственно. Какова вероятность прохождения исходного пучка через эти два фильтра?

3.4 Теорема Шмидта

Теорема. Если $|\Psi\rangle$ – вектор состояния составной системы $A + B$ в пространстве $H_A \otimes H_B$, то существуют ортонормированный базис $|n_A\rangle$ для системы A и ортонормированный базис $|n_B\rangle$ для системы B , а также неотрицательные действительные числа λ_n такие, что

$$|\Psi_{AB}\rangle = \sum_n \sqrt{\lambda_n} |n_A\rangle |n_B\rangle; \quad \sum_n \lambda_n = 1. \quad (3.56)$$

Числа λ_n называются коэффициентами Шмидта.

Для демонстрации теоремы рассмотрим случай, когда состояния $|n_A\rangle$ и $|n_B\rangle$ принадлежат пространству одной размерности [11]. Пусть $|j\rangle$ и $|k\rangle$ образуют произвольный ортонормированный базис для систем A и B соответственно. Тогда состояние составной системы $|\Psi_{AB}\rangle$ может быть представлено в виде

$$|\Psi_{AB}\rangle = \sum_{j,k} a_{jk} |j\rangle |k\rangle, \quad a_{jk} = \langle jk | \Psi_{AB} \rangle. \quad (3.57)$$

Набор чисел a_{jk} образует эрмитово-сопряжённую комплексную матрицу a . Из линейной алгебры известно, что такую матрицу можно привести к диагональному виду. Представим матрицу a в виде $a = u \cdot d \cdot v$, где d – диагональная матрица с неотрицательными элементами, u и v – унитарные

матрицы, т. е. $d = u^{-1} \cdot a \cdot v^{-1}$. Тогда (3.57) можно переписать в виде

$$|\Psi_{AB}\rangle = \sum_{i,j,k} u_{ji} d_{ii} v_{ik} |j\rangle |k\rangle. \quad (3.58)$$

Определим новые базисные состояния для A и B и обозначим их $|i_A\rangle$ и $|i_B\rangle$ соответственно:

$$|i_A\rangle = \sum_j u_{ji} |j\rangle \quad \text{и} \quad |i_B\rangle = \sum_k v_{ik} |k\rangle, \quad (3.59)$$

а $d_{ii} = \sqrt{\lambda_i}$. В результате из (3.58) находим

$$|\Psi_{AB}\rangle = \sum_i \sqrt{\lambda_i} |i_A\rangle |i_B\rangle. \quad (3.60)$$

В силу унитарности матриц u и v наборы состояний $|i_A\rangle$ и $|i_B\rangle$ в (3.59) образуют полную ортонормированную систему, или базис Шмидта. Это и определяет содержание теоремы (3.56).

Число ненулевых значений λ_i в (3.60) или (3.56) называется числом Шмидта для состояния $|\Psi_{AB}\rangle$. Это число характеризует степень запутанности состояний сложной системы.

Можно отметить, что если представить двухкомпонентный вектор в базисе Шмидта, то вычисление оператора плотности подсистемы (вычисление частичного следа) значительно упрощается. Например, для системы $A \otimes B$ в состоянии (3.60) матрица плотности определяется соотношением

$$|\Psi_{AB}\rangle \langle \Psi_{AB}| = \sum_{i,j} \sqrt{\lambda_i} \sqrt{\lambda_j} |i_A\rangle \langle j_A| |i_B\rangle \langle j_B|. \quad (3.61)$$

На основании данного выражения оператор плотности подсистемы A равен

$$\begin{aligned} \hat{\varrho}_A &= Sp_B |\Psi_{AB}\rangle \langle \Psi_{AB}| = \sum_{i,j} \sqrt{\lambda_i} \sqrt{\lambda_j} Sp_B |i_A\rangle \langle j_A| |i_B\rangle \langle j_B| = \\ &= \sum_{i,j} \sqrt{\lambda_i} \sqrt{\lambda_j} |i_A\rangle \langle j_A| \langle i_B| j_B\rangle = \sum_i \lambda_i |i_A\rangle \langle i_A|, \end{aligned} \quad (3.62)$$

так как $\langle i_B| j_B\rangle = \delta_{ij}$. Аналогично

$$\hat{\varrho}_B = Sp_A |\Psi_{AB}\rangle \langle \Psi_{AB}| = \sum_i \lambda_i |i_B\rangle \langle i_B|. \quad (3.63)$$

Как видно из приведённого обсуждения, в базисе Шмидта оба редуцированных оператора плотности диагонализованы, а их спектры одинаковы. Данное обстоятельство позволяет выполнить разложение Шмидта.

Пример 3.1. Разложение Шмидта для заданного двухкубитового состояния

Пусть задано двухкубитовое состояние вида

$$|\psi\rangle = \alpha_- |00\rangle + \beta_+ |01\rangle + \alpha_+ |10\rangle + \beta_- |11\rangle, \quad (3.64)$$

где коэффициенты α_{\pm} и β_{\pm} равны

$$\alpha_{\pm} = \frac{\sqrt{3} \pm \sqrt{2}}{2\sqrt{6}}; \quad \beta_{\pm} = \frac{\sqrt{6} \pm 1}{2\sqrt{6}}.$$

Из (3.64) находим редуцированный оператор плотности:

$$\hat{\varrho}_1 = Sp_2(|\psi\rangle\langle\psi|) = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{4}|0\rangle\langle 1| + \frac{1}{4}|1\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 0|.$$

В матричном виде данную матрицу можно представить следующим образом:

$$\hat{\varrho}_1 \rightarrow \begin{pmatrix} 1/2 & 1/4 \\ 1/4 & 1/2 \end{pmatrix}. \quad (3.65)$$

Собственные значения и собственные векторы редуцированной матрицы плотности (3.65) определяются из уравнений

$$\begin{pmatrix} 1/2 - \lambda & 1/4 \\ 1/4 & 1/2 - \lambda \end{pmatrix} = 0; \quad \begin{pmatrix} 1/2 & 1/4 \\ 1/4 & 1/2 \end{pmatrix} \begin{pmatrix} a_k \\ b_k \end{pmatrix} = \lambda_k \begin{pmatrix} a_k \\ b_k \end{pmatrix}, \quad (3.66)$$

при этом собственные числа равны $\lambda_1 = \frac{1}{4}$, $\lambda_2 = \frac{3}{4}$, а нормированные собственные векторы имеют вид

$$\begin{pmatrix} a_1 \\ b_1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \rightarrow |q_-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}; \quad (3.67)$$

$$\begin{pmatrix} a_2 \\ b_2 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \rightarrow |q_+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}.$$

Найденные собственные векторы являются векторами в базисе Шмидта для первой подсистемы. Базис Шмидта для второй подсистемы очевидным образом образуется после определения базиса первой подсистемы. В результате разложение Шмидта в данном примере есть

$$|\psi\rangle = \frac{\sqrt{3}}{2} |q_+\rangle \left(\frac{|0\rangle + \sqrt{2}|1\rangle}{\sqrt{3}} \right) + \frac{1}{2} |q_-\rangle \left(\frac{-\sqrt{2}|0\rangle + |1\rangle}{\sqrt{3}} \right). \quad (3.68)$$

Упражнение 3.6. Найти разложение Шмидта для двухкубитового состояния

$$|\psi\rangle = \frac{1}{\sqrt{2+2a^2}} (|00\rangle + a|01\rangle + a|10\rangle + |11\rangle); \quad |a| \leq 1.$$

Упражнение 3.7. Найти разложение Шмидта для двухкубитового состояния

$$|\psi\rangle = \frac{1}{\sqrt{14}} (|00\rangle + 2|10\rangle - 3|11\rangle).$$

Упражнение 3.8. Найти разложение Шмидта для состояния

$$|\psi\rangle = \frac{1}{\sqrt{5\sqrt{2}}} (5|00\rangle + 3|10\rangle - 4|11\rangle).$$

Упражнение 3.9. На примере состояния

$$|\psi\rangle = \frac{1}{\sqrt{3\sqrt{2}}} (|100\rangle + |010\rangle + |001\rangle)$$

показать, что для трёх кубит не существует разложения Шмидта, т. е.

$$|\psi\rangle \neq \lambda_1 |000\rangle + \lambda_2 |111\rangle.$$

Часть II

Классические вычисления

Глава 4

Компьютерные технологии

Классические компьютерные технологии основаны на цифровом представлении информации. При этом алфавит представления информации состоит из двух цифр двоичной системы счисления: 0 и 1. Двоичная единица информации называется битом (от английских слов binary digit двоичная цифра). С помощью набора значений бит можно представить любой знак и любое число, а также все без исключения виды информации: текст, графика, звук, видео. Для математического описания процессов обработки и преобразования двоичной (бинарной) информации в современных информационных системах применяется логическая система, введённая Джорджем Булем. Физический принцип обработки результатов в цифровых устройствах основан на управлении электронными переключателями в кристалле большой интегральной схемы, которые выполняют операции с предсказуемыми результатами. Совокупность переключателей образует "вентиль" ("гейт") или оператор, выполняющий заданное преобразование. Последовательность различных комбинаций вентилей формирует цепь преобразования исходных данных (или информации) и даёт возможность, например компьютеру, решать задачи с помощью закодированных импульсов двоичного языка. На вход каждого логического вентиля поступает электрический сигнал одного из двух уровней напряжения V_1 , V_2 , которые вентиль интерпретирует в зависимости от своей функции и выдаёт выходной сигнал, также совпадающий с одним из уровней V_1 , V_2 . Эти уровни соответствуют одному из состояний двоичной системы.

В 1938 г. Клод Шенон установил связь между двоичными числами, булевой алгеброй и электрическими схемами. Идеи Шенона считаются поворотным пунктом в истории развития классической информатики и классической вычислительной техники. Шенон показал, что если построить электрические цепи информационной системы в соответствии с принципами булевой алгебры, то они могут выражать логические отношения, опре-

делять истинность утверждений, а также выполнять сложные вычисления. По этой причине для справки ниже приведены основные понятия алгебры логики. Алгебра логики возникла в середине XIX в. в работах Дж. Булья и была развита Ч. Пирсом (C. S. Peirs), П. С. Порецким, Б. Расселом (B. Russel), Д. Гильбертом (D. Hilbert) и др.

4.1 Основные понятия алгебры логики

Алгебра логики – это раздел математической логики, изучающий *высказывания*, рассматриваемые со стороны их логических значений (истина или ложь), а также логические операции над высказываниями.

Высказыванием называются предложения, которые могут быть охарактеризованы понятиями “истина” или “ложь”.

В математическом аппарате алгебры логики из заданных высказываний можно строить более сложные высказывания с использованием группы *логических связок* “и”, “или”, “если..., то”, “эквивалентно” и т. д. Истинность или ложность сложных высказываний зависит от истинности или ложности исходных высказываний.

Для обозначения истинности высказывания вводятся символы, которые могут использоваться равноправно:

$$\text{Истина} \equiv \text{И} \equiv \text{True} \equiv \text{T} \equiv 1. \quad (4.1)$$

Соответственно, для обозначения ложности высказывания вводятся следующие символы:

$$\text{Ложь} \equiv \text{Л} \equiv \text{False} \equiv \text{F} \equiv 0. \quad (4.2)$$

Для обозначения логических связок приняты следующие их наименования и равноправные обозначения:

$$\left. \begin{array}{l} \text{“и” (конъюнкция)} \equiv \& \equiv \wedge \equiv \text{AND} \equiv \cap \\ \text{“или” (дизъюнкция)} \equiv \vee \equiv \text{OR} \\ \text{“если..., то” (импликация)} \equiv \rightarrow \\ \text{“эквивалентность”} \equiv \sim \\ \text{“отрицание”} \equiv \text{черта над высказыванием} \equiv \neg \equiv \text{NOT} \end{array} \right\} \quad (4.3)$$

Связки рассматриваются в алгебре логики как операции над величинами, принимающими два значения: 0 (ложь) и 1 (истина), а высказывания с произвольными высказываниями и связками образуют формулы. При этом высказывания, образующие формулу, рассматриваются в качестве

переменных, а связки — в качестве функций. Формулы A и B называются равными $A = B$, если они реализуют равные функции.

Для задания функций алгебры логики используются таблицы, содержащие все наборы значений переменных и значений функций. Такие таблицы называются *таблицами истинности*. Пример таблиц истинности для логических связок NOT, AND, OR, импликации и эквивалентности приведён ниже.

a	b	NOT a	$a \wedge b$	$a \vee b$	$a \rightarrow b$	$a \sim b$
0	0	1	0	0	1	1
0	1	1	0	1	1	0
1	0	0	0	1	0	0
1	1	0	1	1	1	1

Сложные формулы в алгебре логики могут быть преобразованы. Для преобразования формул основную роль играют законы, установленные в алгебре логики (где $a, b, c \in \{0, 1\}$):

— закон коммутативности:

$$a \vee b = b \vee a; \quad a \wedge b = b \wedge a; \quad (4.4)$$

— закон ассоциативности:

$$(a \wedge b) \wedge c = a \wedge (b \wedge c); \quad (a \vee b) \vee c = a \vee (b \vee c); \quad (4.5)$$

— закон поглощения:

$$a \wedge (a \vee b) = a; \quad a \vee (a \wedge b) = a; \quad (4.6)$$

— закон дистрибутивности:

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c); \quad a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c); \quad (4.7)$$

— закон противоречия:

$$a \wedge \bar{a} = 0; \quad (4.8)$$

— закон исключения третьего:

$$a \vee \bar{a} = 1; \quad (4.9)$$

$$a \rightarrow b = \bar{a} \vee b; \quad a \sim b = (a \wedge b) \vee (\bar{a} \wedge \bar{b}). \quad (4.10)$$

Множество формул, в построении которых участвуют переменные высказывания (в форме значений 0 и 1) и логические связки \wedge , \vee , \rightarrow , \sim , \neg , называются языком над данными символами. Равенства (4.4) – (4.10) означают, что для всякой формулы в языке над символами \wedge , \vee , \rightarrow , \sim , \neg , 0, 1 найдётся равная ей формула в языке над символами \wedge , \vee , \neg , 0, 1.

Алгебра логики развивалась под влиянием прикладных задач, среди которых приложение к теории электрических схем имеет, возможно, самое важное значение. В общем случае в алгебре логики ставится задача минимизации логического выражения или функции, когда заданная функция приводится к функции, имеющей наименьшее число сомножителей, т. е. минимальную сложность. Такие функции называются минимальными.

Упражнение 4.1. Доказать равенства (4.4) – (4.10).

Упражнение 4.2. В языке над символами \wedge , \vee , \rightarrow , \sim , 0, 1, \oplus , где \oplus обозначает сложение по модулю два, проверить выполнение равенств (4.11) – (4.13):

$$a \vee b = ((a \wedge b) \oplus a) \oplus b; \quad (4.11)$$

$$a \rightarrow b = \bar{a} \wedge b; \quad a \sim b = (a \oplus b) \oplus 1; \quad (4.12)$$

$$a \oplus b = (a \wedge b) \vee (\bar{a} \wedge \bar{b}). \quad (4.13)$$

4.2 Классические логические гейты

Универсальный компьютер – это логическое устройство, реализованное в виде сложной сети взаимосвязанных примитивных элементов. Для классического компьютера можно представить, что связь элементов осуществляется идеальными проводниками, передающими одно из двух стандартных напряжений, представляющих один бит информации 1 или 0. Сами примитивные элементы, или *гейты* (*вентили, операторы*), реализуют функции преобразования, использующиеся в алгебре логики.

Классический компьютер осуществляет вычисление функций по заданным входным n -битам, располагая результат вычисления в m -битах ответа. Функция со значениями m -бит эквивалентна m -функциям, каждая из которых имеет однобитовое значение в качестве результата. Вычисление каждой из этих функций может быть сведено к последовательности элементарных логических операций.

Схематически гейты, соединённые “проводами”, изображаются схемами с указанием бит. Такие схемы называются логическими диаграммами или цепями. Так, на рис. 4.1 представлена схема (логическая диаграмма)

для примитивного элемента цепи, изображённая в трёх тождественных вариантах, в которых над битом "a" выполняется логическая операция отрицания NOT.

$$a \xrightarrow{\text{NOT}} a' \equiv a \longrightarrow \bar{a} \equiv a \cdot \boxed{\text{NOT}} \cdot \bar{a}$$

Рис. 4.1. Логические цепи для обозначения оператора отрицания

На рисунке указано, что бит a проходит через гейт NOT, который изменяет данный бит, превращая 1 в 0 или 0 в 1. Линии до и после гейта NOT служат для указания переноса бита к данному гейту и последующего его переноса после преобразования соответственно. В общем случае линии (проводы) могут представлять как перенос бита из одной точки пространства в другую, так и развитие состояния бита во времени. По определению гейт NOT имеет один входной бит и один бит на выходе. Фактически гейт вычисляет выходной бит в соответствии с функцией $f(a) = 1 \oplus a$, где a принимает битовое значение. В вычислительных устройствах при построении цепи из множества вентилей предполагается, что цепь не содержит замкнутых петель.

В конкретных приложениях используются ряд элементарных логических вентилей, полезных для организации процесса вычисления, имеющих два бита в качестве исходных данных и один результирующий бит. Схематические изображения, алгебраические формулы в бинарной арифметике и таблицы истинности наиболее распространённых из них приведены ниже:

а) AND-гейт



$$c \equiv a \wedge b = a \cdot b$$

a	b	c
0	0	0
0	1	0
1	0	0
1	1	1

б) OR-гейт



$$c \equiv a \vee b = a \oplus b - a \cdot b$$

a	b	c
0	0	0
0	1	1
1	0	1
1	1	1

в) **XOR**-гейт : исключающее или \equiv “или”, но не оба



$$c \equiv a \text{ XOR } b = a(1 - b) \oplus b(1 - a)$$

a	b	c
0	0	0
0	1	1
1	0	1
1	1	0

г) **NAND**-гейт \equiv NOT AND-гейт



$$c \equiv a \text{ NAND } b = \overline{a \cdot b}$$

$$c = 1 - a \cdot b$$

a	b	c
0	0	1
0	1	1
1	0	1
1	1	0

д) **NOR**-гейт \equiv NOT OR-гейт



$$c \equiv a \text{ NOR } b = \overline{a + b}$$

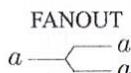
$$c = (1 - a)(1 - b)$$

a	b	c
0	0	1
0	1	0
1	0	0
1	1	0

Следует подчеркнуть, что рассмотренные выше логические гейты, кроме гейта отрицания, выполняют так называемые необратимые операции. Это означает, что однозначно восстановить исходное значение входных данных по их выходному битовому значению невозможно.

Любое вычисление может быть записано в терминах булевского выражения, и любое булевское выражение может быть построено из фиксированного набора логических операторов. Например, набор операторов AND, OR и NOT называется *универсальным*. В действительности можно обойтись только двумя гейтами, такими как AND и NOT, или OR и NOT, или AND и XOR. Устройство, которое может исполнить произвольные комбинации логических операторов из универсального набора, является универсальным компьютером.

Хотя приведённые выше гейты достаточны для математического аппарата алгебры логики, они недостаточны для реализации практической вычислительной машины. В реальном устройстве требуются ещё два гейта: FANOUT (разворачивание) и ERASE (стирание) (рис. 4.2).



FANOUT

$a \longrightarrow a$

ERASE

$a \longrightarrow x$

Рис. 4.2. Изображение операторов FANOUT и ERASE

FANOUT-гейт дублирует входной бит, а гейт ERASE уничтожает входной бит. По сути, FANOUT необходим для организации вычислений, а ERASE для очистки ячеек памяти компьютера. В некоторых приложениях используется, помимо того, гейт EXCHANGE (обмен), схематическое изображение которого и таблица истинности имеют следующий вид:

	a	b	a'	b'
EXCHANGE	0	0	0	0
	a	\times	a'	
	b	\times	b'	
	0	1	1	0
	1	0	0	1
	1	1	1	1

Для примера использования введённой выше стандартной системы обозначений рассмотрим цепь логических операторов, которая суммирует два целых числа, имеющих длину n -бит. Важным структурным элементом для построения такой цепи является “ячейка”, получившая название “полусумматор” ($\text{half-adder} \equiv \text{HA}$). На вход полусумматора подаются два бита: x и y , а на выходе получается сумма $x \oplus y$ по модулю 2, а также бит, осуществляющий перенос (саггу) бита в более высокий разряд, если это необходимо. Состояние данного бита равно 1, если и $x = 1$, и $y = 1$, и равно 0 во всех остальных случаях. Перенос бита позволяет перейти на следующий разряд, если складываются две бинарные единицы: $1 \oplus 1 = 10$.

Логическая диаграмма (схема) цепи полусумматора с использованием рассмотренных выше логических операторов может быть изображена в виде [9], представленном на рис. 4.3.

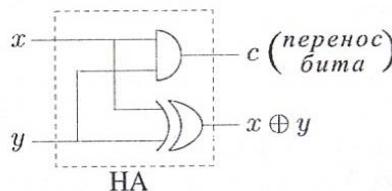


Рис. 4.3. Логическая диаграмма цепи полусумматора

Таблица истинности полусумматора для данной логической диаграммы имеет следующий вид:

x	y	перенос	$x \oplus y$	двоичное число
0	0	0	0	00
0	1	0	1	01
1	0	0	1	01
1	1	1	0	10

Каскад из двух полусумматоров (рис. 4.4) образует оператор, который получил наименование полного сумматора (full-adder \equiv FA) [9].

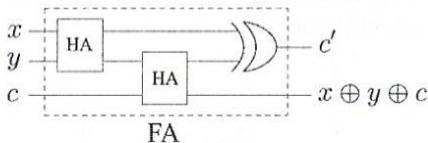


Рис. 4.4. Логическая диаграмма цепи полного сумматора

Полный сумматор имеет три бита на входе, где x, y — данные для сложения, c — перенос бита с предыдущего этапа вычислений и два бита на выходе. Один выходной бит является суммой по модулю 2 всех трёх входящих битов $x \oplus y \oplus c$, а второй выходной бит c' есть перенос бита, который равен 1, если два или больше входных бита равны 1, и равен 0 в противном случае. Изменение входных битовых значений в цепи полного сумматора представлено на рис. 4.5. Вертикальные стрелки на схеме цепи рисунка фиксируют позиции в цепи полного сумматора для определения битовых значений.

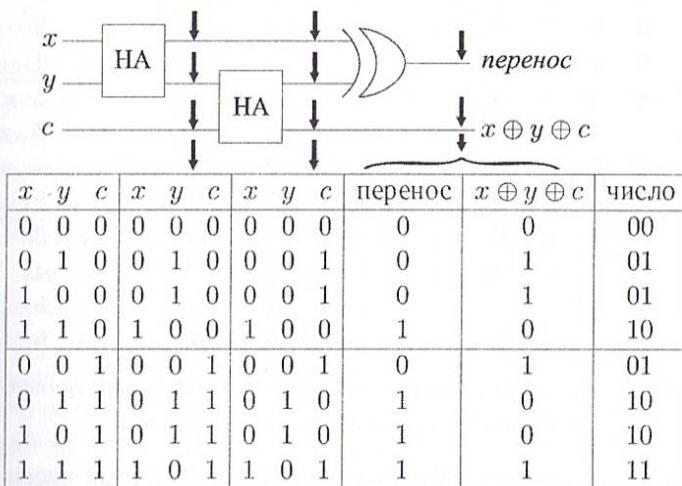


Рис. 4.5. Логическая диаграмма и таблица истинности полного сумматора

Представленная на рис. 4.5 логическая диаграмма определяет одноразрядный цифровой сумматор. Из таких одноразрядных сумматоров составляются многоразрядные сумматоры (обычно четырёхразрядные) последовательного и параллельного действия, которые позволяют проводить сложение n -битовых целых. Сумматоры последовательного действия обладают более низким быстродействием.

Например, каскад НА и FA сумматоров для сложения пары двухбитовых целых $(x_1x_0) + (y_1y_0)$ и таблица истинности представлены на рис. 4.6 (x_0, y_0 — младшие разряды двоичных чисел).

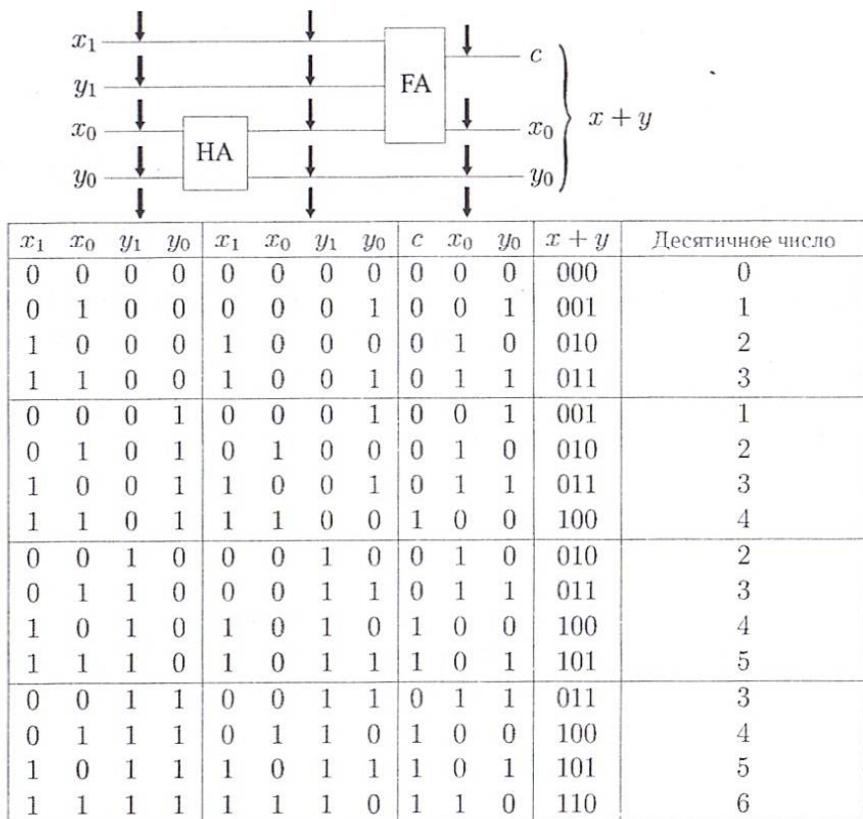


Рис. 4.6. Логическая диаграмма и таблица истинности каскада сумматоров для сложения двух двухбитовых целых чисел

Каскад, осуществляющий сложение двух трёхбитовых чисел $(x_2x_1x_0) + (y_2y_1y_0)$, приведён на рис. 4.7.

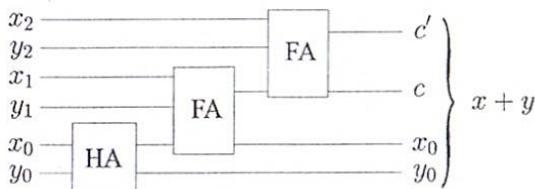


Рис. 4.7. Каскад сумматоров для сложения двух трёхбитовых чисел $x + y$

На рис. 4.7 два целых числа представлены в виде последовательности трёх бит вида $x \equiv (x_2x_1x_0)$ и $y \equiv (y_2y_1y_0)$, где $x_i, y_i, i \in 0, 1, 2$ – битовые значения в соответствующем разряде. Соответственно, x_0, y_0 представляют младшие разряды чисел.

Аналогично может быть построена цепь вычисления произвольной логической функции.

Физическая реализация логических операторов в классическом компьютере осуществляется системой электрических цепей, состоящих из сопротивлений и транзисторов. Например, на рис. 4.8 приведены электрические схемы, реализующие такие операторы, как NOT и NAND.

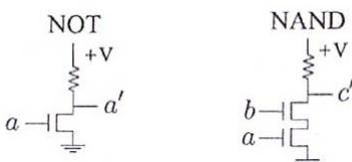


Рис. 4.8. Электрические схемы операторов NOT и NAND

Как отмечалось выше, в реальном компьютере битовые значения 0, 1 представляются двумя различными значениями напряжений (низкое, например, меньше 3 вольт и высокое, например, больше 5 вольт). Напряжение в электрической цепи – это разность потенциалов. В электрической схеме всегда есть один общий проводник, который считается заземленным и потенциал которого условно выбирается равным нулю. По этой причине в электрической цепи из множества элементов используется понятие “потенциал” для определения напряжения в конкретной точке цепи относительно заземленного (общего) проводника.

Как видно, оператор (вентиль) NOT на рис. 4.8 состоит из сопротивления и транзистора. Смысл работы такого вентиля сводится к следующему. Обозначим потенциал, соответствующий высокому напряжению, через V . Тогда, если на проводник a подаётся низкий потенциал (битовое значение 0), транзистор не пропускает ток и на проводнике a' имеется высокий потенциал V (битовое значение 1). Но если на проводник a подать высокий потенциал, транзистор пропускает ток I через сопротивление R и потенциал на линии a' падает на величину $I \cdot R$ и достигает значения ниже низкого потенциала (битовое значение 0). Другими словами, связь битовых значений линий a и a' противоположна, т. е. $a' = \text{NOT}a$. Аналогично можно убедиться, что электрическая схема, состоящая из последовательно включенных в цепь сопротивления и двух транзисторов, эквивалентна логическому вентилю NAND.

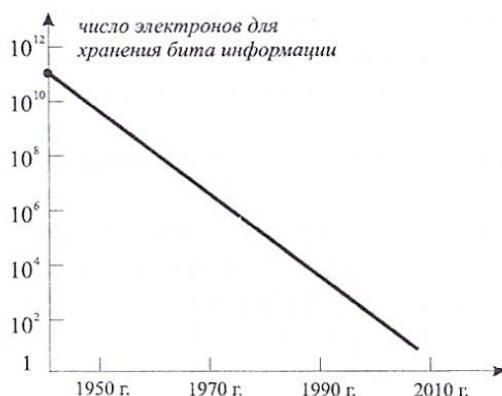


Рис. 4.9. Изменение числа электронов в элементах записи и хранения бита информации по годам

представлена оценка числа примесей в основаниях биполярных транзисторов, требующихся для формирования логических операций в зависимости от времени развития полупроводниковых технологий. По сути, график отражает число электронов, необходимых для хранения одного бита информации. В соответствии с этими данными ясно, что технология достигает субатомных расстояний и фактически переходит на построение информационных систем на атомном и молекулярном уровне, что приводит к необходимости учёта и включения квантово-механических свойств вещества при проектировании логических элементов. Как будет показано ниже, на квантовых компьютерах программы выполняются на квантовых объектах посредством организации унитарной эволюции входных данных. По определению унитарные преобразования обратимы во времени. Таким образом, логическая цепь преобразований должна основываться на обратимых операциях, определение и свойства которых приведены далее.

Упражнение 4.3. Составить логическую диаграмму для полного сумматора, используя операторы AND, XOR и OR.

Упражнение 4.4. Составить логическую диаграмму для полувычитателя.

Упражнение 4.5. Составить логическую диаграмму для полного вычитателя.

Упражнение 4.6. Составить электронную схему для реализации гейта OR.

Электрические цепи классических компьютеров содержат миллионы транзисторов. В этом смысле технологически принципиально важно иметь транзисторы и иные элементы электрических цепей с минимально возможными размерами и объёмами. Непрерывное уменьшение размеров вычислительных устройств, которое наблюдается как тенденция развития информационных систем, может быть отражено на графике (рис. 4.9) [15], где

4.3 Обратимые логические гейты

Условием логической обратимости детерминированных устройств является их возможность восстановления входных и выходных данных друг из друга единственным образом. Если в дополнение к логической обратимости устройство может функционировать в обратном направлении по времени, тогда оно называется физически обратимым, а второй закон термодинамики гарантирует, что устройство не рассеивает теплоту.

При построении логических цепей с обратимыми логическими элементами обычно используют три обратимых гейта (вентиля, оператора): NOT, CNOT, CCNOT, определение которых имеет следующий вид:

- 1. NOT-гейт.** Стандартный гейт отрицания. Данный гейт не теряет информации и является обратимым. Обращение достигается повторным действием NOT-гейта.
- 2. CNOT-гейт:** $\text{CNOT} \equiv \text{CONTROLLED NOT} \equiv$ контролируемое “нет” или контролируемое отрицание. Данный гейт эквивалентно обозначается в цепях одной из двух видов диаграмм (рис. 4.10), соответствующих представленной таблице истинности:

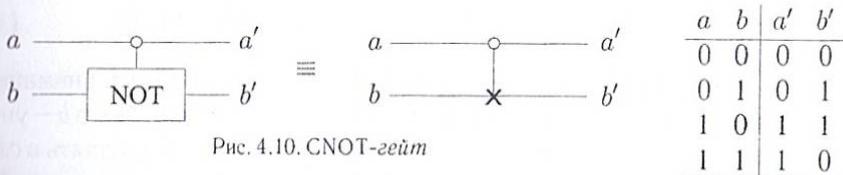


Рис. 4.10. CNOT-гейт

Гейт CNOT имеет две входящие линии a и b — два входных бита и две выходящие линии — два результирующих бита. Бит a' всегда тот же, что и бит a , а соответствующая линия называется контролирующей или управляющей. Если контролирующая линия активирована в состоянии $a = 1$, тогда выходной бит b' определяется как NOT от b . В противном случае при $a = 0$ выходной бит $b' = b$, т. е.

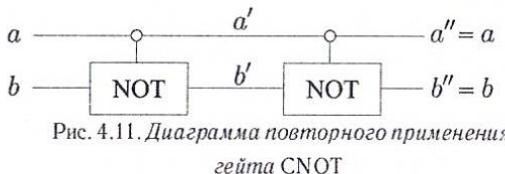
$$b' = \begin{cases} \text{NOT } b, & \text{если } a = 1; \\ b, & \text{если } a = 0. \end{cases} \quad (4.14)$$

Линия $b \rightarrow b'$ называется управляемой или контролируемой. Изображение точки на контролирующей линии является обязательным элементом, так как в логических диаграммах с большим числом линий возможно формальное пересечение вертикальных и горизонтальных

линий, не отражающих связь линий, входящих в определение оператора CNOT.

Из определения гейта CNOT ясно, что:

- действие данного гейта обращается простым повторением (рис. 4.11)



a	b	a'	b'	$a'' = a$	$b'' = b$
0	0	0	0	0	0
0	1	0	1	0	1
1	0	1	1	1	0
1	1	1	0	1	1

- величина b' является гейтом XOR (исключающее или) для бит a и b , а так как операция XOR является операцией суммирования a и b по модулю 2 в бит b' , то символически данную операцию можно записать в виде

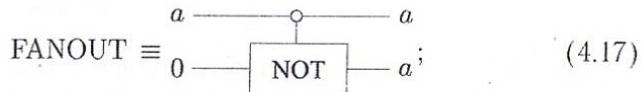
$$\text{XOR} : (a, b) \rightarrow a \oplus b. \quad (4.15)$$

Соответственно, символическое обозначение результата действия гейта CNOT можно представить в виде

$$\text{CNOT} : (a, b) \rightarrow (a, a \oplus b) \equiv (a, \text{XOR} : (a, b)). \quad (4.16)$$

При использовании данной символики следует обратить внимание на порядок записи бит (a, b) в скобках: a – управляющий бит, а b – управляемый. Соблюдение данного порядка необходимо выполнять в сложных или многокубитовых цепях. Подчеркнём также, что сам гейт XOR не является обратимой операцией, так как, например, если результатирующее значение гейта XOR равно 0, то нельзя однозначно определить, из какого входного набора бит $(a, b) = (0, 0)$ или $(a, b) = (1, 1)$, оно произошло. Соответственно, гейт CNOT сохраняет линию $a = a'$, что и устраняет неопределенность гейта XOR;

- гейт CNOT реализует гейт FANOUT (разворачивание), так как при $b = 0$ бит a копируется на линию b' .



или $\text{FANOUT} \equiv \text{CNOT} : (a, 0)$. Эквивалентно функция копирования FANOUT обозначается символом COPY;

- цепь, состоящая из комбинации трёх вентилей CNOT (рис. 4.12), реализует гейт EXCHANGE (обмен) \equiv или гейт SWAP:

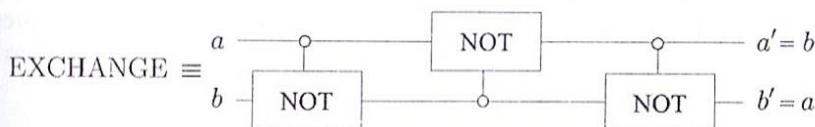


Рис. 4.12. Логическая диаграмма гейта EXCHANGE

3. **CCNOT-гейт:** $\text{CCNOT} \equiv \text{CONTROLLED CONTROLLED NOT} \equiv$ дважды контролируемое отрицание \equiv Тоффоли-гейт.

Данный гейт определяется диаграммой, представленной на рис. 4.13, и таблицей истинности.

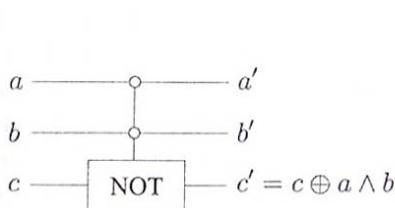


Рис. 4.13. CCNOT-гейт

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

Гейт CCNOT содержит три линии, из которых две линии a и b называются контролирующими и остаются неизменными на выходе, а выход третьей (контролируемой) линии равен $c' = \text{NOT } c$, если обе контролирующие линии активированы в битовые состояния $a = b = 1$, в противном случае значение $c' = c$.

Из определения гейта CCNOT следует, что:

- если на входе контролируемой линии $c = 0$, то $c' = 1$ только при условии $a = 1$ и $b = 1$, в противном случае, если $a = 0$, или $b = 0$, или $a = b = 0$, то на выходе третьей линии получим $c' = 0$. Таким образом, в этом случае ($c = 0$) гейт определяет на контролируемой линии функцию оператора AND от битовых значений контролирующих линий, что символически можно записать следующим образом:

$$\text{CCNOT} : (a, b, 0) \rightarrow (a, b, \text{AND}(a, b)). \quad (4.18)$$

Три комбинации входных бит (a, b) , а именно: $(0, 0), (0, 1), (1, 0)$ – приводят к одному выходному биту логической функции $\text{AND}(a, b) = 0$. Следовательно, для устранения неоднозначности требуется помнить оба входных бита или иметь две контролирующих линии. Сохранение этих битовых значений на линиях a, b на выходе позволяет обратить действие гейта CCNOT;

- повторное выполнение операции CCNOT обращает результат первой операции CCNOT. Логическая диаграмма повторного применения оператора CCNOT (рис. 4.14) и таблица истинности данной операции представлены ниже.

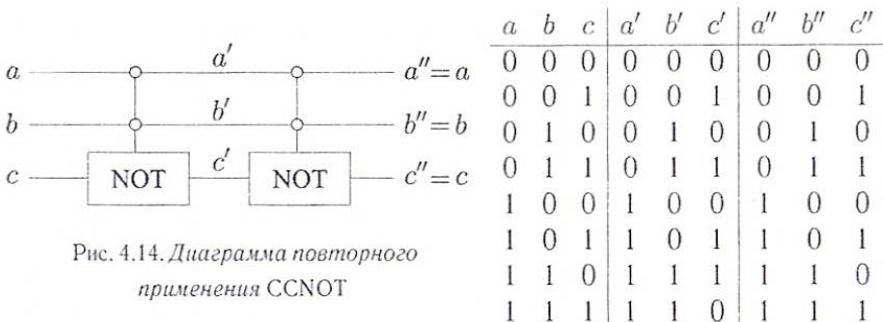


Рис. 4.14. Диаграмма повторного применения CCNOT

Из определения CCNOT-гейта (или Тоффоли-гейта) перебором комбинаций можно установить, что бинарное значение гейта на контролируемой линии может быть представлено в виде различных введённых ранее логических операторов

$$c'' = c \oplus a \wedge b = \begin{cases} a \wedge b & \text{для } c = 0 \quad (\text{AND-гейт}); \\ a \oplus c & \text{для } b = 1 \quad (\text{XOR-гейт}); \\ \bar{c} & \text{для } a = b = 1 \quad (\text{NOT-гейт};) \\ a, & \text{для } b = 1, c = 0 \quad (\text{FANOUT-гейт}). \end{cases} \quad (4.19)$$

То есть данный гейт является универсальным, поскольку он выполняет группу различных логических операций AND, XOR, NOT и FANOUT в зависимости от того, что имеется на входных битах.

Комбинируя обратимые логические элементы, можно составлять сложные логические схемы, выполняющие арифметические операции или реализующие сложные логические выражения, т.е. построить универсальный компьютер. Например, используя последовательность CCNOT-гейта и гейта CNOT, представленную логической диаграммой (рис. 4.15), можно

реализовать операцию сложения двух бит, другими словами, реализовать полусумматор (НА) [9].

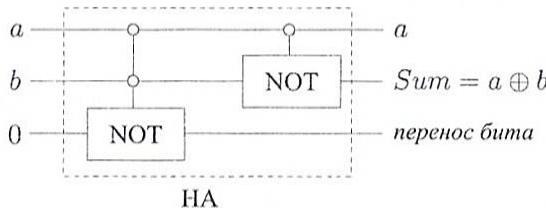


Рис. 4.15. Логическая диаграмма полусумматора на обратимых элементах

Полный сумматор (FA), который использует перенос бита \$c\$ (от предыдущего суммирования) и складывает его с двумя битами (по линиям) \$a\$ и \$b\$, а кроме того, содержит дополнительную линию \$d\$ с равным нулю битом на входе, можно построить на основе комбинации следующих четырёх обратимых логических операторов (рис. 4.16) [9].

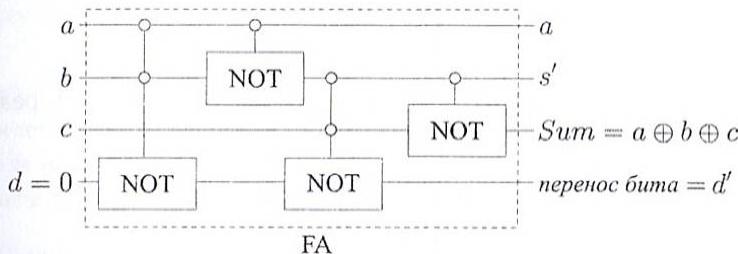


Рис. 4.16. Логическая диаграмма полного сумматора на обратимых элементах

Помимо полной суммы по модулю 2 трёх бит \$a \oplus b \oplus c\$ и переноса бита \$d'\$, в полном сумматоре присутствуют ещё два битовых значения на линиях \$a\$ и \$b\$, не имеющих значения для результата. При этом бит \$a \rightarrow a\$, а бит \$b \rightarrow s' = a \oplus b\$ преобразуется в некоторую промежуточную сумму. Другими словами, на выходе получается не только то, что требовалось получить (сумму \$Sum\$ и перенос бита), но и определённое количество промежуточной информации, которую принято называть “мусором”. Это обстоятельство является типичным при реализации логики вычислений на обратимых гейтах. Наличие мусора в цепях с обратимыми логическими операторами является проблемой, так как разрастание цепей до миллионов гейт означает необходимость хранения огромного количества ненужной информации и неэффективное использование технологических элементов компьютера. Поэтому при организации процесса вычисления на обратимых элементах необходимо ещё и решать задачу борьбы с мусором. В конкретном случае,

представленном на рис. 4.16, мусор может быть сведен в точности к тому, что имеется на входе, если к блоку FA добавить оператор CNOT на две верхние линии [9] (рис. 4.17).

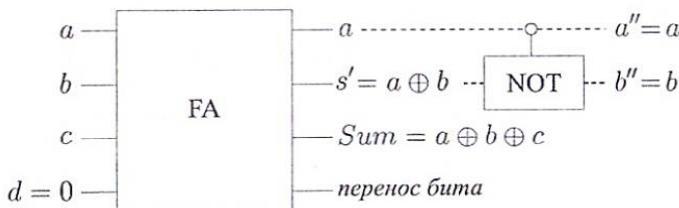


Рис. 4.17. Уничтожение “мусора” у полного сумматора, построенного на обратимых операторах

Действительно, если $a = 0$, то $s' = a \oplus b = b$ и в соответствии с определением гейта CNOT, так как линия a не активирована в состояние 1, битовое значение $b'' = b$. Во втором возможном случае $a = 1$, бит $s' = 1 \oplus b$. При этом

$$s' = \begin{cases} 1, & \text{если } b = 0, \\ 0, & \text{если } b = 1. \end{cases} \quad (4.20)$$

При этом в силу того, что линия a активизирована в состояние 1, результат действия гейта CNOT на линии $b \equiv s'$ будет равен:

$$b'' = \begin{cases} \text{NOT } s' = 0, & \text{если } b = 0 \\ \text{NOT } s' = 1, & \text{если } b = 1 \end{cases} = b. \quad (4.21)$$

Аналогично мусор может быть удален и во всех иных схемах логических цепей. В общем случае схема, представленная на рис. 4.17, может быть упрощена, но для иллюстрации принципов это несущественно.

Таким образом, составляя различные цепи из комбинаций обратимых гейтов, можно построить общий логический блок, который преобразует n -бит обратимым образом. Если сама решаемая задача обратима, тогда “мусорной” информации может не возникать, но в общем случае необходимы дополнительные биты, которые требуются для обращения выполняемой операции. В этом смысле “мусор” содержит информацию, необходимую для обращения процесса вычисления.

На основании (4.17) и обратимости гейта CNOT ясно, что гейт FANOUT также является обратимым гейтом. Другими словами, гейт FANOUT не разрушает информацию, и поэтому возможна его обратимость. Возможность обратимости операции ERASE требует некоторого пояснения. Операция ERASE требуется для периодической “очистки” или обнуления па-

мяти компьютера. Если есть копия некоторого бита, то можно стереть добавочную копию путём операции, обратной FANOUT-гейту. Однако возникает проблема, когда стирается последняя копия бита. В этом случае говорят о так называемом примитивном стирании. Но примитивный ERASE не является абсолютно необходимым в вычислениях, поэтому цепи, построенные на обратимых гейтах, могут реализовать реальные вычисления.

Действительно, вычисление заданной функции $f(a)$ может быть произведено взаимно однозначным соответствием с ее аргументом с сохранением копии входных данных a :

$$f : a \rightarrow (a, f(a)). \quad (4.22)$$

Процедура такого вычисления приводит к прямой проблеме из-за отсутствия примитивного ERASE. Чем больше операторов используется, тем больше “мусорных” бит накапливается, так как в каждом случае сохраняются входные биты для обеспечения обратимости. Таким образом, компьютер, построенный из логически обратимых операторов, ведёт себя следующим образом:

$$f : a \rightarrow (a, j(a), f(a)), \quad (4.23)$$

где $j(a)$ – большое число дополнительных “мусорных” бит.

Беннет решил эту проблему путём стирания “мусорных” бит обратимым образом на промежуточных шагах вычисления. Идея решения проблемы состоит в использовании следующей процедуры:

1. На первом шаге вычисляется f и при этом возникают и “мусорные” биты $j(a)$, и искомый результат (4.23).
2. На втором шаге применяется FANOUT-гейт для дублирования выходного результата $f(a)$ в $f_c(a)$:

$$\text{FANOUT} : (a, j(a), f(a)) \rightarrow (a, j(a), f(a), f_c(a)). \quad (4.24)$$

3. На третьем этапе выполняется операция, обратная вычислению функции f :

$$f^{-1} : (a, j(a), f(a), f_c(a)) \rightarrow (a, f_c(a)). \quad (4.25)$$

Обратная операция удаляет как “мусорные” биты, так и биты первоначально вычисленного выходного результата $f(a)$, не трогая при этом коиню выходного результата $f_c(a)$.

Таким образом, в памяти машины остаётся только набор начальных данных a и копия набора бит вычисленной функции $f(a)$. При этом использование примитивного ERASE не потребовалось.

Упражнение 4.7. Доказать, что логическая диаграмма рис. 4.15 реализует полусумматор.

Упражнение 4.8. Составить логическую диаграмму полувычитателя с использованием обратимых логических операций.

Упражнение 4.9. Доказать, что логическая диаграмма рис. 4.16 реализует полный сумматор.

Упражнение 4.10. Составить логическую диаграмму полного вычитателя с использованием обратимых логических операций.

Упражнение 4.11. Составить логическую диаграмму для выполнения сложения двух трёхбитовых целых чисел с использованием обратимых логических операций.

Часть III

Квантовая модель вычислений

Глава 5

Квантовые компьютерные технологии

5.1 Введение

Переход от классических информационных систем к квантовым и разработка схемы квантовых вычислений возникает по двум причинам. Первая причина технологическая. Фактическое развитие полупроводниковых технологий и технологий изготовления больших интегральных схем приводит к тому, что для записи бита классической информации используются объекты, сравнимые по размерам с молекулярными объектами. Поведение объектов атомно-молекулярного уровня ($\approx 10^{-9} - 10^{-8}$ см) не объясняется в рамках классического описания. Соответственно, предположение о том, что достигнут технологический предел миниатюризации вычислительных систем, не укладывается в логику и историю развития технологических знаний. Поэтому и возникает задача организации вычислений на таких квантовых объектах, как молекулы, атомы и даже элементарные частицы.

Вторая причина, стимулирующая исследования в области квантовых информационных систем, — это проявляющиеся принципиальные ограничения, которые возникают при использовании классических компьютеров. Такие задачи появляются, когда речь идет о возрастающем числе данных и экспоненциальном росте времени вычисления для многих практически интересных и важных классических алгоритмов. Среди них обычно приводится задача факторизации числа N на простые множители. В классической теории вычислений "приемлемыми" рассматриваются такие вычислительные алгоритмы, в которых число шагов растёт как полином небольшой степени от размера входных данных. В противном случае алгоритмы принадлежат классу труднорешаемых задач.

Для задачи факторизации заданного числа входными данными является число N , которое необходимо разложить на множители. Поэтому "дли-

на” входных данных на классическом “бинарном” компьютере есть $\log_2 N$. Основание 2 логарифма связано с использованием двоичной системы исчисления.

Известно, что лучшие алгоритмы факторизации выполняются за число шагов k , которое имеет следующий порядок [18]:

$$k = C \cdot \exp \left\{ (64/9)^{1/3} (\ln N)^{1/3} (\ln \ln N)^{2/3} \right\}. \quad (5.1)$$

То есть алгоритм вычислений приводит к экспоненциальному росту числа шагов по мере роста числа входных данных.

Например, в 1994 г. 129-значное число было факторизовано на 1600 рабочих станциях, распределенных по всему миру [13]. Время факторизации составило 8 месяцев. Используя результаты этого эксперимента, можно качественно оценить порядок величины константы C в (5.1). Оценка числа времени, которое потребуется для факторизации 250-значного числа на тех же 1600 рабочих станциях, даёт $\sim 10^6$ (миллион) лет! Соответственно, для факторизации 1000-значного числа потребуется 10^{25} лет, что на 11 – 12 порядков больше возраста Вселенной, который оценивается в $10^{12} – 10^{13}$ лет.

Абстрактная задача факторизации очень больших чисел, помимо академического интереса, имеет прямое отношение к системам криптографии с открытым ключом, нашедшим широкое применение в современных криптографических системах. Забегая вперед, можно отметить, что факторизация 1000-значного числа с помощью квантового алгоритма потребует (в отличие от классических алгоритмов) всего лишь несколько миллионов шагов. Следовательно, если квантовые алгоритмы удастся реализовать в реальном устройстве, то крипtosистемы с открытым ключом, основанные на сложности факторизации чисел приблизительно с 250 знаками, могут оказаться некриптостойкими.

Существенным фактом развития квантовых вычислений является возможность осуществления эффективного параллелизма в квантовых системах, основанных на атомно-молекулярных объектах, что является привлекательным для решения многих практически важных задач, не доступных для решения за разумное время на классических устройствах.

Исходным моментом развития процедур и технологий вычисления на сложных квантовых системах является исследование преобразований кубита и построение логических цепей с использованием произвольного числа кубит.

5.2 Однокубитовые гейты

Классические компьютерные цепи состоят из проводов и набора логических гейтов (совокупности транзисторов и иных компонент электрических цепей). Провода в этом случае служат для передачи стандартных напряжений по электрическим цепям, а логические гейты осуществляют преобразование “проходящих” через них потенциалов, закодированных в рамках бинарной арифметики. При этом единственным нетривиальным логическим гейтом, который преобразует один бит классической информации в один бит информации, является NOT-гейт, действие которого сводится к преобразованию битов вида: $0 \rightarrow 1$ или $1 \rightarrow 0$. Квантовым аналогом классического бита информации в квантовой теории информации является кубит.

Одиночный кубит по определению является суперпозицией двух квантовых состояний $|0\rangle$ и $|1\rangle$, каждое из которых рассматривается как модель одного бита классической информации:

$$|\psi\rangle = a|0\rangle + b|1\rangle. \quad (5.2)$$

Физически однокубитовыми гейтами (операторами) являются логические элементы \hat{R} , на вход которых подаётся кубит в некотором начальном состоянии $|\psi\rangle$, а на выходе данного элемента появляется кубит в преобразованном состоянии $|\psi'\rangle$:

$$|\psi\rangle = a|0\rangle + b|1\rangle \Rightarrow |\psi'\rangle = c|0\rangle + d|1\rangle; \quad |\psi'\rangle = \hat{R}|\psi\rangle.$$

В соответствии с определением классического NOT-гейта квантовый гейт отрицания (т. е. гейт, преобразующий битовую информацию внутри кубита) определяется следующим образом:

$$\text{NOT : } |\psi\rangle = \text{NOT : } (a|0\rangle + b|1\rangle) = a|1\rangle + b|0\rangle. \quad (5.3)$$

На основании теории представлений состоянию кубита $|\psi\rangle$ (5.2) соответствует двухкомпонентный столбец

$$|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \rightarrow a|0\rangle + b|1\rangle; \quad |a|^2 + |b|^2 = 1. \quad (5.4)$$

Поэтому квантовым аналогом классического NOT-гейта является матрица вида

$$X \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \text{так как} \quad X \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} b \\ a \end{pmatrix}. \quad (5.5)$$

$$X : (a |0\rangle + b |1\rangle) = a |1\rangle + b |0\rangle.$$

Данная матрица X совпадает с матрицей Паули σ_x в s_z -представлении.

В соответствии с принципами квантовой теории квантовые гейты, преобразующие однокубитовое состояние (5.4), являются унитарными матрицами размерности 2×2 . В отличие от классических систем, для кубита можно построить неограниченное число однокубитовых операторов. Однако в силу полноты системы матриц Паули и единичной матрицы I любая 2×2 матрица может быть разложена по этой полной системе матриц. Поэтому для практического использования представляют интерес сами матрицы Паули $X \equiv \sigma_x$, $Y \equiv \sigma_y$, $Z \equiv \sigma_z$ и некоторые их специальные комбинации, среди которых часто используются следующие:

$$\begin{aligned} H &\equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}; & S &\equiv \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}; \\ T &\equiv \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}; & P(\phi_1, \phi_2) &\equiv \begin{pmatrix} e^{i\phi_1} & 0 \\ 0 & e^{i\phi_2} \end{pmatrix}. \end{aligned} \quad (5.6)$$

Приведённые в (5.6) матрицы определяют группу однокубитовых операторов, которые получили следующие наименования: H – гейт Адамара, S – фазовый гейт, T – $\pi/8$ -гейт, а гейт $P(\phi_1, \phi_2)$ – фазовращатель. Из определения перечисленных логических операторов получаем, например, что гейт Адамара выражается через матрицы Паули следующим образом:

$$H = \frac{1}{\sqrt{2}} (\sigma_x + \sigma_z) \equiv \frac{1}{\sqrt{2}} (X + Z). \quad (5.7)$$

Соответственно, фазовый гейт S является квадратом $\pi/8$ гейта $S = T^2$. Название T -гейта ($\pi/8$ -гейт) определяется историческими причинами и возможностью представления матрицы этого гейта с точностью до общего фазового множителя $\exp(i\pi/8)$ в виде

$$T \equiv \exp(i\pi/8) \begin{pmatrix} \exp(-i\pi/8) & 0 \\ 0 & \exp(i\pi/8) \end{pmatrix}. \quad (5.8)$$

Гейт Адамара является одним из наиболее полезных и часто используемых квантовых гейтов в квантовой теории информации. Этот гейт иногда определяют как “квадратный корень” от квантового гейта NOT. Это связано с тем, что гейт Адамара преобразует базисное состояние кубита $|0\rangle$ в равновероятную суперпозицию двух базисных состояний $(|0\rangle + |1\rangle)/\sqrt{2}$, т. е. в “половину пути” между состоянием $|0\rangle$ и состоянием $|1\rangle$ в геометрической интерпретации кубита на сфере Блоха. Соответственно, базисное

состояние $|1\rangle$ преобразуется гейтом Адамара в суперпозицию следующего вида: $(|0\rangle - |1\rangle)/\sqrt{2}$, что также можно интерпретировать как “половину пути” между $|0\rangle$ и $|1\rangle$. Однако квадрат гейта Адамара $H^2 = H \cdot H$ не приводит к квантовому NOT-гейту, так как алгебраические вычисления дают $H^2 \equiv I$. То есть двукратное применение гейта H возвращает систему в исходное состояние. Другими словами, гейт Адамара является обратимым однокубитовым гейтом.

Графическое обозначение последовательности преобразований состояния исходного кубита в состояние кубита на выходе в результате действия однокубитового логического оператора представляют в следующем виде:

$$\begin{array}{c}
 \text{вход} \longrightarrow \boxed{\text{гейт}} \longrightarrow \text{выход} \\
 a|0\rangle + b|1\rangle \longrightarrow \boxed{X} \longrightarrow b|0\rangle + a|1\rangle \\
 a|0\rangle + b|1\rangle \longrightarrow \boxed{Y} \longrightarrow -ib|0\rangle + ia|1\rangle \\
 a|0\rangle + b|1\rangle \longrightarrow \boxed{Z} \longrightarrow a|0\rangle - b|1\rangle \\
 a|0\rangle + b|1\rangle \longrightarrow \boxed{H} \longrightarrow a\frac{|0\rangle + |1\rangle}{\sqrt{2}} + b\frac{|0\rangle - |1\rangle}{\sqrt{2}} \\
 a|0\rangle + b|1\rangle \longrightarrow \boxed{S} \longrightarrow a|0\rangle + ib|1\rangle \\
 a|0\rangle + b|1\rangle \longrightarrow \boxed{T} \longrightarrow a|0\rangle + b\exp(i\pi/4)|1\rangle = \\
 = \exp(i\pi/8)[a\exp(-i\pi/8)|0\rangle + b\exp(i\pi/8)|1\rangle] \\
 a|0\rangle + b|1\rangle \longrightarrow \boxed{P} \longrightarrow a\exp(i\phi_1)|0\rangle + b\exp(i\phi_2)|1\rangle,
 \end{array} \tag{5.9}$$

где линии не являются обозначением “проводов”, а служат для фиксации входящего и выходящего состояния кубита. Данные преобразования часто представляют и в виде алгебраических выражений в форме, принятой в алгебре операторов, например:

$$\begin{aligned}
 X &: (a|0\rangle + b|1\rangle) = b|0\rangle + a|1\rangle; \\
 Y &: (a|0\rangle + b|1\rangle) = -ib|0\rangle + ia|1\rangle; \\
 Z &: (a|0\rangle + b|1\rangle) = a|0\rangle - b|1\rangle; \\
 S &: (a|0\rangle + b|1\rangle) = a|0\rangle + ib|1\rangle; \\
 H &: (a|0\rangle + b|1\rangle) = a\frac{|0\rangle + |1\rangle}{\sqrt{2}} + b\frac{|0\rangle - |1\rangle}{\sqrt{2}}.
 \end{aligned} \tag{5.10}$$

Квантовые гейты являются унитарными операторами, осуществляющими преобразование кубита. В общем случае произвольный унитарный однокубитовый оператор может быть записан в виде

$$U = \exp(i\alpha) R_{\mathbf{n}}(\theta) = \exp(i\alpha) [\cos(\theta/2) - i(\vec{\sigma} \cdot \mathbf{n}) \sin(\theta/2)], \tag{5.11}$$

где $R_{\mathbf{n}}(\theta)$ – оператор поворота (2.39) спинового состояния на угол θ вокруг оси, определённой единичным вектором \mathbf{n} , α и θ – действительные числа.

Используя вид оператора поворота, можно установить много полезных свойств и соотношений для однокубитовых операторов, например: гейт T с точностью до несущественного глобального фазового множителя совпадает с оператором поворота на угол $\pi/4$ вокруг оси $z = R_z(\pi/4)$, так как $T \equiv \exp(i\pi/8)R_z(\pi/4)$. Соответственно, с учётом условия антисимметрии матриц Паули $\sigma_x\sigma_y = -\sigma_y\sigma_x$ можно найти

$$X R_y(\theta) X = R_y(-\theta), \quad (5.12)$$

и аналогичные соотношения для других матриц Паули и операторов поворота вокруг осей x, z .

В алгебре матриц Паули доказывается *теорема $X - Y$ разложения* для однокубитового гейта (оператора). Содержание теоремы утверждает, что существуют действительные числа $\alpha, \beta, \gamma, \delta$, такие, что унитарный оператор U может быть представлен в виде

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta). \quad (5.13)$$

Практически содержание этой теоремы является вытекающим из определения унитарной матрицы следствием, которое означает, что унитарная матрица размерности 2×2 задаётся четырьмя действительными параметрами.

Последовательность однокубитовых операторов можно рассматривать как квантовую цепь, реализующую преобразование кубита. С целью изучения квантовых цепей полезно отметить равенства, справедливость которых можно доказать исходя из определения операторов:

$$HXH = Z; \quad HYH = -Y; \quad HZH = X; \quad HTH = e^{i\alpha} R_x(\pi/4). \quad (5.14)$$

Например:

$$\begin{aligned} HXH &= \frac{1}{2}(\sigma_x + \sigma_z)\sigma_x(\sigma_x + \sigma_z) = \frac{1}{2}(\sigma_x + \sigma_z)(1 + \sigma_x\sigma_z) = \\ &= \frac{1}{2}(\sigma_x + \sigma_z + \sigma_z + \sigma_z\sigma_x\sigma_z) = \sigma_z, \end{aligned} \quad (5.15)$$

так как $\sigma_z\sigma_x\sigma_z = -i\sigma_z\sigma_y = -i(-i\sigma_x) = -\sigma_x$.

Представленные в данном разделе выражения демонстрируют математический аппарат для описания изменения состояния одиночного кубита. Реальная квантовая информационная система оперирует с системой кубит или квантовым регистром, определение которого будет приведено ниже.

Упражнение 5.1. Доказать равенства (5.14).

Упражнение 5.2. Определить результат действия последовательности однокубитовых операторов $H S P T H$ на кубит в состоянии $|1\rangle$.

5.3 Квантовый интерферометр

В качестве примера квантовой цепи с однокубитовыми гейтами рассмотрим последовательное (слева направо) действие квантовыми логическими устройствами (операторами) $H P(\phi_1, \phi_2) H$ на базисное состояние кубита $|0\rangle$, т. е. $|q\rangle = H P(\phi_1, \phi_2) H : |0\rangle$. Квантовая цепь такого преобразования выглядит следующим образом [7]:

$$|0\rangle \xrightarrow{H} |q'\rangle \xrightarrow{P} |q''\rangle \xrightarrow{H} |q\rangle \quad (5.16)$$

Последовательные состояния кубита после действия каждого оператора (гейта) представленной цепи имеют вид

$$|q'\rangle = H |0\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle); \quad (5.17)$$

$$|q''\rangle = P(\phi_1, \phi_2) |q'\rangle = \frac{1}{\sqrt{2}} (e^{i\phi_1} |0\rangle + e^{i\phi_2} |1\rangle); \quad (5.18)$$

$$|q'''\rangle = H |q''\rangle = \frac{1}{2} [(e^{i\phi_1} + e^{i\phi_2}) |0\rangle + (e^{i\phi_1} - e^{i\phi_2}) |1\rangle]. \quad (5.19)$$

Для упрощения последнего выражения воспользуемся тождественными преобразованиями:

$$e^{i\phi_1} \pm e^{i\phi_2} = e^{i(\phi_1+\phi_2)/2} (e^{i(\phi_1-\phi_2)/2} \pm e^{-i(\phi_1-\phi_2)/2}).$$

В результате $|q'''\rangle$ из (5.19) можно представить следующим образом:

$$|q'''\rangle = \exp\left(\frac{\phi_1 + \phi_2}{2}\right) |q\rangle; \quad |q\rangle = \cos\left(\frac{\delta\phi}{2}\right) |0\rangle + i \sin\left(\frac{\delta\phi}{2}\right) |1\rangle,$$

где $\delta\phi = \phi_1 - \phi_2$. Так как общая фаза перед кубитом, с точки зрения квантовой теории, несущественна, окончательный результат действия логических операторов в рассмотренной цепи на кубит в состоянии $|0\rangle$ есть

$$|q\rangle = \cos\left(\frac{\delta\phi}{2}\right) |0\rangle + i \sin\left(\frac{\delta\phi}{2}\right) |1\rangle, \quad \delta\phi \equiv \phi_1 - \phi_2. \quad (5.20)$$

Таким образом, после действия последовательности гейт $H P(\phi_1, \phi_2) H$ на базисное состояние кубита $|0\rangle$ формируется кубит, являющийся суперпозицией базисных состояний $|0\rangle$ и $|1\rangle$. При этом вероятность измерить в

данной суперпозиции базисное состояние $|0\rangle$ или базисное состояние $|1\rangle$ определяется квадратами модулей коэффициентов в суперпозиции кубита $|q\rangle$ (5.20):

$$P_0 = \cos^2\left(\frac{\delta\phi}{2}\right) = \frac{1}{2}[1 + \cos(\delta\phi)]; \quad P_1 = \sin^2\left(\frac{\delta\phi}{2}\right) = \frac{1}{2}[1 - \cos(\delta\phi)]. \quad (5.21)$$

Как видно из (5.21), при $\delta\phi = 0$ (фазовращатели отсутствуют) на выходе рассматриваемой цепи получится то же квантовое состояние $|0\rangle$, что и было на входе. Этот результат тривиален, так как при $\delta\phi = 0$ оператор $P = I$, а $H \cdot H = I$. Но если, например, $\delta\phi = \pi/2$, то возникает следующая суперпозиция базовых состояний: $|q\rangle = (|0\rangle + i|1\rangle)/\sqrt{2}$, вероятность измерения которых одинакова. Наконец, если $\delta\phi = \pi$, то из базисного состояния $|0\rangle$ формируется базисное состояние $|1\rangle$.

При действии рассмотренной выше квантовой цепи на базисное состояние $|1\rangle$ результат будет иметь вид

$$|q\rangle = i \sin\left(\frac{\delta\phi}{2}\right) |0\rangle + \cos\left(\frac{\delta\phi}{2}\right) |1\rangle. \quad (5.22)$$

Рассмотренная выше квантовая цепь является квантовым аналогом оптического интерферометра, построенного из двух светоотводителей (их роль выполняют гейты Адамара), двух зеркал и элементов задержки фазы волны (гейт $P(\phi_1, \phi_2)$) на пути распространения электромагнитной волны по двум оптическим каналам (рис. 5.1).

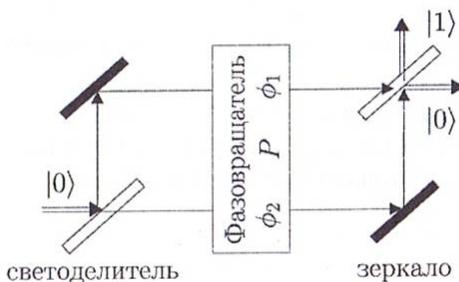


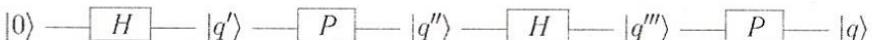
Рис. 5.1. Схема оптического интерферометра

В данном случае состояния $|0\rangle$ и $|1\rangle$ соответствуют, например, вертикальной и горизонтальной поляризации электромагнитного поля.

Можно отметить, что для формирования произвольного однокубитового состояния $|q\rangle = a|0\rangle + b|1\rangle$ можно использовать практически аналогичную (5.16) квантовую цепь, состоящую из следующей последовательности

однокубитовых операторов:

$$|q\rangle = P(\phi_1 = 0, \phi_2 = \pi/2 + \varphi) H P(\phi_1 = 0, \phi_2 = \theta) H : |0\rangle . \quad (5.23)$$



Последовательность изменения состояния кубита в этом случае определяется выражениями:

$$\begin{aligned} |q'\rangle &= H |0\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) , \\ |q''\rangle &= P(\phi_1 = 0, \phi_2 = \theta) |q'\rangle = \frac{1}{\sqrt{2}} (|0\rangle + e^{i\theta} |1\rangle) , \\ |q'''\rangle &= H |q''\rangle = \frac{1}{2} [(1 + e^{i\theta}) |0\rangle + (1 - e^{i\theta}) |1\rangle] . \end{aligned}$$

Наконец, на последнем этапе получаем

$$|q\rangle = P(\phi_1 = 0, \phi_2 = \varphi + \pi/2) |q'''\rangle = \frac{1}{2} (1 + e^{i\theta}) |0\rangle + \frac{1}{2} e^{i(\varphi + \pi/2)} (1 - e^{i\theta}) |1\rangle . \quad (5.24)$$

Выражение (5.24) можно преобразовать с учётом следующих равенств:

$$\frac{1}{2} (1 + e^{i\theta}) = e^{i\theta/2} \cos \frac{\theta}{2}; \quad \frac{1}{2} (1 - e^{i\theta}) = -ie^{i\theta/2} \sin \frac{\theta}{2}.$$

Таким образом, окончательно имеем произвольное однокубитовое состояние:

$$|q\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle , \quad (5.25)$$

так как общая фаза $\exp(i\theta/2)$ не играет роли в определении квантового состояния.

Упражнение 5.3. Доказать равенство (5.22).

Упражнение 5.4. Определить чему равна вероятность измерения состояния $|1\rangle$ кубита в состоянии (5.25) при $\theta = \pi/6$ и $\varphi = \pi/3$?

5.4 Квантовый регистр

Совокупность кубит образует *квантовый регистр*, или q -регистр (кубитовый регистр). Например, при наличии двух кубит $|q_1\rangle$ и $|q_2\rangle$ двухкубитовый квантовый регистр $|q\rangle_2$ может быть эквивалентно определен так:

$$\begin{aligned} |q\rangle_2 &\equiv |q_1 q_2\rangle = |q_1\rangle \otimes |q_2\rangle = (\alpha |0\rangle + \beta |1\rangle) \otimes (\alpha' |0\rangle + \beta' |1\rangle) = \\ &= c_1 |0\rangle \otimes |0\rangle + c_2 |0\rangle \otimes |1\rangle + c_3 |1\rangle \otimes |0\rangle + c_4 |1\rangle \otimes |1\rangle . \end{aligned}$$

Здесь $c_1 = \alpha \cdot \alpha'$; $c_2 = \alpha \cdot \beta'$; $c_3 = \beta \cdot \alpha'$; $c_4 = \beta \cdot \beta'$, \otimes – символ прямого произведения векторов состояний. Четыре прямых произведения двух базисов однокубитовых состояний удобно обозначить следующим образом:

$$|0\rangle_2 \equiv |00\rangle = |0\rangle \otimes |0\rangle; \quad |1\rangle_2 \equiv |01\rangle = |0\rangle \otimes |1\rangle;$$

$$|2\rangle_2 \equiv |10\rangle = |1\rangle \otimes |0\rangle; \quad |3\rangle_2 \equiv |11\rangle = |1\rangle \otimes |1\rangle.$$

Таким образом, для двухкубитовой системы имеется четыре базисных (ортонормированных) $\langle n|k\rangle_2 = \delta_{n,k}$ двухкубитовых состояния $|k\rangle_2$, где $k \in 00, 01, 10, 11$ или для краткости $k \in 0, 1, 2, 3$. Следовательно, произвольное двухкубитовое состояние (или двухкубитовый регистр) может быть представлено в виде

$$|q\rangle_2 \equiv \sum_{k=0}^3 c_k |k\rangle_2; \quad \sum_{k=0}^3 |c_k|^2 = 1. \quad (5.26)$$

Здесь c_k – амплитуда вероятности базисного двухкубитового состояния $|k\rangle_2$ в суперпозиции, задающей двухкубитовый регистр $|q\rangle_2$.

Во избежание путаницы в обозначениях произвольного кубита $|q\rangle$ или регистра кубит $|q\rangle_2 = |q_1 q_2\rangle$ с обозначением базисных векторов $|0\rangle, |1\rangle$ (или базисных векторов состояний регистра $|0\rangle_2, \dots, |3\rangle_2$) ниже используется следующая договоренность. Базисные векторы обозначаются буквами, обычно применяемыми для целых чисел, такими как i, k, l, m, n или a, b, c . В свою очередь, для обозначения произвольного кубита или регистра кубит используются буквы q, r, ϕ, ψ, \dots

Символические дираковские обозначения для регистра кубит вида $|q\rangle_2$ являются условной, упрощённой системой обозначений вектор-столбцов для задания состояний в выбранном представлении. При использовании матричных обозначений для пары кубит $|a\rangle$ и $|b\rangle$ в качестве базисных нужно выбрать вектор-столбцы, являющиеся прямым произведением базисных вектор-столбцов отдельных кубит, например:

$$|0\rangle_2 \equiv |0_a 0_b\rangle = |0_a\rangle \otimes |0_b\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}. \quad (5.27)$$

Аналогично оставшиеся 3 базисных состояния в матричных обозначениях

имеют вид

$$|1\rangle_2 = |0_a 1_b\rangle \equiv \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}; \quad |2\rangle_2 = |1_a 0_b\rangle \equiv \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}; \quad |3\rangle_2 = |1_a 1_b\rangle \equiv \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}. \quad (5.28)$$

В дальнейшем во избежание громоздких индексных обозначений нумерация кубит в регистре будет определяться последовательной записью базисных состояний кубит слева направо, начиная с первого кубита и кончая последним.

Обобщение (5.26) на случай произвольного числа кубит n , т. е. для регистра из n кубит, имеет тривиальный вид:

$$|q\rangle_n \equiv \sum_{k=0}^{2^n-1} c_k |k\rangle_n, \quad \text{где} \quad \sum_{k=0}^{2^n-1} |c_k|^2 = 1. \quad (5.29)$$

Соответственно, 2^n базисных вектора $|k\rangle_n$, $k \in 0, 1, 2, \dots, 2^n - 1$ для регистра из n кубит обозначаются следующим тождественным образом:

$$|0\rangle_n \equiv |00\dots 00\rangle = |0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle;$$

$$|1\rangle_n \equiv |00\dots 01\rangle = |0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle \otimes |1\rangle;$$

$$|2\rangle_n \equiv |00\dots 10\rangle = |0\rangle \otimes |0\rangle \otimes \dots \otimes |1\rangle \otimes |0\rangle;$$

...

$$|2^n - 1\rangle_n \equiv |11\dots 11\rangle = |1\rangle \otimes |1\rangle \otimes \dots \otimes |1\rangle.$$

Здесь, как и в случае двухкубитового регистра, данные базисные состояния регистра из n кубит можно представить ортонормированными векторами размерности 2^n при использовании матричных обозначений.

$$|0\rangle_n \equiv |00\dots 0\rangle = |0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \dots \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \\ 0 \\ \dots \\ 0 \end{pmatrix} \otimes \dots \otimes \begin{pmatrix} 1 \\ 0 \\ 0 \\ \dots \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \dots \\ 0 \end{pmatrix}. \quad (5.30)$$

Соответственно,

$$|1\rangle_n \equiv |00\dots0\rangle = |0\rangle \otimes |0\rangle \otimes \dots \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \dots \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \dots \\ 0 \end{pmatrix} \quad (5.31)$$

и так далее до состояния $|2^n - 1\rangle_n$:

$$|2^n - 1\rangle_n \equiv |11\dots1\rangle = |1\rangle \otimes |1\rangle \otimes \dots \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \dots \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \dots \\ 1 \end{pmatrix}. \quad (5.32)$$

По определению квантовый регистр из n штук кубит содержит 2^n различных классических чисел одновременно. Так, двухкубитовый регистр содержит 4 числа, записанные через его четыре базисных состояния — $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$. Если для них используется бинарная арифметика, то они определяют 4 десятичных числа: 0, 1, 2, 3. При количестве кубит в регистре, равном 500, соответствующий квантовый регистр заключает в себе классических чисел больше, чем число атомов во Вселенной. И это действительно является уникальным свойством регистра кубит, которое не наблюдается в макроскопическом мире. Регистр из 500 кубит имеет 2^{500} базисных вектора, содержащих последовательности из 500 нулей и единиц. Ни одно классическое устройство памяти неспособно даже просто хранить такой объём информации. Если бы было возможно производить, например, вычисления с этим числом значений за один шаг вычислений, то была бы достигнута невероятная параллельность обработки информации. В этом и состоит привлекательность систем обработки квантовых регистров, которые именуются квантовыми компьютерами.

Однако в соответствии с принципами квантовой теории доступ можно получить только к одному из этого ошеломляющего числа значений. Поэтому задача квантовых вычислений и обработки информации состоит не в прямом использовании квантового параллелизма, а в разработке логических устройств и алгоритмов, способных довести амплитуду вероятности искомого результата до значения, максимально близкого к единице, обеспечивая определение искомого результата при измерении квантового регистра. Для описания процесса изменения состояния квантового регистра

вводятся логические операторы, которые получили название “многокубитовые квантовые гейты”.

Упражнение 5.5. Записать все базисные состояния для регистра из трёх кубит, используя символические дираковские обозначения и матричное представление базисных состояний.

Упражнение 5.6. Определить число базисных состояний регистра из пяти кубит.

5.5 Многокубитовые квантовые гейты

Из общего числа логических операторов, осуществляющих преобразование регистра из заданного числа кубит по принципам квантовой теории, необходимо выделить только унитарные операторы. Требование унитарности означает, что логическая операция должна быть обратимой. Классические обратимые операторы формируют класс контролируемых операций. Простейшим двухбитовым контролируемым гейтом (или оператором) в классическом компьютере является CNOT-гейт. В квантовых вычислениях водится, по сути, подобный гейт, который имеет два кубита на входе и два на выходе. Как и в классическом случае, один из пары кубит называется контролирующим, а второй – контролируемым, или кубитом-мишенью. Буквенное обозначение CNOT-квантового гейта не отличается от обозначений классического гейта. Логика выполнения операции при этом определяется следующим образом: если контролирующий кубит находится в однокубитовом базисном состоянии $|1\rangle$, тогда контролируемый кубит подвергается квантовой операции NOT. В случае если контролирующий кубит находится в базисном состоянии $|0\rangle$, то контролируемый кубит остаётся без изменения. Графически “цепь” (логическая диаграмма) квантового CNOT-гейта изображается, как показано на рис. 5.2.

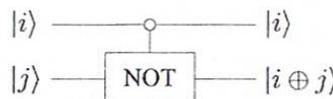


Рис. 5.2. Логическая диаграмма квантового CNOT-гейта

Здесь $i, j \in \{0, 1\}$, а $|i\rangle$ и $|j\rangle$ – базисные однокубитовые состояния. Формальная алгебраическая запись действия оператора CNOT на базисные векторы двухкубитового состояния $|k\rangle_2$, $k \in \{0, 1, 2, 3\}$ может быть представлена в форме

$$\text{CNOT} : |k\rangle_2 \equiv \text{CNOT} : |i, j\rangle = |i, i \oplus j\rangle; \quad i, j \in \{0, 1\}. \quad (5.33)$$

Здесь \oplus — операция сложения по модулю 2. Кроме того, нужно обратить внимание на условность обозначений, состоящую в том, что контролирующий кубит i отображается в записи исходного двухкубитового состояния $|i, j\rangle$ первым, а контролируемый кубит j — вторым.

Следует подчеркнуть, что в определении квантового CNOT-гейта (5.33) используются базисные однокубитовые состояния $|i\rangle$, $|j\rangle$, $i, j \in 0, 1$. Это не означает, что на вход такого гейта нельзя подать суперпозицию базисных состояний (или произвольное двухкубитовое состояние). В случае если на вход квантового гейта CNOT подаётся произвольное двухкубитовое состояние, результат на выходе надо рассматривать последовательно в соответствии с приведённым выше определением (5.33).

Пусть, например, на вход квантового контролируемого отрицания по дано двухкубитовое состояние $|q\rangle_2 = |a\rangle \otimes |b\rangle$, где $|a\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ и $|b\rangle = \beta_0|0\rangle + \beta_1|1\rangle$, а α_i, β_i — комплексные числа. Таким образом, двухкубитовое состояние на входе имеет вид

$$|q\rangle_2 = (\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle) = \sum_{i,j=0}^1 \gamma_{ij} |i, j\rangle \equiv \sum_{k=0}^3 c_k |k\rangle_2.$$

Здесь $\gamma_{ij} = \alpha_i \cdot \beta_j$, а $c_0 = \gamma_{00}$, $c_1 = \gamma_{01}$, $c_2 = \gamma_{10}$ и $c_3 = \gamma_{11}$. В результате действие квантового контролируемого отрицания определяется последовательностью операций:

$$\begin{aligned} \text{CNOT} : \sum_{k=0}^3 c_k |k\rangle_2 &\equiv \text{CNOT} : \sum_{i,j=0}^1 \gamma_{ij} |i, j\rangle = \\ &= \sum_{i,j=0}^1 \gamma_{ij} \text{CNOT} : |i, j\rangle = \sum_{i,j=0}^1 \gamma_{ij} |i, i \oplus j\rangle. \end{aligned} \quad (5.34)$$

Произвольное двухкубитовое квантовое состояние в матричном виде определяется суперпозицией базисных векторов двухкубитовых состояний:

$$|q\rangle_2 = \sum_{k=0}^3 c_k |k\rangle_2 = c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle \equiv \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix}. \quad (5.35)$$

Таким образом, оператор квантового CNOT-гейта является матрицей размерности 4×4 и имеет следующий вид в соответствии с определением в

базисе двухкубитовых состояний $|k\rangle_2$, $k \in 0, 1, 2, 3$:

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \text{ так как } \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} c_0 \\ c_1 \\ c_3 \\ c_2 \end{pmatrix}. \quad (5.36)$$

Соответственно, при использовании алгебраических обозначений действие оператора CNOT может быть представлено в виде

$$\begin{aligned} \text{CNOT} : |q\rangle_2 &= \text{CNOT} : (c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle) = \\ &= c_0|00\rangle + c_1|01\rangle + c_3|10\rangle + c_2|11\rangle. \end{aligned} \quad (5.37)$$

Если вместо оператора отрицания в CNOT выбирать в качестве оператора некоторый произвольный унитарный оператор, действующий на контролируемый кубит $|t\rangle$, то контролируемую U-операцию или с-U-гейт можно графически определить, как показано на рис. 5.3 [7], [8].

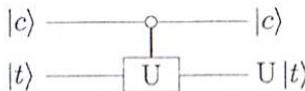


Рис. 5.3. Логическая диаграмма контролируемого U-оператора

Здесь так же, как и в CNOT, оператор U действует на контролируемый кубит $|t\rangle$ только при условии, что контролирующий кубит находится в базисном однокубитовом состоянии $|1\rangle$. Соответственно, в более общем случае можно определить и более сложные контролируемые гейты (рис. 5.4).

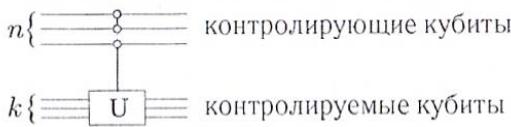


Рис. 5.4. Общая логическая диаграмма контролируемого U-оператора

Определенный так гейт осуществляет некоторое унитарное преобразование над регистром контролируемых кубит только в случае, если контролирующие кубиты находятся в базисном состоянии $|2^n - 1\rangle_n \equiv |1, 1, \dots, 1, 1\rangle$. Наиболее важным из таких операторов является CCNOT-гейт, или гейт Тоффоли [20] (рис. 5.5).

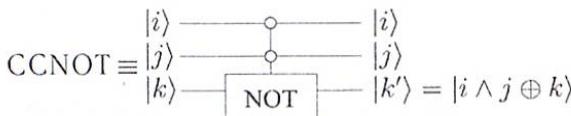


Рис. 5.5. Логическая диаграмма CCNOT-оператора

Здесь, как и в определении CNOT, состояния $|i\rangle, |j\rangle, |k\rangle, |k'\rangle$ – базисные однокубитовые состояния $|0\rangle, |1\rangle$. В данном гейте управляющими являются кубиты $|i\rangle$ и $|j\rangle$, которые образуют регистр управляющих кубит, а управляемым кубитом является кубит $|k\rangle$.

Пространство базисных состояний для регистра из трёх кубит содержит восемь базисных состояний, которые в символическом обозначении имеют вид

$$|0\rangle_3 \equiv |0, 0, 0\rangle, \quad |1\rangle_3 \equiv |0, 0, 1\rangle, \quad |2\rangle_3 \equiv |0, 1, 0\rangle, \quad |3\rangle_3 \equiv |0, 1, 1\rangle,$$

$$|4\rangle_3 \equiv |1, 0, 0\rangle, \quad |5\rangle_3 \equiv |1, 0, 1\rangle, \quad |6\rangle_3 \equiv |1, 1, 0\rangle, \quad |7\rangle_3 \equiv |1, 1, 1\rangle.$$

При использовании матричных обозначений для векторов состояний, аналогичных (5.30)–(5.32), базисные векторы представляют собой вектор-столбцы, содержащие восемь компонент. В этом случае гейт Тоффоли является матрицей размерности 8×8 вида

$$\text{CCNOT} \equiv \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \quad (5.38)$$

Как и для квантового гейта CNOT, квантовый гейт CCNOT определён для базисных однокубитовых состояний по каждой линии. То есть на его вход подаётся трёхкубитовый регистр в базисных однокубитовых состояниях. Для произвольного трёхкубитового состояния $\sum_{ijk} \lambda_{ijk} |i, j, k\rangle$, где $i, j, k \in 0, 1$, а λ_{ijk} – коэффициенты, определяющие амплитуды состояний в регистре. Действие CCNOT в алгебраических обозначениях определяется выражением

$$\text{CCNOT} : \sum_{ijk=0,1} \lambda_{ijk} |i, j, k\rangle = \sum_{ijk=0,1} \lambda_{ijk} |i, j, i \wedge j \oplus k\rangle. \quad (5.39)$$

В теории квантовых вычислений доказывается утверждение о том, что однокубитовые гейты, CNOT-гейт и CCNOT-гейт являются универсальными, т. е. из них можно образовать логические квантовые “цепи” для проведения квантовых операций с кубитами. Например, цепь из последовательности двух операторов CNOT представлена на рис. 5.6 (где $i, j \in 0, 1$).

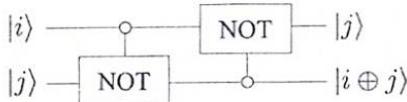


Рис. 5.6. Пример квантовой цепи из двух операторов CNOT

В цепях такого типа для корректного написания алгебраических выражений требуется явно указать у символа гейта индекс (номер) управляющей и управляемой линий. В результате алгебраическое выражение для цепи из рис. 5.6 можно записать в виде

$$\begin{aligned} \text{CNOT}_{2,1} : \text{CNOT}_{1,2} : |i, j\rangle &= \text{CNOT}_{2,1} : |i, i \oplus j\rangle = \\ &= |i \oplus (i \oplus j), i \oplus j\rangle = |j, i \oplus j\rangle. \end{aligned} \quad (5.40)$$

В представленной нотации имеется в виду указание того, что при действии первого оператора $\text{CNOT}_{1,2}$ на двухкубитовый вектор $|i, j\rangle$ первое однокубитовое состояние i определяет управляющий кубит, а второе j — управляемый. Соответственно, в обозначении $\text{CNOT}_{2,1}|a, b\rangle$ кубит b является управляющим, а кубит a — управляемым.

На рис. 5.7 представлена квантовая цепь (логическая диаграмма), осуществляющая обмен базисными однокубитовыми состояниями в двухкубитовом регистре (здесь $i, j \in 0, 1$).

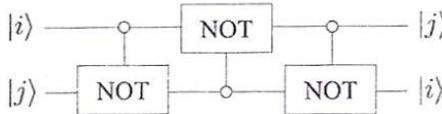


Рис. 5.7. Пример квантовой цепи из трёх операторов CNOT

Символическая последовательность преобразования кубит в однокубитовом базисе в данной цепи трёх преобразований двухкубитового регистра имеет вид

$$\begin{aligned} |i, j\rangle &\rightarrow |i, i \oplus j\rangle \\ &\rightarrow |i \oplus (i \oplus j), i \oplus j\rangle = |j, i \oplus j\rangle \\ &\rightarrow |j, (i \oplus j) \oplus j\rangle = |j, i\rangle. \end{aligned} \quad (5.41)$$

Для произвольного двухкубитового состояния $|q\rangle_{in} = \sum_{ij} \lambda_{ij} |i, j\rangle$ на входе цепи, изображённой на рис. 5.7, алгебраическая запись последова-

тельности трёх представленных преобразований есть

$$\begin{aligned}
 \text{CNOT}_{1,2} : \text{CNOT}_{2,1} : \text{CNOT}_{1,2} : & \sum_{ij \in 0,1} \lambda_{ij} |i, j\rangle = \\
 & = \text{CNOT}_{1,2} : \text{CNOT}_{2,1} : \sum_{ij \in 0,1} \lambda_{ij} |i, i \oplus j\rangle = \\
 & = \text{CNOT}_{1,2} : \sum_{ij \in 0,1} \lambda_{ij} |i \oplus (i \oplus j), i \oplus j\rangle = \\
 & = \text{CNOT}_{1,2} : \sum_{ij \in 0,1} \lambda_{ij} |j, i \oplus j\rangle = \\
 & = \sum_{ij \in 0,1} \lambda_{ij} |j, j \oplus (i \oplus j)\rangle = \sum_{ij \in 0,1} \lambda_{ij} |j, i\rangle .
 \end{aligned} \tag{5.42}$$

В целом, оператор (гейт), осуществляющий обмен кубит, называется SWAP-гейт и обозначается в квантовой цепи двухкубитового регистра, как показано на рис. 5.8.

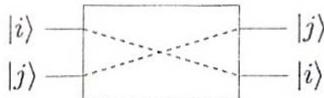


Рис. 5.8. Оператор обмена пары кубит SWAP

В алгебраических обозначениях двухкубитовый SWAP-гейт осуществляет преобразования вида

$$\text{SWAP}_2 : |k_1, k_2\rangle = |k_2, k_1\rangle . \tag{5.43}$$

Таким образом, цепь, представленная на рис. 5.7, — это и есть SWAP_2 -гейт. В матричном виде двухкубитовый SWAP_2 -гейт имеет вид

$$\text{SWAP}_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} . \tag{5.44}$$

Алгебраическое выражение для трёхкубитового преобразования SWAP в регистре трёх кубит имеет следующий вид:

$$\text{SWAP}_3 : |k_1, k_2, k_3\rangle = |k_3, k_2, k_1\rangle .$$

Соответственно, в матричном представлении матрица такого преобразования есть

$$\text{SWAP}_3 \equiv \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \quad (5.45)$$

В общем случае многокубитовый SWAP_n -гейт по определению осуществляет следующую перестановку (рис. 5.9):

$$\text{SWAP}_n : |k_1, k_2, k_3 \dots k_{n-1}, k_n\rangle = |k_n, k_{n-1} \dots k_3, k_2, k_1\rangle.$$

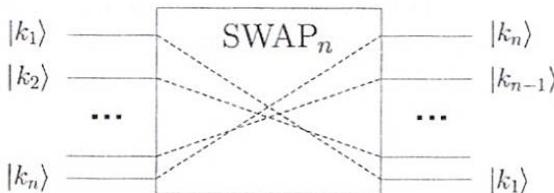


Рис. 5.9. Многокубитовый оператор SWAP_n

Необходимой операцией в цепи преобразований кубита является операция измерения его состояния. Такая операция обычно отображается на рисунках, как, например, на рис. 5.10.

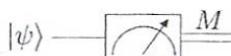


Рис. 5.10. Измерение однокубитового состояния $|\psi\rangle$

Операция измерения кубита $|\psi\rangle = a|0\rangle + b|1\rangle$ преобразует его состояние в одно из возможных базисных состояний $|0\rangle$ или $|1\rangle$, которые моделируют классический бит информации M (изображаемый на выходе двойной линией). При этом $M = 0$ с вероятностью $|a|^2$ и $M = 1$ с вероятностью $|b|^2$.

Упражнение 5.7. Показать, что матричное представление гейта Тоффоли определяется матрицей вида (5.38).

Упражнение 5.8. Вычислить результат действия цепи (рис. 5.6), если на её вход подано произвольное двухкубитовое состояние.

Упражнение 5.9. Показать, что матричное представление оператора SWAP_3 имеет вид (5.45).

5.6 Невозможность клонирования кубита

CNOT-гейт позволяет продемонстрировать фундаментальное свойство теории квантовой информации, состоящее в невозможности произвести простое копирование кубита. Известно, что копирование классического бита информации может быть выполнено с использованием классического CNOT-гейта (рис. 5.11), если на вход контролируемой линии подать бит ноль, а на вход контролирующей линии – бит, предназначенный для копирования:

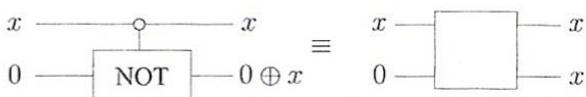


Рис. 5.11. Диаграмма копирования классического бита информации

В квантовом случае для произвольного кубита $|\psi\rangle = a|0\rangle + b|1\rangle$, данного на управляющую линию, и кубита в базисном состоянии $|0\rangle$ на управляемой линии квантового оператора CNOT результат принципиально отличается от классического случая. Если на вход квантового оператора CNOT подано двухкубитовое состояние $|\psi\rangle \otimes |0\rangle$ (рис. 5.12), то на выходе образуется не копия состояния $|\psi\rangle$, а суперпозиция двухкубитовых состояний вида $|0,0\rangle + b|1,1\rangle$ [9].

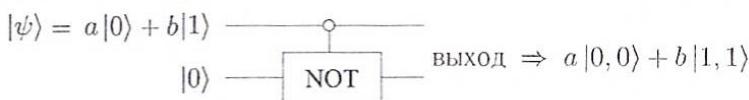


Рис. 5.12. Диаграмма преобразования состояния $|\psi\rangle \otimes |0\rangle$

Действительно, начальное двухкубитовое состояние, которое подаётся на вход квантового гейта CNOT, является суперпозицией состояний и имеет вид

$$\begin{aligned} |\psi\rangle \otimes |0\rangle &= \{a|0\rangle + b|1\rangle\} \otimes |0\rangle = a|0\rangle \otimes |0\rangle + b|1\rangle \otimes |0\rangle = \\ &= a|0,0\rangle + b|1,0\rangle. \end{aligned} \quad (5.46)$$

А так как квантовый гейт CNOT не преобразует состояние контролируемого кубита $|0\rangle$, если состояние контролирующего кубита совпадает с $|0\rangle$, и переворачивает состояние контролируемого кубита при состоянии контролирующего кубита, равного $|1\rangle$, то для слагаемых в суперпозиции (5.46) результат действия квантового CNOT даёт:

$$\text{CNOT : } a|0,0\rangle = a|0,0\rangle; \quad \text{CNOT : } b|1,0\rangle = b|1,1\rangle. \quad (5.47)$$

Таким образом, находим окончательно:

$$\text{CNOT} : |\psi\rangle \otimes |0\rangle = \text{CNOT} : |\psi, 0\rangle = a|0, 0\rangle + b|1, 1\rangle. \quad (5.48)$$

Как видно, результат на выходе гейта не является произведением состояний $|\psi\rangle \otimes |\psi\rangle$, за исключением тривиального случая $a = 0, b = 1$, когда на вход контролирующего кубита подаётся базисное состояние $|\psi\rangle = |1\rangle$. Прямое произведение состояний $|\psi\rangle \otimes |\psi\rangle$ по определению есть

$$|\psi\rangle \otimes |\psi\rangle = a^2|0, 0\rangle + a \cdot b|0, 1\rangle + a \cdot b|1, 0\rangle + b^2|1, 1\rangle, \quad (5.49)$$

что не совпадает с выражением (5.48). Другими словами, цепь, создающая копию классического бита, в квантовом случае не создаёт копию кубита. Фактически утверждение о невозможности создания копии кубита является фундаментальным для квантовой теории и не зависит от выбора цепи вентилей. Общее свойство невозможности копирования кубита известно в квантовой теории информации как *теорема о неклонируемости кубита* (no-cloning theorem).

5.7 Состояния Белла

Анализ различных суперпозиций двухкубитовых состояний демонстрирует проявление их необычных свойств с точки зрения классической теории и даже вызвавших дискуссию о применимости и интерпретации квантовой теории в период ее становления. Рассмотрим квантовую цепь, состоящую из однокубитового гейта Адамара H и двухкубитового квантового CNOT-гейта, определённую на рис. 5.13.

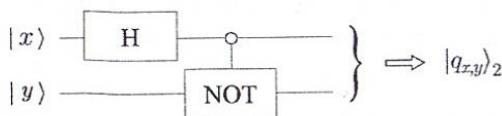


Рис. 5.13. Логическая диаграмма формирования квантовых состояний Белла

Вычислим результат действия такой цепи квантовых вентилей на четыре возможных базисных набора двухкубитовых состояний $|x, y\rangle : |0, 0\rangle, |0, 1\rangle, |1, 0\rangle, |1, 1\rangle$.

Например, после действия гейта Адамара H на $|x, y\rangle = |0, 0\rangle \equiv |0\rangle_2$ на выходе будем иметь следующее двухкубитовое состояние:

$$H : |0\rangle_2 = (|0\rangle + |1\rangle) \otimes |0\rangle / \sqrt{2} = (|00\rangle + |10\rangle) / \sqrt{2}.$$

Данное двухкубитовое состояние является исходным для квантового гейта CNOT, после действия которого получим двухкубитовое состояние вида $(|0, 0\rangle + |1, 1\rangle)/\sqrt{2}$, которое является результирующим для всей цепи. Удивительной особенностью этого результирующего двухкубитового состояния является утверждение, вытекающее из постулата об измерении. Если измерение состояния первого кубита даёт результат $|0\rangle$, то второй кубит также оказывается в состоянии $|0\rangle$. Соответственно, если при измерении состояния первого кубита получен результат $|1\rangle$, то это означает, что второй кубит также находится в состоянии $|1\rangle$, т. е. между кубитами существует связь. При этом показано, что даже если кубиты разнесены на некоторое расстояние друг от друга, эта связь проявляется экспериментально.

Для всех четырёх базисных двухкубитовых начальных состояний можно записать квантовый аналог таблицы истинности для цепи Белла:

Вход	Выход
$ 0, 0\rangle \equiv 0\rangle_2$	$(0, 0\rangle + 1, 1\rangle)/\sqrt{2} \equiv q_{00}\rangle_2$
$ 0, 1\rangle \equiv 1\rangle_2$	$(0, 1\rangle + 1, 0\rangle)/\sqrt{2} \equiv q_{01}\rangle_2$
$ 1, 0\rangle \equiv 2\rangle_2$	$(0, 0\rangle - 1, 1\rangle)/\sqrt{2} \equiv q_{10}\rangle_2$
$ 1, 1\rangle \equiv 3\rangle_2$	$(0, 1\rangle - 1, 0\rangle)/\sqrt{2} \equiv q_{11}\rangle_2$

Двухкубитовые состояния $|q_{i,j}\rangle_2$, $i, j \in 0, 1$ называются *состояниями Белла* или *EPR-парами* (EPR=Einstein-Podolsky-Rosen). Сокращенно эти состояния можно записать в виде

$$|q_{i,j}\rangle_2 \equiv \frac{|0, j\rangle + (-1)^i |1, \text{NOT } j\rangle}{\sqrt{2}}. \quad (5.50)$$

Состояния Белла (5.50) образуют ортонормированное множество состояний, $\langle q_{i,j} | q_{l,m} \rangle_2 = \delta_{il}\delta_{jm}$, что равносильно тому, что они однозначно различимы.

При создании квантовой теории такие состояния послужили причиной возникновения критики квантовой теории. Например, Эйнштейном, который так и не принял принципы квантовой теории, наличие такой квантовой связи интерпретировалось как нарушение *принципа ограниченности скорости передачи сигнала величиной скорости света*. Первоначально проявление эффекта квантовой связи между кубитами после измерения первого кубита интерпретировалось как мгновенный процесс. Исследованию такого рода состояний в квантовой теории в связи с этим уделено большое внимание. В настоящее время это явление экспериментально подтверждено и находится в согласии с фундаментальными физи-

ческими принципами, включая принцип ограниченности скорости передачи информации. В общем случае состояния, аналогичные рассмотренному, как в системах из двух кубит, так и в системах с произвольным числом кубит получили наименование *запутанных* (или *перепутанных*) состояний, а само явление – *перепутанность*, или *запутывание*.

Перепутанные пары можно обобщить до перепутанных кубит с произвольным числом кубит. Например, перепутанные состояния трёх кубит вида

$$|q\rangle_3 = \frac{|0, 0, 0\rangle + |1, 1, 1\rangle}{\sqrt{2}} \quad (5.51)$$

принято называть “состояниями Гринберга – Хорна – Цайлингера” или сокращённо ГХЦ-состояниями. Квантовая цепь, приводящая к такому перепутанному трёхкубитовому состоянию, может быть представлена последовательностью логических операторов в виде

$$|q\rangle_3 = \text{CNOT}_{1,3} : \text{CNOT}_{1,2} : H_1 : |0, 0, 0\rangle.$$

Здесь использовано обобщение оператора $\text{CNOT}_{i,j}$ путём явного указания номеров кубит, участвующих в процессе преобразования. Обобщение необходимо для определения цепи в многокубитовой системе. Так, первый индекс i указывает на номер контролирующего кубита, а второй индекс j – на номер контролируемого кубита. Соответственно, H_i – гейт Адамара, применённый к i -му кубиту. Графически квантовая цепь, приводящая к состоянию трёх кубит (5.51), есть цепь, представленная на рис. 5.14.

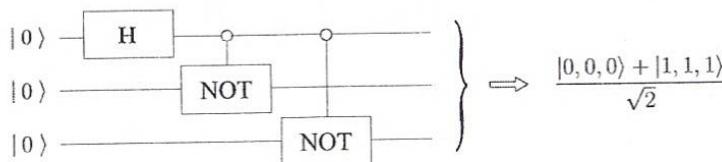


Рис. 5.14. Логическая диаграмма для построения ГХЦ-состояний

Любая квантовая система находится в контакте с окружающей средой, квантовое состояние которой может меняться случайным образом. Так как квантовый регистр вместе с внешней средой образуют систему, для которой справедливы постулаты квантовой теории, то реально возникает перепутанность квантового регистра и внешней среды. Эта перепутанность случайным образом меняет квантовый регистр. Данное явление, по сути, разрушающее квантовое состояние регистра, называется *декогеренцией* и является серьезной проблемой для реализации квантовых компьютеров. Даже существует мнение, что из-за декогеренции состояний кванто-

вого регистра создание масштабного квантового компьютера невозможно в принципе.

Упражнение 5.10. Определить все типы трёхкубитовых состояний, которые могут быть сгенерированы квантовой цепью, приводящей к ГХЦ-состояниям.

Упражнение 5.11. Составить квантовую цепь для построения четырёхкубитового запутанного состояния.

5.8 Декогеренция

Любая квантовая система (квантовый регистр, квантовые гейты) находится в контакте с окружающей средой. Окружающая среда осуществляет реальное воздействие на квантовые объекты. Даже если квантовая система помещена в изолированный объём, в котором создан “идеальный” вакуум, тепловое излучение стенок сосуда оказывает влияние на квантовую систему. С точки зрения квантовой теории квантовая система и окружающая среда в целом образуют замкнутую систему, для которой идеология квантовой механики остаётся справедливой. Но это значит, что изменение состояния окружающей среды некоторым образом влияет на состояние исследуемой квантовой системы. Перепутанность (запутанность) квантовой системы с окружающей средой хотя и незначительно при выполнении специальных условий, но случайным образом меняет систему с течением времени. Такое влияние приводит к явлению, которое называется *декогеренция квантового состояния*. Данное явление нежелательно для квантовых информационных систем, так как является причиной возникновения ошибок, неконтролируемого разрушения или изменения заданной суперпозиции квантового состояния и существенно препятствует созданию реальных квантовых информационных систем или реализации квантовых алгоритмов.

Для демонстрации эффекта декогерентности рассмотрим простейший случай влияния окружающей среды на квантовый интерферометр (5.16). Исходное состояние квантовой системы, как и раньше, есть $|0\rangle$, а начальное состояние окружающей среды обозначим через $|U\rangle$. После прохождения кубита через гейт Адамара H и фазовращатель $P(\phi_1, \phi_2)$ состояние целой системы кубит – окружающая среда имеет вид [7]:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}} \left[e^{i\phi_1} |0\rangle + e^{i\phi_2} |1\rangle \right] \otimes |U\rangle .$$

Пусть далее в окружающей среде происходят изменения, случайным об-

разом приводящие данную суперпозицию к виду

$$|\psi_2\rangle = \frac{1}{\sqrt{2}} \left[e^{i\phi_1} |0\rangle \otimes |U_0\rangle + e^{i\phi_2} |1\rangle \otimes |U_1\rangle \right].$$

Здесь $|U_0\rangle$ и $|U_1\rangle$ – некоторые (в общем случае неортогональные) состояния окружающей среды. Последующее действие гейта Адамара осуществляет интерференцию состояний возникшей суперпозиции, что приводит к следующему результату для целой системы:

$$\begin{aligned} |\psi_3\rangle &= H : |\psi_2\rangle = \\ &= \frac{1}{2} \left[e^{i\phi_1} |0\rangle \otimes |U_0\rangle + e^{i\phi_1} |1\rangle \otimes |U_0\rangle + e^{i\phi_2} |0\rangle \otimes |U_1\rangle - e^{i\phi_2} |1\rangle \otimes |U_1\rangle \right] = \\ &= \frac{1}{2} e^{i\Delta} \left\{ [e^{i\delta} |U_0\rangle + e^{-i\delta} |U_1\rangle] \otimes |0\rangle + [e^{i\delta} |U_0\rangle - e^{-i\delta} |U_1\rangle] \otimes |1\rangle \right\}, \end{aligned}$$

где $\Delta \equiv (\phi_1 + \phi_2)/2$ и $\delta \equiv (\phi_1 - \phi_2)/2$. Определение вероятности того, что в результате измерения будет получено одно из состояний кубита $|0\rangle$ или $|1\rangle$, сопряжено с необходимостью учёта возможной неортогональности состояний окружающей среды $|U_0\rangle$ и $|U_1\rangle$. С этой целью выразим вектор состояния $|U_1\rangle$ в виде суперпозиции векторов по “направлению” вектора $|U_0\rangle$ и по “направлению”, ортогональному $|U_0\rangle$.

Вспомним элементарные соотношения из трёхмерной векторной алгебры. Пусть имеется два вектора \vec{a} и \vec{b} . Представим вектор \vec{b} в виде векторной суммы вектора \vec{b}_{\parallel} , параллельного вектору \vec{a} , и вектора \vec{b}_{\perp} , ортогонального \vec{a} . При этом очевидно, что

$$\vec{b}_{\parallel} = (\vec{a} \cdot \vec{b}) \frac{\vec{a}}{|\vec{a}|}; \quad |\vec{b}_{\perp}| = \sqrt{(\vec{b} - \vec{b}_{\parallel})^2} = \sqrt{b^2 - 2(\vec{b} \cdot \vec{a})^2 / |\vec{a}| + (\vec{b} \cdot \vec{a})^2}. \quad (5.52)$$

Для единичных векторов находим из (5.52), что $|\vec{b}_{\perp}| = \sqrt{1 - (\vec{a} \cdot \vec{b})^2}$.

Таким образом, так как состояния окружающей среды $|U_0\rangle$ и $|U_1\rangle$ – единичные векторы в пространстве состояний, находим:

$$|U_1\rangle = \langle U_0 | U_1 \rangle |U_0\rangle + \sqrt{1 - \langle U_0 | U_1 \rangle^2} |U_{\perp}\rangle.$$

Здесь $\langle U_0 | U_{\perp} \rangle = 0$. В результате вероятности измерения состояния $|0\rangle$ и $|1\rangle$ определяются выражениями

$$P_0 = \frac{1}{2} (1 + \langle U_0 | U_1 \rangle \cos(\delta)); \quad P_1 = \frac{1}{2} (1 - \langle U_0 | U_1 \rangle \cos(\delta)).$$

Данные выражения отличаются множителем $\langle U_0 | U_1 \rangle$ перед косинусом от выражений (5.21), найденных для идеального интерферометра, не взаимодействующего с окружающей средой. При этом очевидно, что если выполняется условие $\langle U_0 | U_1 \rangle = 1$, т. е. два состояния окружающей среды с

точки зрения квантовой теории равны, то запутанность кубита со средой отсутствует и интерферометр приводит к строго определённому результату, т. е. интерферометр работает детерминированно. Если же $\langle U_0 | U_1 \rangle = 0$, возникает максимальная запутанность состояния кубита с окружающей средой и результат измерения оказывается полностью случайным. Соответственно, промежуточные значения $\langle U_0 | U_1 \rangle$ приводят к случайным изменениям результата работы интерферометра, которые могут оказаться большими или маленькими в зависимости от изменения состояния окружающей среды (Вселенной).

Строгая теория декогерентности квантовых состояний опирается на теорию матрицы плотности и в данном изложении не приводится.

5.9 Квантовый параллелизм

Квантовый параллелизм – это фундаментальное свойство квантовых вычислений. Данное свойство позволяет квантовым компьютерам вычислять функцию $f(x)$ для различных значений x одновременно.

Для иллюстрации квантового параллелизма рассмотрим функцию f от битовой переменной x , результатом вычисления которой также является битовое значение

$$f(x) : \{0, 1\} \rightarrow \{0, 1\}. \quad (5.53)$$

Приемлемый способ вычисления этой функции на квантовом компьютере – это рассмотрение двухкубитового квантового компьютера, который оперирует с состоянием $|x, y\rangle$. Используя соответствующую последовательность логических гейтов, можно преобразовать исходное состояние $|x, y\rangle$ в состояние $|x, y \oplus f(x)\rangle$. Здесь можно сказать, что x, y – регистры квантового компьютера. При этом первый регистр обычно называется *регистром данных*, а второй – *регистром результата*. Положим, что преобразование $|x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$ осуществляется некоторым унитарным преобразованием U . В теории мы можем рассматривать U как некий “чёрный ящик”, не вдаваясь в его физическую реализацию (рис. 5.15).

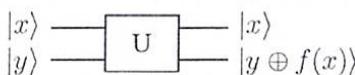


Рис. 5.15. Логическая диаграмма унитарного U -преобразования

Как следует из заданного преобразования, если $y = 0$, то

$$U : |x, 0\rangle \rightarrow |x, f(x)\rangle. \quad (5.54)$$

То есть в этом случае результирующее состояние контролируемого кубита совпадает со значением вычисляемой бинарной функции $f(x)$.

Рассмотрим для примера квантовую цепь рис. 5.16, которая действует на входное двухкубитовое состояние, содержащее равновероятную суперпозицию базовых состояний на линии контролирующего кубита (или регистра данных) и базисное однокубитовое состояние $|0\rangle$ на линии контролируемого кубита (или регистра результата).

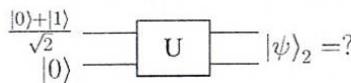


Рис. 5.16. Диаграмма U-преобразования для заданного исходного состояния

То есть на регистр данных ($|x\rangle$) попадает суперпозиция $(|0\rangle + |1\rangle)/\sqrt{2}$, которая может быть создана действием гейта Адамара на кубит данных $|0\rangle$. В результате действия "чёрного ящика" U результирующее состояние $|\psi\rangle_2$ будет иметь вид суперпозиции, указанной на рис. 5.17.

$$\frac{|0\rangle+|1\rangle}{\sqrt{2}} \xrightarrow{|0\rangle} |0\rangle \xrightarrow{\text{U}} |\psi\rangle_2 = \frac{|0, f(0)\rangle}{\sqrt{2}} + \frac{|1, f(1)\rangle}{\sqrt{2}}$$

Рис. 5.17. Результат U-преобразования для заданного исходного состояния

В данном результирующем состоянии представленные слагаемые содержат информацию как о значении $f(0)$, так и о значении $f(1)$. Фактически это соответствует вычислению функции $f(x)$ для двух значений аргумента x одновременно. Это свойство и обозначается в квантовых вычислениях как "квантовый параллелизм". В отличие от организации параллельных вычислений в классических компьютерах, когда технически создается несколько параллельных цепей, производящих вычисления одновременно, в квантовом компьютере это осуществляется в одной цепи на суперпозиции состояний.

Данная процедура вычисления может быть легко обобщена для функции от произвольного числа бит, если в качестве набора данных выбрать квантовый регистр из n кубит. Для перехода к многокубитовым состояниям введём преобразование, получившее наименование преобразование Уолша – Адамара (Walsh – Hadamard). Оно представляет собой прямое произведение n однокубитовых операторов Адамара:

$$\hat{W}^{(n)} \equiv H_1 \otimes H_2 \otimes H_3 \otimes \cdots \otimes H_n. \quad (5.55)$$

Данный оператор действует параллельно на n -кубит. Например, в случае $n = 2$ при действии на кубиты в начальном состоянии $|0\rangle_2 = |0, 0\rangle$ получим

$$\begin{array}{c} |0\rangle \xrightarrow{\boxed{H}} |0\rangle \\ |0\rangle \xrightarrow{\boxed{H}} |0\rangle \end{array} \quad |\psi\rangle_2 \equiv \frac{|0\rangle + |1\rangle}{\sqrt{2}} \cdot \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{|0, 0\rangle + |0, 1\rangle + |1, 0\rangle + |1, 1\rangle}{2}. \quad (5.56)$$

В общем случае результат действия гейта Уолша – Адамара на n штук кубитов, первоначально находящихся в выделенном базисном n -кубитовом состоянии $|0\rangle_n = |0, 0, \dots, 0, 0\rangle$, приводит к суперпозиции всех n -кубитовых базисных состояний $|k\rangle_n$:

$$\hat{W}^{(n)} : |0\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle_n. \quad (5.57)$$

В данном случае преобразование Уолша – Адамара производит суперпозицию всех базисных состояний с равной амплитудой. Напомним, что базисные состояния $|k\rangle_n$ определены следующим образом:

$$|0\rangle_n = |0, 0, \dots, 0, 0\rangle, \quad |1\rangle_n = |0, 0, \dots, 0, 1\rangle, \quad |2\rangle_n = |0, 0, \dots, 1, 0\rangle, \dots$$

В результате квантовые параллельные вычисления однобитовой функции $f(x)$ с n -битовым входом x могут быть построены следующим образом. Приготовим $n + 1$ -кубитовое состояние $|0\rangle_{n+1}$ на входе. Применим преобразование Уолша – Адамара к первым n -кубитам с последующим применением определённого ранее преобразования U . В результате получим состояние

$$U : \hat{W}^{(n)} : |0\rangle_{n+1} \rightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle_n \otimes |f(x)\rangle. \quad (5.58)$$

В определённом смысле квантовый параллелизм способен вычислить возможные значения функции f одновременно для всех значений x , хотя оператор U применяется только один раз. Однако такой параллелизм оказывается не очень полезным.

Действительно, в рассмотренном двухкубитовом примере (рис. 5.17) измерение состояния даст либо состояние $|0, f(0)\rangle$, либо $|1, f(1)\rangle$. Аналогично в общем случае измерение состояния $\sum_x |x, f(x)\rangle$ может дать только $f(x)$ для одного значения x . Конечно, и классический компьютер всё это делает без труда. Таким образом, квантовые вычисления должны приводить к результату, более значительному, чем параллелизм, указанный

выше. Необходимо извлекать информацию о более чем одном значении функции $f(x)$ из суперпозиции состояний, подобной $\sum_x |x, f(x)\rangle$. Такая задача решается при построении специальных квантовых алгоритмов.

Для полноты изложения ниже приводится результат действия оператора Уолша — Адамара на произвольное начальное n -кубитовое базисное состояние $|i\rangle_n$ (отметим, что выше был приведён результат действия оператора Уолша — Адамара только на многокубитовое базисное состояние $|0\rangle_n$). Например, таким произвольным n -кубитовым состоянием может быть состояние вида $|x\rangle \equiv \underbrace{|01011\dots\rangle}_n$) или аналогичное. В этом общем случае действие оператора $W^{(n)}$ на произвольное n -кубитовое состояние даёт следующий результат:

$$\hat{W}^{(n)} |i\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} (-1)^{i \cdot k} |k\rangle_n, \quad (5.59)$$

где i, k — битовые последовательности, определяющие состояния регистров кубит:

$$|i\rangle_n = |i_0, i_1, i_2, \dots\rangle, \quad |k\rangle_n = |k_0, k_1, k_2, \dots\rangle, \quad i_m, k_l \in \{0, 1\};$$

$i \cdot k$ — их побитовое скалярное произведение по модулю 2, определяемое как

$$i \cdot k \equiv \sum_{m=0}^{2^n-1} (i_n \wedge k_m) = i_0 \cdot k_0 \oplus i_1 \cdot k_1 \oplus \dots \quad (5.60)$$

Упражнение 5.12. Вычислить результат действия последовательности операторов $\hat{W}^{(2)} \hat{H}_1 \hat{W}^{(2)}$ на двухкубитовый регистр в состоянии $|0\rangle_2$.

Упражнение 5.13. Вычислить результат действия оператора $\hat{W}^{(4)}$ на состояние $|5\rangle_4$.

Глава 6

Квантовые алгоритмы

6.1 Алгоритм Дойча (Deutsch)

Алгоритм Дойча [7], [8], [9] является примером квантового алгоритма, который позволяет использовать квантовый параллелизм и получить результат с использованием всех возможных значений функции, вычисленных за один цикл работы квантового компьютера. В этом смысле алгоритм сочетает квантовый параллелизм с квантово-механической интерференцией. Рассмотрим квантовую цепь, приведённую на рис. 6.1.

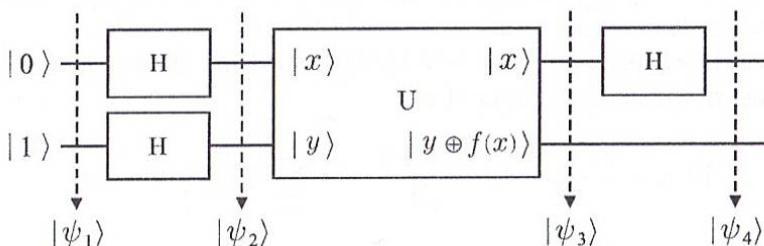


Рис. 6.1. Квантовая цепь алгоритма Дойча

Определённый в данной цепи унитарный оператор \hat{U} в общем случае действует на базисные двухкубитовые состояния $|k\rangle_2 = |k_1, k_2\rangle$ по правилу

$$\hat{U} : |k\rangle_2 \equiv \hat{U} : |k_1, k_2\rangle \rightarrow |k_1, k_2 \oplus f(k_1)\rangle, \quad k_1, k_2 \in 0, 1. \quad (6.1)$$

Здесь функция $f(k_1) \in 0, 1$ является битовой функцией от битового аргумента $k_1 \in 0, 1$. Результат действия оператора \hat{U} на двухкубитовое состояние $|k\rangle_2 = |k_1, k_2\rangle$, где $k_1, k_2 \in 0, 1$, можно представить в виде разложения по полному набору базисных двухкубитовых состояний $|n\rangle_2 = |n_1, n_2\rangle$, где

$n_1, n_2 \in \{0, 1\}$:

$$\hat{U} : |k\rangle_2 = \sum_{n=0}^3 b_n(k) |n\rangle_2 = \sum_{n_1, n_2=0,1} b_{n_1 n_2}(k_1, k_2) |n_1, n_2\rangle, \quad (6.2)$$

где

$$b_n(k) \equiv \langle n | \hat{U} | k \rangle \equiv b_{n_1 n_2}(k_1, k_2) = \langle n_1, n_2 | \hat{U} | k_1, k_2 \rangle. \quad (6.3)$$

Соответственно, вычисление матричного элемента $b_n(k)$ для произвольной битовой функции $f(x)$ от битового аргумента x даёт следующий общий результат:

$$b_n(k) = \langle n_1, n_2 | \hat{U} | k_1, k_2 \rangle = \langle n_2 | k_2 \oplus f(k_1) \rangle \delta_{n_1, k_1}. \quad (6.4)$$

Здесь δ_{n_1, k_1} — символ Кронекера, равный единице при $n_1 = k_1$ и нулю при $n_1 \neq k_1$.

В соответствии с цепью, представленной на рис. 6.1, исходное состояние цепи есть двухкубитовое состояние вида

$$|\psi_1\rangle_2 = |0, 1\rangle. \quad (6.5)$$

На первом этапе работы квантовой цепи, осуществляющей преобразование $|\psi_1\rangle_2 \rightarrow |\psi_2\rangle_2$, однокубитовые гейты Адамара приводят исходные кубиты в суперпозиции вида $(|0\rangle + |1\rangle)/\sqrt{2}$ и $(|0\rangle - |1\rangle)/\sqrt{2}$.

Таким образом, после действия операторов Адамара исходное двухкубитовое состояние будет иметь вид

$$|\psi_2\rangle_2 = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \equiv \frac{1}{2} \sum_{k=0}^1 |k\rangle \otimes (|0\rangle - |1\rangle). \quad (6.6)$$

В соответствии с определением (6.1) действие оператора \hat{U} на двухкубитовое состояние вида $|k\rangle \otimes (|0\rangle - |1\rangle)$ приводит к следующему результату:

$$\hat{U} [|k\rangle \otimes (|0\rangle - |1\rangle)] = \begin{cases} |0, 0 \oplus f(0)\rangle - |0, 1 \oplus f(0)\rangle, & \text{для } |k\rangle = 0; \\ |1, 0 \oplus f(1)\rangle - |1, 1 \oplus f(1)\rangle, & \text{для } |k\rangle = 1. \end{cases} \quad (6.7)$$

Функция $f(i)$ принимает значения 0 или 1 при значениях аргумента $i = 0, 1$. При $|k\rangle = |0\rangle$ вычисление выражения (6.7) с определёнными значениями функции f даёт следующий результат:

$$\hat{U} [|0\rangle \otimes (|0\rangle - |1\rangle)] = \begin{cases} |0, 0\rangle - |0, 1\rangle, & f(0) = 0 \\ |0, 1\rangle - |0, 0\rangle, & f(0) = 1 \end{cases} = (-1)^{f(0)} |0\rangle \otimes (|0\rangle - |1\rangle). \quad (6.8)$$

Соответственно, при $|k\rangle = |1\rangle$ из (6.7) для двух возможных значений функции f получим

$$\hat{U} \left[|1\rangle \otimes (|0\rangle - |1\rangle) \right] = \begin{cases} |1, 0\rangle - |1, 1\rangle, & f(1) = 0 \\ |1, 1\rangle - |1, 0\rangle, & f(1) = 1 \end{cases} = (-1)^{f(1)} |1\rangle \otimes (|0\rangle - |1\rangle). \quad (6.9)$$

Объединяя равенства (6.8) и (6.9), можно установить общее для них соотношение, справедливое при любых $|k\rangle \in |0\rangle, |1\rangle$:

$$\hat{U} \left[|k\rangle \otimes (|0\rangle - |1\rangle) \right] = (-1)^{f(k)} |k\rangle \otimes (|0\rangle - |1\rangle). \quad (6.10)$$

Таким образом, действия оператора \hat{U} на двухкубитовое состояние $|\psi_2\rangle_2$ из (6.6) преобразует это состояние в двухкубитовое состояние $|\psi_3\rangle_2$ вида

$$\hat{U} : |\psi_2\rangle_2 \rightarrow |\psi_3\rangle_2 = \frac{1}{2} \sum_{k=0}^1 (-1)^{f(k)} |k\rangle \otimes (|0\rangle - |1\rangle). \quad (6.11)$$

В общем случае функция $f(k)$ может оказаться либо постоянной функцией от своих двух битовых переменных $f(0) = f(1)$, либо функцией с разными битовыми значениями от двух разных битовых аргументов $f(0) \neq f(1)$. Поэтому выражение (6.11) можно переписать следующим образом:

$$|\psi_3\rangle_2 = (-1)^{f(0)} \cdot \begin{cases} (|0\rangle + |1\rangle)/\sqrt{2} \otimes (|0\rangle - |1\rangle)/\sqrt{2}, & \text{если } f(0) = f(1); \\ (|0\rangle - |1\rangle)/\sqrt{2} \otimes (|0\rangle - |1\rangle)/\sqrt{2}, & \text{если } f(0) \neq f(1). \end{cases} \quad (6.12)$$

Действуя в соответствии с квантовой цепью, приведённой на рис. 6.1, гейтом Адамара на первый кубит, находим из (6.12):

$$H_1 : |\psi_3\rangle_2 \rightarrow |\psi_4\rangle_2 = \begin{cases} (-1)^{f(0)} |0\rangle \otimes (|0\rangle - |1\rangle)/\sqrt{2}, & \text{если } f(0) = f(1); \\ (-1)^{f(0)} |1\rangle \otimes (|0\rangle - |1\rangle)/\sqrt{2}, & \text{если } f(0) \neq f(1). \end{cases} \quad (6.13)$$

Наконец, учитывая, что $f(0) \oplus f(1) = 0$, если функция постоянная, т. е. $f(0) = f(1)$, и $f(0) \oplus f(1) = 1$, если $f(0) \neq f(1)$, можно окончательно переписать выражение (6.13) в виде

$$|\psi_3\rangle_2 = (-1)^{f(0)} |f(0) \oplus f(1)\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \quad (6.14)$$

Последнее соотношение примечательно тем, что состояние одного из кубит определяется суммой двух возможных бинарных значений функции f .

Другими словами, данный кубит содержит информацию обо всех (их всего два) бинарных значениях функции f . Таким образом, измеряя состояние этого кубита, можно найти сумму всех (двух) значений данной битовой функции $f(0) \oplus f(1)$. То есть рассмотренная квантовая цепь даёт возможность определить *глобальное свойство* бинарной функции $f(x)$, используя только одно вычисление в представленной квантовой цепи. Формально это быстрее, чем достижение того же результата с использованием классического вычислительного устройства, которое потребует выполнения как минимум двух вычислений данной функции $f(0)$ и $f(1)$ с последующим сложением полученных результатов. Рассмотренный алгоритм может быть использован для решения задачи отнесения бинарной функции к определённому классу [14].

Пусть, например, имеется четыре устройства, выполняющих четыре разных преобразования, которые описываются четырьмя бинарными функциями $f_i(x)$, $i \in \{1, 2, 3, 4\}$ от двоичной переменной $x = 0, 1$. При этом функции f_1 и f_2 — постоянные и принимают значения $f_1(x) = 0$, $f_2(x) = 1$, а две другие функции f_3 и f_4 определены следующим образом: $f_3(x) = x$, $f_4(x) = \text{NOT}(x)$. При этом функции f_3 и f_4 называются сбалансированными. Требуется определить, к какой группе (постоянныe или сбалансированные) относится функция преобразования какого-то из этих четырёх устройств, если исходно это неизвестно.

Классическое решение такой задачи предполагает проведение как минимум двух операций вычисления $f(0)$ и $f(1)$ на выбранном устройстве. Если два последовательных вычисления дают один результат, то функция данного устройства относится к группе постоянных функций. В противном случае, если результаты различаются, — к группе сбалансированных функций. Квантовый алгоритм позволяет решить данную задачу (отнесение к группе) за одну операцию. Действительно, если состояние кубита, содержащего сумму $f(0) \oplus f(1)$, окажется совпадающим с состоянием $|0\rangle$, то функция относится к группе постоянных функций (без указания на значение этой постоянной). Если же состояние кубита квантовой цепи, содержащего сумму $f(0) \oplus f(1)$, окажется совпадающим с состоянием $|1\rangle$, то функция однозначно относится к группе сбалансированных функций (и снова без определения конкретного вида функции).

Конечно, такая примитивная задача не внушает большого оптимизма для объяснения преимуществ квантового компьютера и служит только для демонстрации одной важной идеи о том, что в квантовых системах могут быть реализованы состояния, идентификация которых основана на вычис-

лении всех значений исходной функции за один акт процедуры вычислений в квантовой цепи.

Если рассматривать приведённую на рис. 6.1 квантовую цепь как квантовый компьютер, то можно сказать, что квантовый компьютер работает как устройство, выполняющее определённую унитарную операцию. В квантовых вычислениях такое устройство принято рассматривать, не вдаваясь в описание его технической реализации. В данном примере унитарная операция вида (6.1) действует в пространстве четырёх базисных двухкубитовых состояний $|k\rangle_2$, и результат её действия на произвольное двухкубитовое состояние на основании (6.3) определяется матрицей следующего вида:

$$\hat{U}_f \rightarrow \begin{pmatrix} b_0(0) & b_1(0) & b_2(0) & b_3(0) \\ b_0(1) & b_1(1) & b_2(1) & b_3(1) \\ b_0(2) & b_1(2) & b_2(2) & b_3(2) \\ b_0(3) & b_1(3) & b_2(3) & b_3(3) \end{pmatrix}. \quad (6.15)$$

Исходя из вида двухкубитовых состояний $|\psi_1\rangle_2$ и $|\psi_2\rangle_2$ квантовой цепи, приведённой на рис. 6.1, четыре оператора \hat{U} , определяющих результат для рассмотренных четырёх функций $f_i(x), i \in 1, 2, 3, 4$, можно представить четырьмя матрицами размерности 4×4 . Так, для функций $f_1(x) = 0$ и $f_2(x) = 1$ на основании (6.4) получим [3]

$$\hat{U}_{f_1} \equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \equiv \hat{I}; \quad \hat{U}_{f_2} \equiv \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \equiv \hat{I} \otimes \text{NOT}. \quad (6.16)$$

Соответствующие квантовые цепи в этом случае имеют вид, изображённый на рис. 6.2.

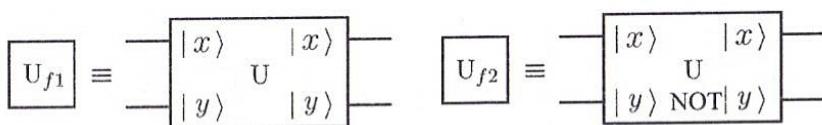


Рис. 6.2. Квантовые цепи операторов U_{f1} и U_{f2}

Аналогично для функций $f_3(x) = x$ и $f_4(x) = \text{NOT}(x)$ операторы определяются следующими матрицами в пространстве двухкубитовых состоя-

ний:

$$\hat{U}_{f_3} \equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \equiv \text{CNOT}; \quad \hat{U}_{f_4} \equiv \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \equiv \text{CNOT}(\hat{I} \otimes \text{NOT}). \quad (6.17)$$

Данным квантовым устройствам соответствуют квантовые цепи, представленные на рис. 6.3.

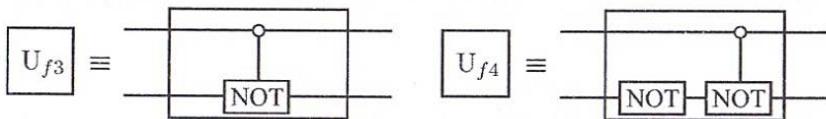


Рис. 6.3. Квантовые цепи операторов U_{f_3} и U_{f_4}

В заключение можно отметить, что данный алгоритм Дойча был реализован экспериментально на простейших ЯМР-квантовых компьютерах (ЯМР – ядерный магнитный резонанс) [3], что является прямым доказательством справедливости предложенной выше квантовой схемы вычислений и принципиально указывает на возможность использования преимуществ квантовых информационных систем.

6.2 Алгоритм Дойча – Джозса (Deutsch – Jozsa)

Данный алгоритм является обобщением алгоритма Дойча для случая, когда $|x\rangle$ являются векторами в 2^n -мерном базисном пространстве много-кубитовых состояний $|x\rangle_n = |x_0, x_1, \dots, x_{n-1}\rangle$, $x_i \in \{0, 1\}$, $|y\rangle$ – однокубитовое состояние, а унитарный оператор \hat{U} действует на $n + 1$ -мерный вектор состояния [15]. Квантовая цепь задачи представлена на рис. 6.4.

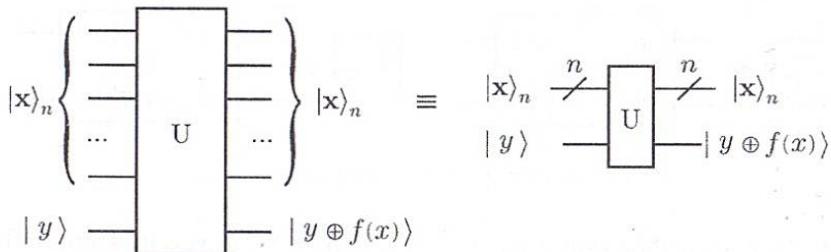


Рис. 6.4. Логическая диаграмма алгоритма Дойча – Джозса

Задача в данном случае формулируется подобно задаче Дойча и имеет целью определить, является ли бинарная функция $f(\mathbf{x})$, $f \in \{0, 1\}$, где \mathbf{x} — многомерный вектор, постоянной или сбалансированной. Под постоянством функции понимается выполнение равенств $f(\mathbf{x}) = 0$ или $f(\mathbf{x}) = 1$ при произвольных \mathbf{x} , а сбалансированность означает, что функция принимает значение 0 для одной половины данных \mathbf{x} и значение, равное 1, для другой половины данных \mathbf{x} . Квантовый алгоритм Дойча – Джозса позволяет решить эту задачу за n операций, тогда как классический алгоритм имеет решение только за 2^n операций.

Алгоритм может быть продемонстрирован на примере следующей задачи. Абонент А, находясь в некотором месте, выбирает произвольное число x из множества $0 \div 2^n - 1$ двоичных чисел и посыпает его по почте абоненту Б, находящемуся в другом месте. Абонент Б вычисляет некоторую функцию от полученного значения $f(x)$ и сообщает абоненту А результат вычислений, который может быть или 0, или 1, почтовым отправлением в адрес абонента А. При этом абонент Б имеет возможность использовать функцию $f(x)$, одну из двух типов. Либо $f(x)$ постоянна для всех значений x , либо $f(x)$ сбалансированна, при этом она равна 1 точно для половины всех возможных значений x и равна 0 для другой половины. Задача абонента А состоит в том, чтобы по полученной от абонента Б информации достоверно определить, затратив при этом минимум корреспонденции, какой тип функции выбран абонентом Б для вычислений.

В классическом случае А может послать Б только одно значение x в каждом письме. Поэтому абонент А будет вынужден запросить ответ у абонента Б по меньшей мере $2^n/2 + 1$ раз, так как теоретически А может получить $2^n/2$ нулей до получения значения, равного 1, объясняющего А, что абонент Б использует сбалансированную функцию. Поэтому для определения типа функции абонент А может применять классический алгоритм $2^n/2 + 1$ раз. Подчеркнём, что при использовании бинарной арифметики в каждом письме абонент А посыпает абоненту Б n бит информации x_0, x_1, \dots, x_n для представления числа.

Однако если абоненты А и Б могут обмениваться кубитами, абонент Б может вычислять $f(\mathbf{x})$, используя унитарное преобразование U_f , тогда абонент А может определить тип функции в унитарном преобразовании устройства абонента Б одной корреспонденцией, используя следующий алгоритм.

Пусть абонент А имеет n -кубитовый регистр, находящийся исходно в состоянии $|0\rangle_n$ для формирования двоичного представления числа своего запроса, и однокубитовый регистр в состоянии $|1\rangle$, который он представляет абоненту Б для размещения ответа. Абонент А приготавливает как регистр запроса, так и регистр ответа в состоянии суперпозиции в соответствии с квантовой цепью (рис. 6.5) и передаёт весь регистр кубит абоненту Б. Далее абонент Б проводит вычисление $f(x)$ с использованием унитарного преобразования \hat{U} , помещающего результат в регистр ответа, и передаёт все кубиты обратно абоненту А. Абонент А осуществляет преобразование состояний, используя гейт Адамара для регистра запроса, и заканчивает исследования путём проведения измерения с целью определения, является f постоянной функцией или сбалансированной.

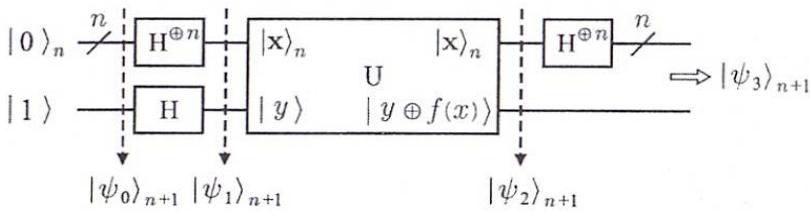


Рис. 6.5. Пошаговое выполнение алгоритма Дойча – Джозса

Пошаговое выполнение алгоритма, представленное квантовой цепью на рис. 6.5, состоит из последовательности операций над $n + 1$ кубитовым состоянием. Исходное $n + 1$ кубитовое состояние, приготовленное абонентом А, есть

$$|\psi_0\rangle_{n+1} = |0\rangle_n \otimes |1\rangle, \quad (6.18)$$

где регистр запроса определяется n -кубитовым регистром состояний, в котором каждый кубит находится в состоянии $|0\rangle$. После применения гейта Уолша – Адамара к кубитам регистра запроса и гейта Адамара к регистру ответа (в данном случае один кубит) возникнет состояние $|\psi_1\rangle_{n+1}$ вида

$$|\psi_1\rangle_{n+1} = \sum_{i=0}^{2^n-1} \frac{|i\rangle_n}{\sqrt{2^n}} \otimes \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]. \quad (6.19)$$

Здесь $|i\rangle_n \equiv |i_0, i_1, i_2, \dots, i_n\rangle$, $i_k \in \{0, 1\}$.

Регистр запроса теперь является суперпозицией всех значений x , от которых зависит функция $f(x)$, а регистр ответа находится в суперпозиции однокубитовых состояний $|0\rangle$ и $|1\rangle$. Данные кубиты передаются абоненту

Б для проведения вычислений. Вычисление функции f производится унитарным оператором \hat{U} :

$$\hat{U} : |\mathbf{x}, y\rangle_{n+1} \rightarrow |\mathbf{x}, y \oplus f(\mathbf{x})\rangle_{n+1}. \quad (6.20)$$

В результате образуется состояние $|\psi_2\rangle_{n+1}$ вида

$$|\psi_2\rangle_{n+1} = \hat{U} : |\psi_1\rangle_{n+1} = \sum_{i=0}^{2^n-1} \frac{(-1)^{f(i)} |i\rangle_n}{\sqrt{2^n}} \otimes \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]. \quad (6.21)$$

Вывод данного соотношения аналогичен выводу равенства (6.11), так как по определению оператора \hat{U} имеем

$$\hat{U} : |i\rangle_n \otimes \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] = |i_n, 0 \oplus f(i)\rangle_{n+1} - |i_n, 1 \oplus f(i)\rangle_{n+1}. \quad (6.22)$$

Например, для постоянной функции $f(i) = 0$ получим из (6.22)

$$\hat{U} : |i\rangle_n \otimes \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] = |i_n, 0\rangle_{n+1} - |i_n, 1\rangle_{n+1} = |i\rangle_n \otimes \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right], \quad (6.23)$$

что является частным случаем (6.21), так как $f(i) = 0$ и $(-1)^{f(i)} = 1$. Таким же образом для функции $f(i) = 1$ из (6.22) найдём

$$\hat{U} : |i\rangle_n \otimes \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] = |i_n, 1\rangle_{n+1} - |i_n, 0\rangle_{n+1} = -|i\rangle_n \otimes \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right], \quad (6.24)$$

так как в этом случае $-1 = (-1)^{f(i)}$, что также является частным случаем выражения (6.21). Аналогично можно получить результат (6.21) для сбалансированных функций.

Полученный в (6.21) регистр кубит передаётся назад абоненту А. Данный квантовый регистр содержит результат вычисления функции в амплитудах суперпозиции. Далее А использует интерференцию слагаемых в суперпозиции путём действия гейта Уолша – Адамара на регистр запроса. Используя полученный ранее результат (5.59), находим

$$W^{(n)} |i\rangle_n = W^{(n)} |i_0, \dots, i_{n-1}\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} (-1)^{i_0 \cdot k_0 + \dots + i_{n-1} \cdot k_{n-1}} |k_0, \dots, k_{n-1}\rangle, \quad (6.25)$$

что может быть записано в компактном виде:

$$W^{(n)} |i\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} (-1)^{i \cdot k} |k\rangle, \quad (6.26)$$

$i \cdot k$ – побитовое внутреннее произведение по модулю 2, где $i = (i_0, i_1, \dots)$ и $k = (k_0, k_1, \dots)$ ($i_l, k_m \in 0, 1$). Используя (6.26), можно записать результат вычисления состояния $|\psi_3\rangle_{n+1}$:

$$|\psi_3\rangle_{n+1} = \sum_{k=0}^{2^n-1} \left[\frac{1}{2^n} \sum_{i=0}^{2^n-1} (-1)^{i \cdot k + f(i)} \right] |k\rangle_n \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \sum_{k=0}^{2^n-1} A_k |k\rangle_n \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \quad (6.27)$$

Таким образом, в регистре запроса, состоящем из n кубит, сформирована суперпозиция n штук базисных состояний $|k\rangle_n \equiv |k_0, k_1, \dots, k_{n-1}\rangle$, амплитуды вероятностей которых равны

$$A_k = \frac{1}{2^n} \sum_{i=0}^{2^n-1} (-1)^{i \cdot k + f(i)}. \quad (6.28)$$

Теперь абонент А может исследовать регистр запроса, проводя его измерения, и определить тип функции, которую использовал абонент Б для вычислений. Так, если Б использовал постоянную функцию $f(x) = c$, $c \in 0, 1$, то амплитуда состояния $|0\rangle_n$ равна $+1$ или -1 в зависимости от значения константы $f = c$. Данное утверждение следует из (6.28), так как при $k = 0$ внутреннее побитовое произведение $i \cdot k = 0$ ($|0\rangle_n \equiv |0, 0, \dots, 0\rangle$, соответственно, вектор есть $|k\rangle_n \equiv |k_0, k_1, \dots, k_{n-1}\rangle$). Следовательно,

$$A_0 = \frac{1}{2^n} \sum_{i=0}^{2^n-1} (-1)^{0+c} = (-1)^c \frac{1}{2^n} \sum_{i=0}^{2^n-1} 1 = (-1)^c. \quad (6.29)$$

Так как состояние $|\psi_3\rangle_{n+1}$ имеет единичную длину, отсюда вытекает, что для всех других состояний амплитуды A_k , $k \in 1, 2, \dots, 2^n - 1$ равны 0 и измерение даст нулевые значения для всех остальных базисных кубит в регистре запроса.

Другими словами, при измерении регистра запроса с вероятностью, равной 1, при $f = \text{const}$ будет получаться состояние $|0\rangle_n = |0, 0, \dots, 0\rangle$. Если же f сбалансированна, тогда положительный и отрицательный вклады в амплитуду A_0 взаимно сокращаются, приводя амплитуду A_0 к нулевому значению. В результате проведённые измерения кубита запроса позволят абоненту А однозначно идентифицировать тип функции, использованный абонентом Б при вычислении.

Суммарно алгоритм Дойча – Джозса включает в себя следующее.

1. Наличие унитарного оператора \hat{U} , который выполняет преобразование $|x\rangle_n \otimes |y\rangle \rightarrow |x\rangle_n \otimes |y \oplus f(x)\rangle$ для $x \in \{0, \dots, 2^n - 1\}$ и $f(x) \in \{0, 1\}$.

Функция $f(x)$ — либо константа для всех x , либо сбалансированна, так что $f(x) = 1$ для половины значений x и $f(x) = 0$ для другой половины значений x .

2. Инициализацию $(n + 1)$ -кубитового регистра в состояние $|0\rangle_n \otimes |1\rangle$.
3. Создание суперпозиции с использованием гейтов Адамара:

$$\frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle_n \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

4. Вычисление функции f с использованием оператора \hat{U} :

$$\sum_i (-1)^{f(i)} |i\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

5. Преобразование Уолша — Адамара с регистром запроса:

$$\sum_i \sum_k \frac{1}{2^n} (-1)^{i \cdot k + f(i)} |k\rangle_n \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

6. Измерение регистра запроса $\rightarrow |k\rangle_n$ для получения ответа задачи.

6.3 Алгоритм Саймона

Алгоритм Саймона [8] сформулирован для решения задачи определения периода функции с использованием принципа интерференции квантовых состояний. Пусть есть двоичная функция $f : (0, 1)^n \rightarrow (0, 1)^n$, определённая на множестве двоичных векторов x . Функция является периодической в том смысле, что $f(x) = f(x \oplus r)$, где r — двоичный период. Путём вычисления функции найти период.

В рамках классических вычислений для решения такой задачи потребуется выполнить экспоненциальное (2^n) число вычислений такой функции для сравнения значений во всех её точках. Квантовый алгоритм Саймона позволяет найти период всего за $O(n)$ вычислительных процедур. Для получения такого результата определим унитарный оператор вычисления функции f стандартным образом:

$$\hat{U}_f : |x\rangle_n \otimes |y\rangle_n \rightarrow |x\rangle_n \otimes |y \oplus f(x)\rangle_n. \quad (6.30)$$

Квантовая цепь алгоритма Саймона приведена на рис. 6.6.

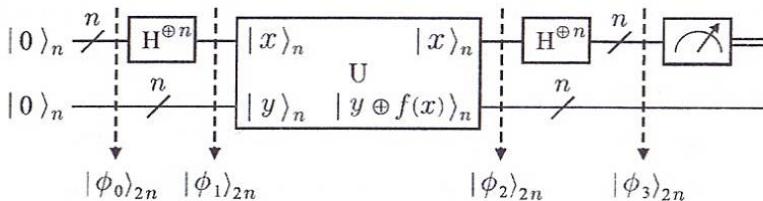


Рис. 6.6. Пошаговая логическая диаграмма алгоритма Саймона

Исходным квантовым состоянием в данном алгоритме является квантовый регистр, составленный из двух регистров $|x\rangle_n$ и $|y\rangle_n$ по n штук кубит каждый. При этом регистр $|x\rangle_n$ будем называть регистром данных, а регистр $|y\rangle_n$ – регистром результата. Оба регистра первоначально приведены в состояние $|0\rangle_n$. Таким образом, общий начальный регистр определяется $2n$ -кубитовым состоянием вида $|\phi_0\rangle_{2n} = |0\rangle_n \otimes |0\rangle_n$. Далее с регистром данных выполним преобразование Уолша – Адамара $W^{(n)}$, после чего система в целом переходит в состояние $|\phi_1\rangle_{2n}$, которое определяется выражением

$$|\phi_1\rangle_{2n} \equiv W^{(n)} \otimes I^{(n)} : |\phi_0\rangle_{2n} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle_n \otimes |0\rangle_n. \quad (6.31)$$

Здесь $I^{(n)}$ – единичный оператор. Данный регистр подаётся на унитарный оператор (гейт) \hat{U}_f (6.30), на выходе которого возникает $2n$ -кубитовый регистр $|\phi_2\rangle_{2n}$:

$$|\phi_2\rangle_{2n} \equiv \hat{U}_f : |\phi_1\rangle_{2n} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle_n \otimes |f(x)\rangle_n. \quad (6.32)$$

Несмотря на то что регистр $|\phi_2\rangle_{2n}$ в своей суперпозиции содержит все заданные аргументы x и все значения функций $f(x)$, воспользоваться этими значениями не удаётся в силу постулата об измерении квантового состояния. По этой причине рассматриваемый алгоритм Саймона предполагает выполнение последующего применения преобразования Уолша – Адамара с регистром данных, в результате чего возникает квантовая интерференция регистра данных и регистра результата, позволяющая сделать выводы о периоде функции $f(x)$:

$$|\phi_3\rangle_{2n} = W^{(n)} \otimes I^{(n)} : |\phi_2\rangle_{2n} = \frac{1}{2^n} \sum_{x'=0}^{2^n-1} \sum_{x=0}^{2^n-1} (-1)^{x' \cdot x} |x'\rangle_n \otimes |f(x)\rangle_n. \quad (6.33)$$

В соответствии с алгоритмом Саймона можно найти решение поставленной выше задачи и определить двоичный период заданной функции. Для этого необходимо выполнить анализ результатов измерения регистра данных $|x'\rangle$ в $|\phi_3\rangle_{2n}$ при проведении нескольких повторений вычислений в соответствии с цепью, представленной на рис. 6.6. Другими словами, повторяя некоторое число раз работу квантовой машины.

Для объяснения смысла сделанного утверждения рассмотрим выражение (6.33) более подробно. Если функция $f(x)$ имеет двоичный период r , то очевидно, что выражение (6.32) может быть тождественно переписано в виде

$$|\phi_2\rangle_{2n} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x \oplus r\rangle_n \otimes |f(x \oplus r)\rangle_n. \quad (6.34)$$

Складывая выражения (6.32) и (6.34) с учетом $f(x) = f(x \oplus r)$ и разделив результат пополам, получим эквивалентное (6.32) выражение для $2n$ -кубитового состояния $|\phi_2\rangle_{2n}$:

$$|\phi_2\rangle_{2n} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \frac{|x\rangle_n + |x \oplus r\rangle_n}{2} \otimes |f(x)\rangle_n. \quad (6.35)$$

Действуя гейтом Уолша – Адамара на регистр данных в (6.35), находим выражение, эквивалентное (6.33), в котором явно присутствует двоичный период $r = (r_0, r_1, r_2, \dots)$:

$$\begin{aligned} |\phi_3\rangle_{2n} &= W^{(n)} \otimes I^{(n)} : |\phi_2\rangle_{2n} = \\ &= \frac{1}{\sqrt{2^{n+2}}} \sum_{x=0}^{2^n-1} W^{(n)}(|x\rangle_n + |x \oplus r\rangle_n) \otimes |f(x)\rangle_n = \\ &= \frac{1}{2^{n+1}} \sum_{x'=0}^{2^n-1} \sum_{x=0}^{2^n-1} a_{x'x} |x'\rangle_n \otimes |f(x)\rangle_n. \end{aligned} \quad (6.36)$$

Здесь

$$a_{x'x} \equiv (-1)^{x \cdot x'} + (-1)^{(x \oplus r) \cdot x'}.$$

Так как амплитудный множитель $a_{x'x}$ равен

$$a_{x'x} = 2 \cdot (-1)^{x \cdot x'}, \quad \text{если } r \cdot x' = 0; \quad a_{x'x} = 0, \quad \text{если } r \cdot x' = 1,$$

то это означает, что при измерении регистра данных в $2n$ -кубитовом регистре $|\phi_3\rangle_{2n}$ могут быть с равной вероятностью обнаружены только такие n -кубитовые состояния $|x'\rangle_n$, для которых произведение $r \cdot x' = 0$. Обозначим эти состояния через $|x'_\alpha\rangle_n$.

Таким образом, алгоритм Саймона предполагает многократное, порядка n раз, вычисление по указанной выше цепи с последующим измерением регистра данных. Результат каждого из измерений обозначим $|x'_i\rangle_n$, где $i \in \{1, 2, 3, \dots\}$ — номер вычислений. Набор двоичных данных $|x'_i\rangle_n$, полученных в результате измерений регистра данных, позволяет построить систему уравнений для определения r , так как должно выполняться равенство

$$r \cdot x'_i = 0, \quad i = 1, 2, 3, \dots, N. \quad (6.37)$$

Здесь N — число повторений алгоритма Саймона, а $r \cdot x'_i$ — побитовое скалярное произведение векторов r и x'_i . Решение данной системы алгебраических уравнений, в которых бинарное значение r неизвестно, находится обычными классическими методами без привлечения квантовых цепей. В результате для определения периода функции потребуется линейное с n число повторений одной процедуры в сравнении с экспоненциально (степени n) большим числом вычисления функции в классическом случае.

Пример 6.1. Нахождение периода функции

В качестве простейшего примера рассмотрим случай, когда регистр данных и регистр результата являются двухкубитовыми регистрами. Следовательно, имеется только четыре базисных состояния в регистре данных: $|0\rangle_2 = |0, 0\rangle$, $|1\rangle_2 = |0, 1\rangle$, $|2\rangle_2 = |1, 0\rangle$, $|3\rangle_2 = |1, 1\rangle$. Соответственно, имеется четыре значения функции: $f(0) \equiv f(0, 0)$, $f(1) \equiv f(0, 1)$, $f(2) \equiv f(1, 0)$, $f(3) \equiv f(1, 1)$. В соответствии с (6.33) выпишем в явном виде суммы по $x, x' \in \{0, 1\}$:

$$\begin{aligned} |\phi_3\rangle_4 &= \frac{1}{2^2} \sum_{x'=0}^3 \sum_{x=0}^3 (-1)^{x' \cdot x} |x'\rangle_n \otimes |f(x)\rangle_n = \\ &= \frac{1}{4} [|0\rangle_2 + |1\rangle_2 + |2\rangle_2 + |3\rangle_2] \otimes |f(0)\rangle_2 + \\ &\quad + \frac{1}{4} [|0\rangle_2 - |1\rangle_2 + |2\rangle_2 - |3\rangle_2] \otimes |f(1)\rangle_2 + \\ &\quad + \frac{1}{4} [|0\rangle_2 + |1\rangle_2 - |2\rangle_2 - |3\rangle_2] \otimes |f(2)\rangle_2 + \\ &\quad + \frac{1}{4} [|0\rangle_2 - |1\rangle_2 - |2\rangle_2 + |3\rangle_2] \otimes |f(3)\rangle_2. \end{aligned} \quad (6.38)$$

Если функция f имеет двоичный период $r = 2 \rightarrow (1, 0)$, то $f(0) = f(2)$ и $f(1) = f(3)$. С учётом данного условия периодичности функции равенство

(6.38) можно представить в виде

$$\begin{aligned} |\phi_3\rangle_4 &= \frac{1}{2} [|0\rangle_2 + |1\rangle_2] \otimes |f(0)\rangle_2 + \frac{1}{2} [|0\rangle_2 - |1\rangle_2] \otimes |f(1)\rangle_2 = \\ &= |0\rangle_2 \otimes \frac{|f(0)\rangle_2 + |f(1)\rangle_2}{2} + |1\rangle_2 \otimes \frac{|f(0)\rangle_2 - |f(1)\rangle_2}{2}. \end{aligned}$$

Из последнего равенства видно, что при измерении регистра данных (после прохождения квантовой цепи Саймона) с равной вероятностью может быть получено либо только состояние $|0\rangle_2 = |0, 0\rangle$, либо $|1\rangle_2 = |0, 1\rangle$. Состояния $|2\rangle_2 = |1, 0\rangle$ и $|3\rangle_2 = |1, 1\rangle$ при измерении регистра данных для данной функции никогда не будут получены. При выполнении работы цепи несколько раз (в минимальном случае два раза) будут зафиксированы только два различных бинарных вектора $z_1 = (0, 0)$ и $z_2 = (0, 1)$ при измерении регистра результата. Минимальным числом испытаний является два, так как в произвольном случае один зафиксированный результат может повториться несколько раз. Таким образом, это означает, что в данном примере должно выполняться условие ортогональности бинарных векторов z_i и r , или $z_i \cdot r = 0, i \in 1, 2$. Так как $r = (r_0, r_1)$ – двоичный вектор и требуется определить $r_0, r_1 \in 0, 1$, то очевидно, что нетривиальным решением системы уравнений (6.37) может быть только вектор $r = (1, 0)$. Таким образом, найдено, что десятичный период функции равен $r = 2$.

Упражнение 6.1. Показать, что для трёхкубитового регистра данных и трёхкубитового регистра результата в цепи Саймона для функции, имеющей период, равный $r = 4 \rightarrow (1, 0, 0)$, $f(x) = f(x + r)$, в процессе измерения могут быть зафиксированы только следующие четыре из восьми возможных трёхкубитовые состояния: $|0\rangle_3 = |0, 0, 0\rangle$, $|1\rangle_3 = |0, 0, 1\rangle$, $|2\rangle_3 = |0, 1, 0\rangle$, $|3\rangle_3 = |0, 1, 1\rangle$.

Упражнение 6.2. Показать, что для трёхкубитового регистра данных и трёхкубитового регистра результата в процессе измерения в цепи Саймона для функции f , имеющей период $r = 2$, при измерении регистра данных могут быть получены только два трёхкубитовых состояния: $|0\rangle_3 = |0, 0, 0\rangle$ и $|1\rangle_3 = |0, 0, 1\rangle$.

Упражнение 6.3. Показать, что для трёхкубитового регистра данных и трёхкубитового регистра результата в процессе измерения в цепи Саймона для постоянной функции всегда будет получено только одно трёхкубитовое состояние $|0\rangle_3 = |0, 0, 0\rangle$.

Алгоритм Саймона может быть обобщён на случай, когда функция имеет несколько периодов или различное число кубит в регистрах данных и регистре результата.

6.4 Квантовое преобразование Фурье

Квантовое преобразование Фурье (КПФ) – аналог классического быстрого преобразования Фурье (БПФ), являющегося эффективной вычислительной реализацией так называемого дискретного преобразования Фурье (ДПФ). За счет квантового параллелизма квантовое преобразование Фурье выполняется экспоненциально быстрее в сравнении с классическим аналогом. Однако прямое использование данного преимущества невозможно, так как все вычисленные в суперпозиции коэффициенты Фурье в виде амплитуд вероятностей одновременно недоступны для измерения. Поэтому КПФ рассматривается в основном как структурный элемент в цепи преобразований различных сложных квантовых алгоритмов.

Классическое дискретное Фурье-преобразование обычно определяется как преобразование набора $(x_0, x_1, \dots, x_{N-1})$ N -комплексных чисел в набор комплексных чисел $(y_0, y_1, \dots, y_{N-1})$, определённых соотношением

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \exp \left(i \frac{2\pi}{N} k j \right) x_j, \quad i \equiv \sqrt{-1}, \quad k \in 0, 1, \dots, N-1. \quad (6.39)$$

Здесь и ниже i – это всегда мнимая единица. Данное выражение удобно представить следующим образом:

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} q^{k \cdot j} x_j, \quad q \equiv \exp \left(i \frac{2\pi}{N} \right), \quad k \in 0, 1, \dots, N-1. \quad (6.40)$$

Обратное преобразование Фурье имеет вид

$$x_m = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp \left(-i \frac{2\pi}{N} m k \right) y_k = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} (q^*)^{k \cdot m} y_k. \quad (6.41)$$

Дискретное Фурье-преобразование определяет связь между двумя векторами \mathbf{x}, \mathbf{y} , что обозначается в операторном виде как $\mathbf{y} = DFT(\mathbf{x})$ или $\mathbf{y} = \hat{F}(\mathbf{x})$. Оператор Фурье преобразования по определению унитарный: $\hat{F} = \hat{F}^\dagger$. Если рассматривать компоненты векторов \mathbf{x}, \mathbf{y} в виде столбцов, то оператор дискретного Фурье-преобразования может быть представлен в виде квадратной матрицы размерности $N \times N$, а само преобразование –

в следующей матричной форме:

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ \vdots \\ y_{N-1} \end{pmatrix} = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & q & q^2 & \dots & q^{(N-1)} \\ 1 & q^2 & q^4 & \dots & q^{2(N-1)} \\ \vdots & \dots & \dots & \ddots & \dots \\ 1 & q^{(N-1)} & q^{2(N-1)} & \dots & q^{(N-1)^2} \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_{N-1} \end{pmatrix}, \quad (6.42)$$

где $q \equiv \exp(i2\pi/N)$. Так как q^k — периодическая функция с периодом N , т. е. $q^k = q^{k+N}$, выражение (6.42) может быть упрощено, а матрица \hat{F} становится симметрической. Например, для $N = 4$ матрица Фурье-преобразования имеет следующий вид ($q \equiv \exp(i\pi/2) = i$):

$$\hat{F} = \frac{1}{\sqrt{4}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & q & q^2 & q^3 \\ 1 & q^2 & q^4 & q^6 \\ 1 & q^3 & q^6 & q^9 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & q & q^2 & q^3 \\ 1 & q^2 & 1 & q^2 \\ 1 & q^3 & q^2 & q \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}. \quad (6.43)$$

Квантовое Фурье-преобразование формально аналогично классическому, хотя обозначения для квантовых Фурье-преобразований несколько отличаются. Квантовое Фурье-преобразование ортонормированного, многокубитового базиса $|0\rangle_n, |1\rangle_n, \dots, |N-1\rangle_n$ определено как линейное преобразование базисных состояний в результате действия унитарного оператора Фурье-преобразования $\hat{F}|j\rangle_n$:

$$\hat{F}|j\rangle_n \equiv |\overline{j}\rangle_n = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp\left(i\frac{2\pi}{N}jk\right) |k\rangle_n = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} q^{jk} |k\rangle_n. \quad (6.44)$$

В последующем $N = 2^n$, где n — число кубит в регистре, а набор состояний $|0\rangle_n, \dots, |2^n-1\rangle_n$ — вычислительный базис для n -кубитового квантового регистра, представленный заданием десятичных чисел, нумерующих состояние. Так как для обозначения номера базисных состояний используются целые десятичные числа $k \in 0, 1, \dots, 2^n - 1$, а в двоичной системе эти векторы состояний определяются бинарной последовательностью ($|0\rangle_n = |0, 0, \dots, 0, 0\rangle_n, |1\rangle_n = |0, 0, \dots, 0, 1\rangle_n, \dots$), то для дальнейших выражений произвольное десятичное целое число k удобно представить в двоичном виде, используя следующее бинарное представление:

$$k \equiv (k_1, k_2, \dots, k_n) \equiv k_1 2^{n-1} + k_2 2^{n-2} + \dots + k_n 2^0 = \sum_{\ell=1}^n k_\ell 2^{n-\ell}, \quad (6.45)$$

где $k_l \in \{0, 1\}$. Рассмотрим подробно преобразование (6.44) с учётом бинарного представления базисных векторов регистра из n штук кубит и представления целых чисел в форме (6.45). Так как для квантовых регистров всегда $N = 2^n$, перепишем (6.44) с учётом равенства (6.45) и определения $|k\rangle_n = |k_1, k_2, \dots, k_n\rangle_n$, где $k_l \in \{0, 1\}$, следующим образом:

$$\overline{|j\rangle_n} = \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^1 \cdots \sum_{k_n=0}^1 \exp \left[i2\pi j \left(\frac{k_1}{2} + \frac{k_2}{2^2} + \cdots + \frac{k_n}{2^n} \right) \right] |k_1, k_2, \dots, k_n\rangle_n. \quad (6.46)$$

А так как по определению имеют место равенства

$$\exp \left(\sum_{m=1}^p \alpha_m \right) = \prod_{m=1}^p \exp(\alpha_m);$$

$$|k_1, k_2, \dots, k_n\rangle_n = |k_1\rangle \otimes |k_2\rangle \otimes \cdots \otimes |k_n\rangle \equiv \bigotimes_{\ell=1}^n |k_\ell\rangle,$$

то, объединяя множители в прямом произведении при одинаковых $|k_\ell\rangle$, перепишем выражение (6.46) в виде

$$\overline{|j\rangle_n} = \frac{1}{\sqrt{2^n}} \bigotimes_{\ell=1}^n \sum_{k_\ell=0}^1 \exp \left(i2\pi j \frac{k_\ell}{2^\ell} \right) |k_\ell\rangle. \quad (6.47)$$

Просуммировав последнее выражение по $k_\ell = 0, 1$, получим

$$\overline{|j\rangle_n} = \bigotimes_{\ell=1}^n |\mu_\ell(j)\rangle; \quad |\mu_\ell(j)\rangle \equiv \frac{1}{\sqrt{2}} \left[|0\rangle + \exp \left(i2\pi j \frac{1}{2^\ell} \right) |1\rangle \right]. \quad (6.48)$$

Упражнение 6.4. Построить матрицу Фурье-преобразования для случая $N = 8$.

6.5 Квантовый алгоритм преобразования Фурье

При построении квантовой цепи Фурье-преобразования для придания выражению (6.48) вида, из которого можно установить последовательность операций над кубитами, рассмотрим сначала случай системы из двух кубит:

$$\begin{aligned} \overline{|j\rangle_2} &= |\mu_1\rangle \otimes |\mu_2\rangle = \\ &= \frac{1}{\sqrt{2}} \left[|0\rangle + \exp \left(i2\pi j \frac{1}{2^1} \right) |1\rangle \right] \otimes \frac{1}{\sqrt{2}} \left[|0\rangle + \exp \left(i2\pi j \frac{1}{2^2} \right) |1\rangle \right]. \end{aligned} \quad (6.49)$$

Для двух кубит целое число j в двоичном представлении с учётом равенства (6.45) есть $j \equiv (j_1, j_2) = j_1 2^1 + j_2 2^0$, $j_\ell \in 0, 1$. Таким образом,

$$\begin{aligned} \exp\left(i2\pi j \frac{1}{2^1}\right) &= \exp\left(i2\pi (j_1 2 + j_2) \frac{1}{2}\right) = \\ &= \exp\left(i2\pi \left(j_1 + \frac{j_2}{2}\right)\right) = \exp\left(i2\pi \frac{j_2}{2}\right), \end{aligned}$$

так как $\exp(i2\pi j_1) = 1$ при целом j_1 . Аналогично найдём, что

$$\exp\left(i2\pi j \frac{1}{2^2}\right) = \exp\left(i2\pi (j_1 2 + j_2) \frac{1}{2^2}\right) = \exp\left(i2\pi \left(\frac{j_1}{2} + \frac{j_2}{2^2}\right)\right).$$

Для дальнейших преобразований введём следующее обозначение при записи бинарной функции, содержащей обратные степени 2:

$$O, k_1 k_2 \dots k_m \equiv \frac{k_1}{2^1} + \frac{k_2}{2^2} + \frac{k_3}{2^3} + \dots + \frac{k_m}{2^m}, \quad k_\ell \in 0, 1. \quad (6.50)$$

С учётом данного обозначения выражение (6.49) примет вид

$$\begin{aligned} \overline{|j\rangle}_2 &\equiv \overline{|j_1, j_2\rangle} = \\ &= \frac{1}{\sqrt{2}} [|0\rangle + \exp(i2\pi O, j_2) |1\rangle] \otimes \frac{1}{\sqrt{2}} [|0\rangle + \exp(i2\pi O, j_1, j_2) |1\rangle]. \end{aligned} \quad (6.51)$$

В общем случае произвольного числа битовых переменных квантовое Фурье-преобразование может быть задано в следующей форме прямого тензорного произведения однокубитовых состояний:

$$\begin{aligned} \hat{F} |j\rangle_n &\equiv \overline{|j\rangle}_n \equiv \overline{|j_1, j_2, \dots, j_n\rangle} = |\mu_1(j)\rangle \otimes |\mu_2(j)\rangle \cdots \otimes |\mu_n(j)\rangle = \\ &= \frac{1}{\sqrt{2^n}} (|0\rangle + \exp(2\pi i O, j_n) |1\rangle) \otimes (|0\rangle + \exp(2\pi i O, j_{n-1}, j_n) |1\rangle) \otimes \dots \\ &\quad \dots \otimes (|0\rangle + e^{2\pi i O, j_1 j_2 \dots j_n} |1\rangle). \end{aligned} \quad (6.52)$$

Это представление настолько полезно, что его можно рассматривать как определение квантового Фурье-преобразования.

Для общности отметим, что состояние $|\mu_k(j)\rangle$, где бинарное представление j имеет вид $j \equiv (j_1, j_2, \dots, j_{n-k}, j_{n-k+1}, j_{n-k+2}, \dots, j_{n-1}, j_n)$, $j_\ell \in 0, 1$, может быть записано следующим образом:

$$|\mu_k(j)\rangle = \frac{1}{\sqrt{2}} [|0\rangle + \exp(i2\pi O, j_{n-k+1}, j_{n-k+2}, \dots, j_{n-1}, j_n) |1\rangle]. \quad (6.53)$$

Представление Фурье-преобразования в форме произведения однокубитовых состояний (6.52) позволяет построить квантовую цепь для выполнения квантовых Фурье-преобразований. Для этого рассмотрим последовательно одно-, двух- и трёхкубитовые состояния. При наличии одного кубита после выполнения квантового преобразования Фурье на основании (6.52) получим кубит, находящийся в суперпозиции вида

$$\begin{aligned} \overline{|j\rangle_1} &\equiv \overline{|j_1\rangle} \equiv \hat{F}|j_1\rangle = |\mu_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \exp(2\pi i O_{j_1})|1\rangle) = \\ &= \begin{cases} (|0\rangle + |1\rangle)/\sqrt{2}, & j_1 = 0; \\ (|0\rangle - |1\rangle)/\sqrt{2}, & j_1 = 1; \end{cases} \end{aligned} \quad (6.54)$$

что, очевидно, соответствует действию гейта Адамара Н. Следовательно, такая квантовая цепь имеет тривиальный вид (рис. 6.7).



Рис. 6.7. Логическая диаграмма Фурье-преобразования однокубитового состояния

При наличии двух кубит $|j\rangle_2 = |j_1, j_2\rangle$ из (6.52) результат квантового Фурье-преобразования есть прямое произведение двух кубит $|\mu_1\rangle, |\mu_2\rangle$:

$$\begin{aligned} \hat{F}|j\rangle_2 &\equiv \overline{|j\rangle_2} \equiv \overline{|j_1, j_2\rangle} = |\mu_1\rangle \otimes |\mu_2\rangle = \\ &= \frac{1}{\sqrt{2^2}}(|0\rangle + \exp(2\pi i O_{j_2})|1\rangle) \otimes (|0\rangle + \exp(2\pi i O_{j_1 j_2})|1\rangle). \end{aligned} \quad (6.55)$$

Рассмотрим подробнее кубит $|\mu_2\rangle$:

$$|\mu_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i O_{j_1 j_2}}|1\rangle) = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i O_{j_1}} \exp\left[2\pi i \left(\frac{j_2}{2^2}\right)\right]|1\rangle\right). \quad (6.56)$$

Другими словами, кубит $|\mu_2(j)\rangle$ получается в результате действия на кубит $|j_1\rangle$ гейта Адамара и контролируемого кубитом $|j_2\rangle$ гейта R_2 , меняющего фазу у базисного состояния $|1\rangle$ исходного кубита j_1 на величину $\exp(i2\pi/2^2)$ при $j_2 = 1$. При $j_2 = 0$ изменения фазы не происходит, так как $\exp(i2\pi0/2^2) = 1$. В результате квантовая цепь для преобразования кубита $|j_1\rangle$ в $|\mu_2(j)\rangle$ выглядит, как представленная на рис. 6.8.

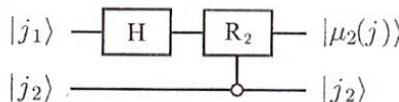


Рис. 6.8. Квантовая цепь формирования кубита $|\mu_2(j)\rangle$

Объединяя данное преобразование с преобразованием для нахождения $|\mu_1(j)\rangle$ (рис. 6.7), получим квантовую цепь, представленную на рис. 6.9.

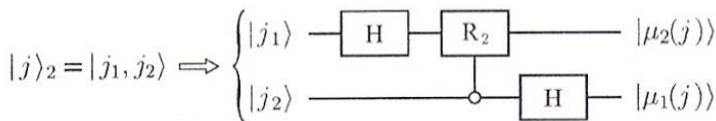


Рис. 6.9. Объединённая цепь формирования кубитов $|\mu_1(j)\rangle$ и $|\mu_2(j)\rangle$

Как следует из полученного результата, для его согласования с формулой (6.52) необходимо переставить кубиты $|\mu_1\rangle$ и $|\mu_2\rangle$ местами, так как результат Фурье-преобразования записывается в виде прямого произведения $|\mu_1\rangle \otimes |\mu_2\rangle$, а не $|\mu_2\rangle \otimes |\mu_1\rangle$, как это следует из представленной выше цепи. Перестановка кубит в цепи может быть осуществлена действием оператора SWAP. Таким образом, суммарно квантовая цепь двухкубитового преобразования Фурье может быть изображена, как показано на рис. 6.10.

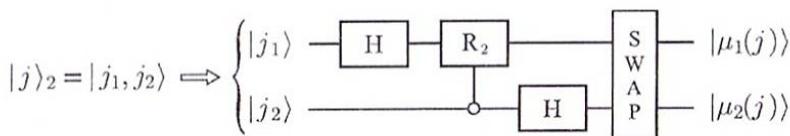


Рис. 6.10. Логическая диаграмма Фурье-преобразования двухкубитового состояния

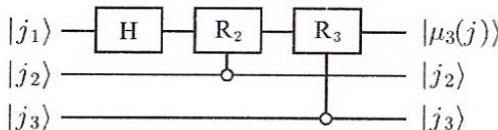
В случае трёх кубит результат квантового преобразования Фурье приводит к прямому произведению кубит следующего вида:

$$\hat{F}|j\rangle_3 = |\mu_1\rangle \otimes |\mu_2\rangle \otimes |\mu_3\rangle = \frac{1}{\sqrt{2^3}} (|0\rangle + \exp(2\pi i O_{j_3}) |1\rangle) \otimes \\ \otimes (|0\rangle + \exp(2\pi i O_{j_2 j_3}) |1\rangle) \otimes (|0\rangle + \exp(2\pi i O_{j_1 j_2 j_3}) |1\rangle). \quad (6.57)$$

Здесь $\hat{F}|j\rangle_3 \equiv \overline{|j_1, j_2, j_3\rangle}$. Так, например, для кубита $|\mu_3\rangle$ находим

$$|\mu_3\rangle = \frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i O_{j_1 j_2 j_3}} |1\rangle) = \\ = \frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i O_{j_1 j_2}} \exp\left(2\pi i \frac{j_3}{2^3}\right) |1\rangle \right). \quad (6.58)$$

Из полученного выражения с учётом соотношений для двухкубитовой системы ясно, что квантовая цепь формирования кубита $|\mu_3\rangle$ выглядит, как показано на рис. 6.11.

Рис. 6.11. Квантовая цепь формирования кубита $|\mu_3(j)\rangle$

Здесь R_k – контролируемый гейт изменения фазы у однокубитового базисного состояния $|1\rangle$ на величину $R_k \equiv \exp(i2\pi/2^k)$ при значении бита, равном единице, на контролирующей линии и на величину $R_k \equiv 1$ при значении бита контролирующей линии, равного нулю. Объединяя данный результат с цепью формирования кубитов $|\mu_2(j)\rangle$ и $|\mu_1(j)\rangle$ (см. рис. 6.9), находим окончательное изображение квантовой цепи преобразования Фурье трёхкубитового регистра (рис. 6.12).

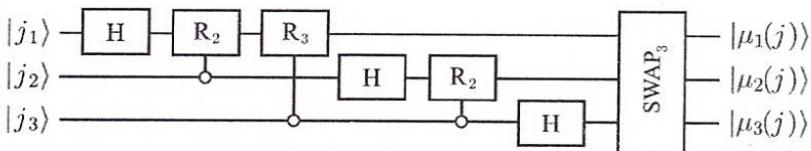
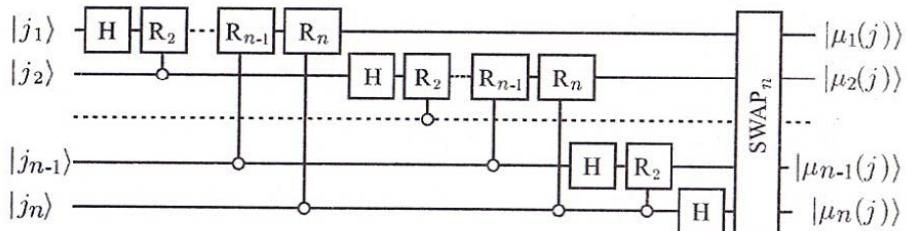


Рис. 6.12. Логическая диаграмма Фурье-преобразования трёхкубитового состояния

Очевидно, что в произвольном случае регистра из n -кубит квантовая цепь Фурье-преобразования выглядит, как показано на рис. 6.13.

Рис. 6.13. Логическая диаграмма Фурье-преобразования регистра n -кубит

Данная квантовая цепь соответствует следующей последовательности вычисления преобразования Фурье. Применяя гейт Адамара к первому кубиту $|j_1\rangle$, получим

$$\frac{1}{\sqrt{2}} (|0\rangle + \exp(2\pi i O, j_1) |1\rangle) \otimes |j_2, j_3, \dots, j_n\rangle_{n-1}, \quad (6.59)$$

так как $\exp(2\pi i O, j_1) = -1$, когда $j_1 = 1$, и равна $+1$ в случае $j_1 = 0$. Используя контролируемый R_2 -гейт, производим следующее преобразование

в соответствии с квантовой цепью:

$$\frac{1}{\sqrt{2}} (|0\rangle + \exp(2\pi i O, j_1 j_2) |1\rangle) \otimes |j_2, j_3, \dots, j_n\rangle_{n-1}. \quad (6.60)$$

Продолжая вычисление действий контролируемых R_3 -, R_4 - до R_n -гейтов, каждый из которых добавляет множитель к фазе коэффициента при базисном состоянии $|1\rangle$ первого кубита, в конце этой процедуры получим состояние

$$\frac{1}{\sqrt{2}} (|0\rangle + \exp(2\pi i O, j_1 j_2 \dots j_n) |1\rangle) \otimes |j_2, j_3, \dots, j_n\rangle_{n-1}. \quad (6.61)$$

Преобразуя аналогичной процедурой второй кубит, получим

$$\begin{aligned} & \frac{1}{\sqrt{2}} (|0\rangle + \exp(2\pi i O, j_1 j_2 \dots j_n) |1\rangle) \otimes \\ & \otimes (|0\rangle + \exp(2\pi i O, j_2 j_3 \dots j_n) |1\rangle) \otimes |j_3, j_4, \dots, j_n\rangle_{n-2}. \end{aligned} \quad (6.62)$$

Продолжая последовательно аналогичные преобразования для каждого следующего кубита, находим конечное состояние

$$\begin{aligned} & \frac{1}{\sqrt{2^n}} (|0\rangle + \exp(2\pi i O, j_1 j_2 \dots j_n) |1\rangle) \otimes \\ & \otimes (|0\rangle + \exp(2\pi i O, j_2 \dots j_n) |1\rangle) \otimes \dots \otimes (|0\rangle + \exp(2\pi i O, j_n) |1\rangle). \end{aligned} \quad (6.63)$$

Используя далее SWAP_n -оператор, состояние регистра кубит приводится к формуле (6.52), т. е. выполнено квантовое Фурье-преобразование.

Пример 6.2. Эквивалентность способов представления квантового преобразования Фурье

На приведённом ниже примере продемонстрируем эквивалентность алгоритмов квантового Фурье-преобразования, основанных на произведении (6.52) и определении (6.44), а также то, что построенная выше квантовая цепь соответствует заданной процедуре вычисления квантового Фурье-преобразования. Рассмотрим для простоты изложения двухкубитовый регистр $|k\rangle_2 = |k_1, k_2\rangle = |k_1\rangle \otimes |k_2\rangle$, $k_\ell \in 0, 1$. В соответствии с определением (6.44) с учётом десятичной нумерации базисных квантовых состояний находим:

$$\overline{|0\rangle_2} = \frac{1}{2} \sum_{k=0}^3 |k\rangle_2 = \frac{1}{2} [|0\rangle_2 + |1\rangle_2 + |2\rangle_2 + |3\rangle_2]. \quad (6.64)$$

$$\begin{aligned} \overline{|1\rangle_2} &= \frac{1}{2} \sum_{k=0}^3 \exp\left(i\frac{\pi}{2} k\right) |k\rangle_2 = \\ &= \frac{1}{2} \left[|0\rangle_2 + \exp\left(i\frac{\pi}{2}\right) |1\rangle_2 + \exp(i\pi) |2\rangle_2 + \exp\left(i\frac{3\pi}{2}\right) |3\rangle_2 \right]. \end{aligned} \quad (6.65)$$

$$\begin{aligned} \overline{|2\rangle_2} &= \frac{1}{2} \sum_{k=0}^3 \exp(i\pi k) |k\rangle_2 = \\ &= \frac{1}{2} [|0\rangle_2 + \exp(i\pi) |1\rangle_2 + \exp(i2\pi) |2\rangle_2 + \exp(i3\pi) |3\rangle_2]. \end{aligned} \quad (6.66)$$

$$\begin{aligned} \overline{|3\rangle_2} &= \frac{1}{2} \sum_{k=0}^3 \exp\left(i\frac{3\pi}{2} k\right) |k\rangle_2 = \\ &= \frac{1}{2} \left[|0\rangle_2 + \exp\left(i\frac{3\pi}{2}\right) |1\rangle_2 + \exp(i3\pi) |2\rangle_2 + \exp\left(i\frac{9\pi}{2}\right) |3\rangle_2 \right]. \end{aligned} \quad (6.67)$$

В матричном виде после вычисления значения экспонент представленные выше равенства имеют вид

$$\begin{pmatrix} \overline{|0\rangle_2} \\ \overline{|1\rangle_2} \\ \overline{|2\rangle_2} \\ \overline{|3\rangle_2} \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \begin{pmatrix} |0\rangle_2 \\ |1\rangle_2 \\ |2\rangle_2 \\ |3\rangle_2 \end{pmatrix}. \quad (6.68)$$

В свою очередь, на основании (6.52) имеем

$$\overline{|j\rangle} = \overline{|j_1, j_2\rangle} = \frac{1}{2} \left[|0\rangle + \exp\left(i2\pi\frac{j_2}{2}\right) |1\rangle \right] \otimes \left[|0\rangle + \exp\left(i2\pi\left(\frac{j_1}{2} + \frac{j_2}{4}\right)\right) \right]. \quad (6.69)$$

Перебирая бинарные значения $j_1, j_2 \in 0, 1$, получим на основании (6.69) четыре двухкубитовых базисных состояния:

$$\overline{|0\rangle_2} = \overline{|0, 0\rangle} = \frac{1}{2} [|0\rangle_2 + |1\rangle_2 + |2\rangle_2 + |3\rangle_2]; \quad (6.70)$$

$$\overline{|1\rangle_2} = \overline{|0, 1\rangle} = \frac{1}{2} [|0\rangle_2 + i|1\rangle_2 - |2\rangle_2 - i|3\rangle_2]; \quad (6.71)$$

$$\overline{|2\rangle_2} = \overline{|0, 1\rangle} = \frac{1}{2} [|0\rangle_2 - |1\rangle_2 + |2\rangle_2 - |3\rangle_2]; \quad (6.72)$$

$$\overline{|3\rangle_2} = \overline{|0, 1\rangle} = \frac{1}{2} [|0\rangle_2 - i|1\rangle_2 - |2\rangle_2 + i|3\rangle_2]; \quad (6.73)$$

что в матричном виде точно совпадает с (6.68). Таким образом, на данном простом примере видна эквивалентность выражений (6.52) и (6.44) для описания квантового Фурье-преобразования в случае двухкубитовых состояний.

Пример 6.3. Операторный метод преобразования Фурье

Операторный метод для описания преобразования Фурье можно продемонстрировать на примере простого двухкубитового состояния. В соответствии с определением при выполнении Фурье-преобразования сначала на первый кубит двухкубитового состояния действует оператор Адамара. В результате образуется следующее двухкубитовое состояние:

$$\begin{aligned} |\phi_1\rangle_2 &\equiv \hat{U}_1 |k\rangle_2 = \hat{H}_1 : |k\rangle_2 = \hat{H}_1 : |k_1, k_2\rangle = \\ &= \frac{1}{\sqrt{2}} [|0\rangle + \exp(i 2\pi O, k_1) |1\rangle] \otimes |k_2\rangle. \end{aligned}$$

Так как $\exp(2\pi i O, k_1) = -1$, когда $k_1 = 1$, и равна $+1$ в случае $k_1 = 0$, что и соответствует определению оператора Адамара, то унитарный оператор \hat{U}_1 , преобразующий исходное двухкубитовое состояние $|k\rangle_2$ в двухкубитовое состояние $|\phi_1\rangle_2$ ($\hat{U}_1 : |k\rangle_2 = |\phi_1\rangle_2$), равен

$$\hat{U}_1 \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}; \quad |\phi_1\rangle_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} |0, 0\rangle + |1, 0\rangle \\ |0, 1\rangle + |1, 1\rangle \\ |0, 0\rangle - |1, 0\rangle \\ |0, 1\rangle - |1, 1\rangle \end{pmatrix}. \quad (6.74)$$

Действие контролируемого приращения фазы R_2 на двухкубитовое состояние $|\phi_1\rangle_2$ определяется унитарным оператором \hat{U}_2 , приводящим к двухкубитовому состоянию $|\phi_2\rangle_2$ ($\hat{U}_2 : |\phi_1\rangle_2 = |\phi_2\rangle_2$):

$$\hat{U}_2 \equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{pmatrix}; \quad |\phi_2\rangle_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} |0, 0\rangle + |1, 0\rangle \\ |0, 1\rangle + i |1, 1\rangle \\ |0, 0\rangle - |1, 0\rangle \\ |0, 1\rangle - i |1, 1\rangle \end{pmatrix}. \quad (6.75)$$

На третьем шаге после действия оператора Адамара на второй кубит из пары, действие которого определяется унитарным оператором \hat{U}_3 , находим:

$$\hat{U}_3 : |\phi_2\rangle_2 = |\phi_3\rangle_2; \quad \hat{U}_3 \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}. \quad (6.76)$$

$$|\phi_3\rangle_2 = \frac{1}{2} \begin{pmatrix} |0, 0\rangle + |0, 1\rangle + |1, 0\rangle + |1, 1\rangle \\ |0, 0\rangle - |0, 1\rangle + i |1, 0\rangle - i |1, 1\rangle \\ |0, 0\rangle + |0, 1\rangle - |1, 0\rangle - |1, 1\rangle \\ |0, 0\rangle - |0, 1\rangle - i |1, 0\rangle + i |1, 1\rangle \end{pmatrix}. \quad (6.77)$$

Наконец, на последнем шаге используем SWAP-гейт, матричный вид которого обозначим через \hat{U}_4 :

$$\hat{U}_4 : |\phi_3\rangle_2 = |\phi_4\rangle_2; \quad \hat{U}_4 \equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \quad (6.78)$$

В результате находим для $|\phi_4\rangle_2$

$$= \frac{1}{2} \begin{pmatrix} |0,0\rangle + |0,1\rangle + |1,0\rangle + |1,1\rangle \\ |0,0\rangle + i|0,1\rangle - |1,0\rangle - |1,1\rangle \\ |0,0\rangle - |0,1\rangle + |1,0\rangle - |1,1\rangle \\ |0,0\rangle - i|0,1\rangle - |1,0\rangle + i|1,1\rangle \end{pmatrix}, \quad (6.79)$$

что в точности совпадает с (6.68). Другими словами, квантовое Фурье-преобразование для двух кубит можно представить в операторном виде:

$$QFT |k\rangle_2 = \hat{U}_4 \cdot \hat{U}_3 \cdot \hat{U}_2 \cdot \hat{U}_1 : |k\rangle_2,$$

где операторы \hat{U}_i определены выше.

Упражнение 6.5. Выполнить обратное преобразование Фурье для базисных состояний трёхкубитового регистра.

6.6 Оценка фазы

Задача “оценки фазы” является относительно абстрактной задачей, реальное применение которой будет представлено в следующем разделе. Постановка задачи может быть сформулирована следующим образом. Предположим, что имеется квантовый n -кубитовый регистр вида

$$|q\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \exp(i 2\pi \varphi k) |k\rangle_n; \quad k \in \{0, 1, 2, \dots, 2^n - 1\}, \quad (6.80)$$

где φ — произвольное число в диапазоне $\varphi \in [0, 1]$. Диапазон изменения числа φ охватывает общий случай в силу периодичности экспоненты $\exp(i 2\pi \varphi) = \exp(i 2\pi (\varphi + k))$, где k — целое число. Задача состоит в том, чтобы получить надёжную оценку фазового множителя φ . Под оценкой понимается определение приближённого (или точного) значения φ .

Решение поставленной задачи может быть найдено с использованием обратного квантового Фурье-преобразования (6.41), которое позволяет переписать (6.80) в виде

$$\hat{F}^\dagger |q\rangle_n \equiv |Q\rangle_n = \frac{1}{2^n} \sum_{j=0}^{2^n-1} \sum_{k=0}^{2^n-1} \exp(i 2\pi \varphi k) \exp\left(-i 2\pi \frac{k}{2^n} j\right) |j\rangle_n \quad (6.81)$$

или

$$|Q\rangle_n = \sum_{j=0}^{2^n-1} \sum_{k=0}^{2^n-1} \frac{1}{2^n} \left[\exp \left(i 2\pi \left(\varphi - \frac{j}{2^n} \right) \right) \right]^k |j\rangle_n = \sum_{j=0}^{2^n-1} a_j |j\rangle_n. \quad (6.82)$$

Здесь a_j — амплитуда вероятности найти в результате измерения регистра $|Q\rangle_n$ n -кубитовое состояние $|j\rangle_n$, которое в бинарном обозначении есть $|j\rangle_n = |j_1, j_2, \dots, j_n\rangle$:

$$a_j = \sum_{k=0}^{2^n-1} \frac{1}{2^n} \left[\exp \left(i 2\pi \left(\varphi - \frac{j}{2^n} \right) \right) \right]^k. \quad (6.83)$$

В выражении (6.83) существенно отметить то обстоятельство, что если $\varphi = j/2^n$, то при измерении $|Q\rangle_n$ получится точно состояние $|j\rangle = |2^n\varphi\rangle$. Знание j позволяет простым делением числа j на 2^n вычислить множитель φ , т. е. найти искомый фазовый множитель, так как в этом тривиальном случае $\varphi = j/2^n$. При этом

$$a_{j=2^n\varphi} = \sum_{k=0}^{2^n-1} \frac{1}{2^n} = 1$$

и, следовательно, амплитуды всех остальных состояний оказались бы равными нулю в соответствии с условием нормировки состояния $|Q\rangle_n$. Однако в общем случае точное равенство $\varphi = j/2^n$ не выполняется. Но, применяя изложенную выше процедуру обратного преобразования Фурье исходного состояния и последующего измерения полученного многокубитового состояния, можно найти фазовый множитель φ приближённо.

Для пояснения сделанного утверждения рассмотрим подробно амплитуду a_j вероятности состояния $|j\rangle$. Как следует из (6.83), данная амплитуда представляет собой сумму геометрической прогрессии с показателем прогрессии, равным

$$s = \frac{1}{2^n} \left[\exp \left(i 2\pi \left(\varphi - \frac{j}{2^n} \right) \right) \right]. \quad (6.84)$$

В результате амплитуда a_j может быть записана в виде

$$a_j = \sum_{k=0}^{2^n-1} s^k = \frac{1}{2^n} \frac{1 - s^{2^n}}{1 - s} = \frac{1}{2^n} \frac{1 - \exp [i 2\pi (2^n \varphi - j)]}{1 - \exp [i 2\pi (\varphi - j/2^n)]}. \quad (6.85)$$

Таким образом, вероятность измерения состояния $|j\rangle$ в общем случае определяется выражением

$$P_j = |a_j|^2 = \frac{1}{2^{2n}} \frac{\sin^2 (\pi (2^n \varphi - j))}{\sin^2 (\pi (\varphi - j/2^n))}. \quad (6.86)$$

Анализ полученного выражения показывает, что в случае $\varphi \neq j/2^n$ вероятность получить приближённое значение $j \approx 2^n\varphi$ больше $8/\pi^2 \approx 0,81$. В этом смысле алгоритм оценки квантовой фазы для произвольного числа является вероятностным алгоритмом, а точность вычисления числа φ , как будет показано ниже, возрастает с ростом числа кубит, использующихся для его определения.

Для составления квантовой цепи, приводящей к решению сформулированной задачи, введём несколько простых обозначений и рассмотрим ряд элементарных примеров. Допустим, надо оценить число, лежащее в интервале $\varphi \in [0, 1]$, задающее квантовое состояние вида

$$|q\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \exp(i 2\pi \varphi k) |k\rangle_n. \quad (6.87)$$

Значения φ достаточно рассматривать в диапазоне $[0, 1)$, так как для любого целого числа $k \exp(i 2\pi k) = 1$. Бинарное представление числа φ в общем случае имеет вид

$$\varphi \equiv O, x_1 x_2 x_3, \dots \equiv \frac{x_1}{2} + \frac{x_2}{2^2} + \frac{x_3}{2^3} \dots, \quad \text{где} \quad x_i \in \{0, 1\}.$$

С учётом данного определения при использовании бинарной арифметики введём тривиальные символические равенства при заданном φ , которые получаются при умножении $\varphi = O, x_1, x_2, x_3, \dots$ на целое число 2^n :

$$2\varphi \rightarrow O, x_2 x_3 \dots; \quad 2^{n-1}\varphi \rightarrow O, x_n x_{n+1}, \dots$$

Данные операторные соотношения основаны на тождестве $\exp(i 2\pi k) = 1$, которое имеет место при целых k и элементарных свойствах экспоненциальной функции. Например,

$$\begin{aligned} \exp[i 2\pi(2\varphi)] &= \exp\left[i 2\pi\left(x_1 + \frac{x_2}{2} + \frac{x_3}{2^2} + \dots\right)\right] = \\ &= \exp[i 2\pi x_1] \exp[i 2\pi(O, x_2 x_3 \dots)] = \exp[i 2\pi(O, x_2 x_3 \dots)], \end{aligned}$$

что символически обозначается как $2\varphi \rightarrow O, x_2 x_3 \dots$. В общем случае при умножении φ на 2^n получим

$$\exp[i 2\pi(2^n \varphi)] = \exp[i 2\pi(O, x_{n+1} x_{n+2} \dots)], \quad \text{или} \quad 2^n \varphi \rightarrow O, x_{n+1} x_{n+2} \dots \quad (6.88)$$

Для наглядности вывода общего решения задачи оценки фазы рассмотрим тривиальный случай однокубитового состояния $n = 1$ в (6.87), в котором $\varphi = O, x_1 = x_1/2$, где $x_1 \in \{0, 1\}$. В этом случае исходное квантовое

состояние есть

$$|q\rangle = \frac{1}{\sqrt{2}} (|0\rangle + \exp[i2\pi(O, x_1)]|1\rangle) \equiv \frac{1}{\sqrt{2}} [|0\rangle + (-1)^{x_1}|1\rangle]. \quad (6.89)$$

Если на данный начальный вектор состояния подействовать гейтом Адамара, то однозначно возникает однокубитовое состояние $|x_1\rangle$, измерение которого точно определяет величину x_1 , так как

$$H : |q\rangle = \frac{1}{2} [|0\rangle + |1\rangle + (-1)^{x_1}|0\rangle - (-1)^{x_1}|1\rangle] = |x_1\rangle.$$

Полученный результат означает, что, подействовав на исходную суперпозицию (6.89) гейтом Адамара, по результатам измерения можно определить точное значение фазового множителя $\varphi = x_1/2$. Как показано ранее, в случае однокубитового состояния гейт Адамара осуществляет квантовое преобразование Фурье (и прямое, и обратное).

Рассмотрим далее суперпозицию (6.87) для двухкубитового регистра:

$$\begin{aligned} |q\rangle_2 &= \frac{1}{2} \sum_{k=0}^3 \exp(i2\pi\varphi k) |k\rangle_2 = \\ &= \frac{1}{2} [|0\rangle_2 + \exp(i2\pi\varphi)|1\rangle_2 + \exp(i2\pi\varphi 2)|2\rangle_2 + \exp(i2\pi\varphi 3)|3\rangle_2]. \end{aligned} \quad (6.90)$$

Данное выражение эквивалентно прямому произведению однокубитовых состояний вид

$$|q\rangle_2 = \frac{1}{2} \left(|0\rangle + \exp(i2\pi 2\varphi)|1\rangle \right) \otimes \left(|0\rangle + \exp(i2\pi\varphi)|1\rangle \right).$$

Если, например, бинарное значение $\varphi = 0$, $x_1, x_2 = x_1/2 + x_2/2^2$, где $x_i \in 0, 1$, то с учетом равенства (6.88) состояние $|q\rangle_2$ можно переписать в виде

$$|q\rangle_2 = \frac{1}{2} \left(|0\rangle + e^{i2\pi(O, x_2)}|1\rangle \right) \otimes \left(|0\rangle + e^{i2\pi(O, x_1 x_2)}|1\rangle \right) \equiv |q_1\rangle \otimes |q_2\rangle. \quad (6.91)$$

Отметим, что с использованием обозначения (6.53), введённого в теории квантового Фурье-преобразования, кубиты $|q_1\rangle$ и $|q_2\rangle$ равны соответственно:

$$\begin{aligned} |q_1\rangle &= \frac{1}{\sqrt{2}} [|0\rangle + \exp(i2\pi(O, x_2))|1\rangle] \equiv |\mu_1(x)\rangle; \\ |q_2\rangle &= \frac{1}{\sqrt{2}} [|0\rangle + \exp(i2\pi(O, x_1 x_2))|1\rangle] \equiv |\mu_2(x)\rangle. \end{aligned} \quad (6.92)$$

Данные сокращённые обозначения ($|\mu_k(x)\rangle$) полезны при изображении регистра кубит в квантовых цепях. Для общности напомним, что если бинарное задание x имеет вид $x \equiv (x_1, x_2, \dots, x_n)$, то, например,

$$\begin{aligned} |\mu_1(x)\rangle &= \frac{1}{\sqrt{2}} \left[|0\rangle + e^{i2\pi(O, x_n)} |1\rangle \right]; \quad |\mu_2(x)\rangle = \frac{1}{\sqrt{2}} \left[|0\rangle + e^{i2\pi(O, x_{n-1}, x_n)} |1\rangle \right]; \\ \dots \quad |\mu_{n-1}(x)\rangle &= \frac{1}{\sqrt{2}} \left[|0\rangle + e^{i2\pi(O, x_2, x_3, \dots, x_n)} |1\rangle \right]; \\ |\mu_n(x)\rangle &= \frac{1}{\sqrt{2}} \left[|0\rangle + e^{i2\pi(O, x_1, x_2, \dots, x_n)} |1\rangle \right]. \end{aligned}$$

Для дальнейших преобразований напомним определение гейта контролируемого изменения фазы R_k у базисного состояния $|1\rangle$ контролируемого кубита:

$$R_k(i, j) |0\rangle \equiv |0\rangle; \quad R_k(i, j) |1\rangle \equiv \exp(i 2\pi/2^k) |1\rangle,$$

здесь i — номер линии контролирующего кубита, j — номер линии контролируемого кубита, с которым осуществляется данное преобразование. Обратный к $R_k(i, j)$ гейт обозначается $R_k^{-1}(i, j)$ и отличается от $R_k(i, j)$ знаком в показателе экспоненты.

Выполним с двухкубитовым регистром (6.91) преобразование, которое определяется следующей последовательностью действия операторов R_2 , гейтов Адамара и гейта SWAP₂:

$$\text{SWAP}_2 : S : |q\rangle_2 \equiv \text{SWAP}_2 : (H_2 R_2^{-1}(1, 2)) \otimes H_1 : |q\rangle_2.$$

В результате до действия оператора SWAP₂ получим регистр $|z\rangle_2$:

$$\begin{aligned} |z\rangle_2 &= S : |q\rangle_2 = H_2 R_2^{-1}(1, 2) \otimes H_1 : |q_1\rangle \otimes |q_2\rangle = \\ &= H_2 R_2^{-1}(1, 2) : \frac{1}{2} \left(H_1 : \left[|0\rangle + \exp(i 2\pi O, x_2) |1\rangle \right] \right) \otimes |q_2\rangle = \\ &= \frac{1}{2\sqrt{2}} H_2 R_2^{-1}(1, 2) : \left[|0\rangle + |1\rangle + \exp(i 2\pi O, x_2) \left(|0\rangle - |1\rangle \right) \right] \otimes |q_2\rangle = \\ &= \frac{1}{\sqrt{2}} H_2 R_2^{-1}(1, 2) : |x_2\rangle \otimes |q_2\rangle = \\ &= \frac{1}{\sqrt{2}} |x_2\rangle \otimes H_2 R_2^{-1}(1, 2) : \left[|0\rangle + \exp(i 2\pi O, x_1 x_2) |1\rangle \right] = \\ &= \frac{1}{\sqrt{2}} |x_2\rangle \otimes H_2 : \left[|0\rangle + \exp\left(-i \frac{2\pi}{4} x_2\right) \exp(i 2\pi O, x_1 x_2) |1\rangle \right] = \\ &= \frac{1}{2} |x_2\rangle \otimes \left(|0\rangle + |1\rangle + \exp(i 2\pi O, x_1) \left(|0\rangle - |1\rangle \right) \right) = |x_2\rangle \otimes |x_1\rangle = |x_2, x_1\rangle_2. \end{aligned}$$

После действия оператора SWAP_2 на $|z\rangle_2$ получим

$$|\psi\rangle_2 = \text{SWAP}_2 : |z\rangle_2 = |x_1, x_2\rangle.$$

Таким образом, при измерении конечного двухкубитового состояния $|\psi\rangle_2$ точно определится фазовый множитель $\varphi = 0, x_1 x_2$. Необходимо подчеркнуть, что точный результат получился в связи с тем, что искомый фазовый множитель точно совпадает с правильной дробью и имеет вид

$$\varphi = O, x_1 x_2 = x_1/2 + x_2/4.$$

Представленное преобразование, выполненное с регистром $|q\rangle_2$, является обратным квантовым преобразованием Фурье и может быть изображено квантовой цепью, приведённой на рис. 6.14.

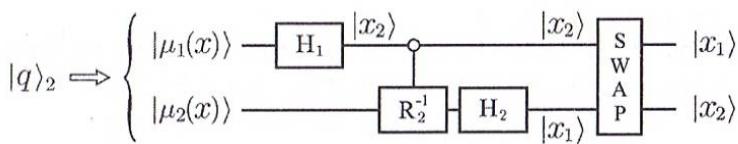


Рис. 6.14. Логическая диаграмма оценки фазы двухкубитового состояния

В общем случае имеет место равенство, которое и позволяет построить квантовую цепь для оценки фазы при использовании многокубитового квантового регистра:

$$|q\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \exp(i 2\pi \varphi k) |k\rangle_n = \quad (6.93)$$

$$\begin{aligned} &= \frac{|0\rangle + e^{i2\pi(2^{n-1}\varphi)} |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{i2\pi(2^{n-2}\varphi)} |1\rangle}{\sqrt{2}} \otimes \dots \otimes \frac{|0\rangle + e^{i2\pi(2^0\varphi)} |1\rangle}{\sqrt{2}} = \\ &= \frac{|0\rangle + e^{i2\pi(0, x_n x_{n+1} \dots)} |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{i2\pi(0, x_{n-1} x_n x_{n+1} \dots)} |1\rangle}{\sqrt{2}} \otimes \dots \\ &\dots \otimes \frac{|0\rangle + e^{i2\pi(0, x_2 x_3 \dots)} |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{i2\pi(0, x_1 x_2 \dots)} |1\rangle}{\sqrt{2}}. \end{aligned}$$

Квантовая цепь, осуществляющая квантовое Фурье-преобразование с исходным n -кубитовым регистром $|x\rangle_n = |x_1, x_2, \dots, x_n\rangle$, где $x_i \in \{0, 1\}$, изображена на рис. 6.15.

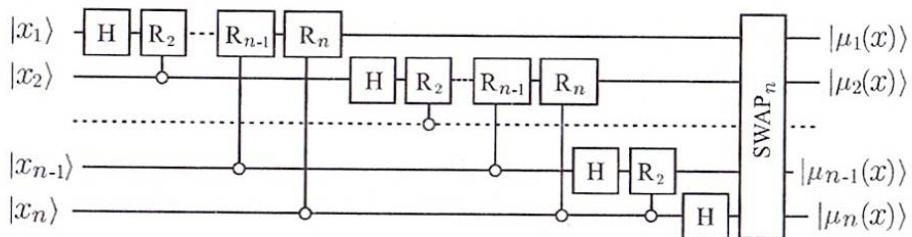


Рис. 6.15. Логическая диаграмма квантового Фурье-преобразования

Справа на рис. 6.15 изображено n -кубитовое состояние, совпадающее с (6.93). Из данного рисунка видно, что квантовое Фурье-преобразование является обращением операции оценки фазы. Это следует из приведённой квантовой цепи, если "прочитать" данную цепь справа налево (6.93). Как видно, обратное преобразование от $|q\rangle_n = \bigotimes_{i=1}^n |\mu_i\rangle$ приведёт к n -кубитовому состоянию $|x\rangle_n = |x_1, x_2, \dots, x_n\rangle$, где $x_i \in \{0, 1\}$, определяющее мультибитовое представление φ .

Таким образом, алгоритм оценки фазы состоит в реализации обратного Фурье-преобразования с n -кубитовым регистром (6.80). При этом размер данного регистра будет определять точность вычисления числа φ .

Упражнение 6.6. Решить задачу оценки фазы для трёхкубитового регистра и бинарного представления $\varphi = 0, x_1, x_2, x_3 = x_1/2 + x_2/2^2 + x_3/2^3$, где $x_i \in \{0, 1\}$.

6.7 Возврат фазы в регистр данных

В соответствии с определением гейта CNOT справедливы следующие равенства:

$$\begin{aligned} \text{CNOT} : |x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) &= |x\rangle \otimes (-1)^x \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \equiv \\ &\equiv (-1)^x |x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right), \end{aligned} \quad (6.94)$$

где $x \in \{0, 1\}$. Данное выражение демонстрирует возможность отнесения фазы $(-1)^x$ как к управляемому кубиту, так и к управляющему. По определению гейта CNOT осуществляет операцию отрицания именно с управляемым кубитом (если управляющий кубит в состоянии $|1\rangle$), оставляя без изменения управляющий кубит. Однако общий фазовый множитель для отдельного кубита не играет роли по принципам квантовой теории. Отсюда возникает возможность ассоциирования фазы с управляющим кубитом,

что позволяет ввести понятие возврата фазы, которое будет определено ниже. Кроме того, из выражения (6.94) ясно следует, что суперпозиция состояний вида $(|0\rangle - |1\rangle)/\sqrt{2}$ является собственным вектором однокубитового оператора NOT с собственным значением, равным -1 , а также собственным вектором единичного оператора I с собственным значением, равным $+1$.

Обобщение выражения (6.94) на случай, когда управляющий кубит находится в произвольной суперпозиции двух базисных состояний $|0\rangle$, $|1\rangle$, имеет следующий вид:

$$\text{CNOT} : \sum_{x=0}^1 \alpha_x |x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) = \sum_{x=0}^1 (-1)^x \alpha_x |x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right). \quad (6.95)$$

В результате, например, действие последовательности операторов $H_2 : \text{CNOT}_{1,2} : H_2$ на двухкубитовый регистр $(\alpha_0 |0\rangle + \alpha_1 |1\rangle) \otimes |1\rangle$ приводит к следующему двухкубитовому состоянию $(\alpha_0 |0\rangle - \alpha_1 |1\rangle) \otimes |1\rangle$, в котором у первого кубита произошло изменение фазы перед базисным однокубитовым состоянием $|1\rangle$. Данной последовательности операций над кубитами соответствует квантовая цепь, приведённая на рис. 6.16.

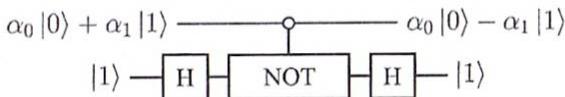


Рис. 6.16. Логическая диаграмма изменения фазы однокубитового состояния

Рассмотрим теперь общий случай двухкубитового унитарного оператора (гейта) U , введённого ранее, который реализует бинарную функцию $f : (0, 1) \rightarrow (0, 1)$. Действие данного гейта определено выражением

$$U : |x\rangle \otimes |y\rangle \rightarrow |x\rangle \otimes |y \oplus f(x)\rangle.$$

В соответствии с формулой (6.10), связывая фазовый множитель $(-1)^{f(x)}$ с управляющим кубитом, получаем равенство

$$U : |x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) = (-1)^{f(x)} |x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right). \quad (6.96)$$

Отметим, что состояние управляемого регистра $(|0\rangle - |1\rangle)/\sqrt{2}$ является собственным вектором оператора U с собственным числом, равным $(-1)^{f(x)}$. Таким образом, действие гейта U можно рассматривать как операцию возврата собственного числа $(-1)^{f(x)}$ на управляющий кубит. Данное явление принято называть возвратом фазы, в данном случае на управляющий кубит, а в общем случае произвольного регистра данных — возвратом фазы в регистр данных.

Соответственно, если управляющий кубит находится в произвольной суперпозиции состояний $|0\rangle$, $|1\rangle$, то результат действия гейта U имеет вид

$$U : \sum_{x=0}^1 \alpha_x |x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) = \sum_{x=0}^1 (-1)^{f(x)} \alpha_x |x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right). \quad (6.97)$$

В заключение подчеркнём, что оператор U можно также рассматривать как однокубитовый контролируемый оператор $c\text{-}U$, действующий на управляемый кубит с учётом состояния управляющего кубита. Соответствующая квантовая цепь может быть изображена эквивалентно, как показано на рис. 6.17.

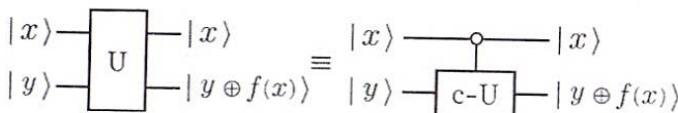


Рис. 6.17. Логическая диаграмма контролируемого унитарного оператора

6.8 Оценка собственного значения унитарного оператора

Процедура оценки фазы является ключевой для многих известных квантовых алгоритмов, в том числе и для квантового алгоритма вычисления собственного числа унитарного оператора.

Пусть имеется унитарный оператор \hat{U} , собственный вектор которого есть $|u\rangle_m$. Собственное число любого унитарного оператора по модулю равно единице, поэтому оно может быть представлено в виде $\exp(i2\pi\varphi_u)$, где $\varphi_u \in [0, 1]$. Уравнение на собственные векторы \hat{U} имеет вид

$$\hat{U}|u\rangle_m = \exp(i2\pi\varphi_u)|u\rangle_m.$$

Указанный выше диапазон изменения числа φ_u достаточен в силу периодичности экспоненты $\exp(i2\pi\varphi_u) = \exp(i2\pi(\varphi_u+k))$, где k – целое число. Таким образом, задача определения собственного числа унитарного оператора сводится к определению “фазового множителя” φ_u , что аналогично задаче оценки фазы.

Предположим далее, что имеется квантовая цепь, осуществляющая оператор контролируемого преобразования $c\text{-}U$. Соответственно, многокубитовый регистр результата (управляемый регистр) приготовлен в состоянии $|u\rangle_m$, а управляющий кубит – это однокубитовое состояние $|0\rangle$ или $|1\rangle$. При этом при значении управляющего кубита, совпадающего с $|0\rangle$, оператор U

не действует на собственный вектор $|u\rangle_m$, а в случае управляющего кубита $|1\rangle$ результат действия определяется выражением

$$c\text{-U} : |1\rangle \otimes |u\rangle_m = |1\rangle \otimes c\text{-U} : |u\rangle_m = \exp(i2\pi\varphi_u) |1\rangle \otimes |u\rangle_m. \quad (6.98)$$

Таким образом, можно сказать, что собственное значение оператора U после его действия на собственный вектор $|u\rangle_m$ возвращено управляющему кубиту. Поэтому, если управляющий кубит находится в произвольной суперпозиции базисных однокубитовых состояний, то применение $c\text{-U}$ гейта позволяет получить суперпозицию кубита, в которую введено собственное число оператора U :

$$c\text{-U} : (c_0|0\rangle + c_1|1\rangle) \otimes |u\rangle_m = \left(c_0|0\rangle + \exp(i2\pi\varphi_u)c_1|1\rangle \right) \otimes |u\rangle_m. \quad (6.99)$$

Решение задачи оценки фазы, как следует из (6.93), опирается на представление многокубитового регистра $|q\rangle_n$ в виде произведения

$$|q\rangle_n = \frac{|0\rangle + e^{i2\pi(2^{n-1}\varphi_u)}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{i2\pi(2^{n-2}\varphi_u)}|1\rangle}{\sqrt{2}} \otimes \dots \otimes \frac{|0\rangle + e^{i2\pi(2^0\varphi_u)}|1\rangle}{\sqrt{2}}. \quad (6.100)$$

Это означает, что если построить квантовую цепь, приводящую к созданию такого состояния, то, применив к этому состоянию обратное преобразование Фурье, можно вычислить приближённо (или в частных случаях точно) искомое собственное значение оператора U .

Для сокращения обозначений в изображении квантовой цепи данного алгоритма введём кубит $|s_k\rangle$ по определению:

$$|s_k\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + \exp(i2\pi 2^k\varphi_u)|1\rangle); \quad k = 0, 1, 2, \dots$$

В этом случае регистр $|q\rangle_n$ (6.100) имеет вид прямого произведения:

$$|q\rangle_n = |s_{n-1}\rangle \otimes |s_{n-2}\rangle \otimes \dots \otimes |s_1\rangle \otimes |s_0\rangle.$$

При построении состояния вида (6.100) необходимо отметить, что состояние $|u\rangle_m$ является собственным для U^2 с собственным числом, равным $\exp(2i2\pi\varphi_u)$. И аналогично для любого целого n имеет место общее равенство

$$U^n |u\rangle_m = \exp(n i 2\pi \varphi_u) |u\rangle_m.$$

Следовательно, для вычисления результата действия $c\text{-U}$ -гейта получим соотношение

$$(c\text{-U})^{2^n} : \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |u\rangle_m \right) = \left(\frac{|0\rangle + \exp(i2\pi(2^n\varphi_u))|1\rangle}{\sqrt{2}} \otimes |u\rangle_m \right). \quad (6.101)$$

На основании данного равенства очевидно, что квантовая цепь, приведённая ниже (рис. 6.18), формирует состояние, соответствующее выражению (6.100).

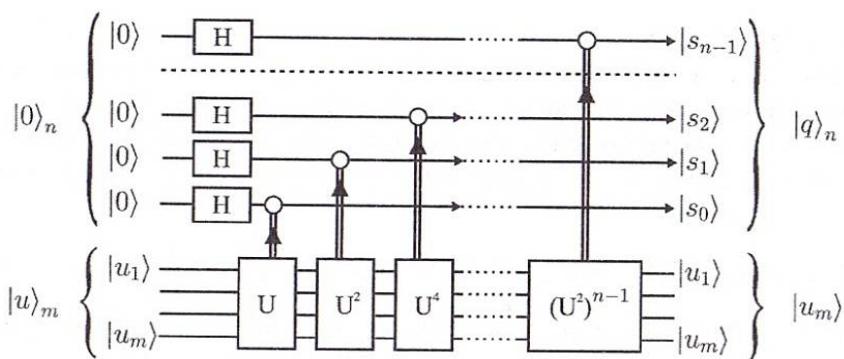


Рис. 6.18. Квантовая цепь предварительного этапа алгоритма оценки собственного числа унитарного оператора

В результате квантовый алгоритм оценки собственного значения унитарного оператора может быть определён в несколько этапов, и при его реализации используются два квантовых регистра. Первый регистр содержит n кубит, первоначально находящихся в состоянии $|0\rangle_n$. Второй регистр задаёт собственный вектор состояния $|u\rangle_m = |u_1, u_2, \dots, u_m\rangle$ и содержит столько кубит, сколько необходимо, чтобы определить $|u\rangle_m$.

Первый шаг процедуры оценки фазы определяется квантовой цепью, формирующей состояние (6.100) в первом регистре, и при этом не меняется состояние второго регистра. Данная цепь состоит в использовании гейта Уолша – Адамара в применении к первому регистру с последующим применением с-U-операций. Действие контролируемого U оператора определено равенством (6.101).

Второй шаг алгоритма оценки собственного числа состоит в применении алгоритма оценки фазы, т. е. в выполнении обратного квантового преобразования Фурье с первым регистром. Третий шаг – это измерение состояния первого регистра. Знание состояния первого регистра приблизённо определяет бинарное представление фазового множителя φ_u . Схематично весь алгоритм определяется квантовой цепью, представленной на рис. 6.19.

Формальное описание алгоритма оценки собственного числа унитарного оператора требует на входе квантовую машину, которая осуществляет контролируемую $(c\text{-}U)^k$ операцию для целого k . Кроме того, необходимо

собственное состояние $|u\rangle_m$ унитарного оператора \hat{U} с собственным числом $e^{i2\pi\varphi}$.

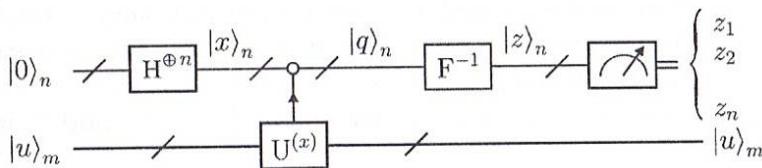


Рис. 6.19. Квантовая цепь алгоритма оценки собственного числа унитарного оператора

В результате для исходного регистра из n кубит, находящихся в состоянии $|0\rangle_n$, и регистра кубит $|u\rangle_m$ с собственными значениями оператора U (число кубит m выбирается так, чтобы задать собственное состояние $|u\rangle_m = |u_1, u_2, \dots, u_m\rangle$) реализуется следующий алгоритм:

1. Задание начального состояния двумя регистрами: $|0\rangle_n$ – регистр данных и $|u\rangle_m$ – регистр собственных чисел.

2. Создание суперпозиции вида $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle_n |u\rangle_m$.

3. Выполнение операции: $c-U \quad \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle_n, U^x |u\rangle_m = |q\rangle_n \otimes |u\rangle_m$.

4. Выполнение обратного Фурье-преобразования с регистром данных

$$\hat{F}^{-1} |q\rangle_n = |z\rangle_n.$$

5. Измерение регистра данных $|z\rangle_n = |z_1, z_2, \dots, z_n\rangle$. Битовое значение фазы φ определяется приближённым значением $\varphi_t \approx (z_1, z_2, \dots, z_n)$.

Процедура оценки фазы может быть использована также для решения ряда иных интересных в практическом смысле задач, таких как проблема нахождения периода и проблема факторизации чисел.

6.9 Алгоритм Шора

Известная задача факторизации целых чисел состоит в определении простых множителей p и q для заданного целого числа $N = p \cdot q$. Классическое решение такой задачи опирается на алгоритм нахождения порядка числа в арифметике по модулю. Порядком числа x по модулю N называется наименьшее натуральное число r , для которого выполняется равенство

$$x^r \bmod N = 1. \quad (6.102)$$

При этом число x удовлетворяет условию $x < N$ и, кроме того, числа x, N взаимно просты. Взаимная простота двух чисел означает, что наибольший общий делитель (gcd – greatest common divisor) этих чисел равен 1, или $gcd(x, N) = 1$. Исходя из определения порядка числа r ясно, что для него выполняется неравенство $1 < r < N$.

Порядок числа связан с периодом функции $f_m(x) = x^m \bmod N$, так как $f_{m+r}(x) = f_m(x)$:

$$f_{m+r}(x) = x^{m+r} \bmod N = [(x^m \bmod N) \cdot (x^r \bmod N)] \bmod N = f_m(x).$$

В данном равенстве учтено, что по определению (6.102) $x^r \bmod N \equiv 1$.

Используя выражение (6.102), можно построить алгоритм для определения простых множителей числа. Пусть задано число Z и требуется определить простые множители этого числа. Если число Z чётно, то будем делить это число на 2 до тех пор, пока результат деления не станет нечётным числом, которое обозначим через N . Далее выберем случайным образом число $x < N$. Если $gcd(x, N) = c$ и $c \neq 1$, то N можно разделить на c . Данный шаг можно повторять до тех пор, пока c не станет равным 1. Поэтому достаточно рассмотреть случай, когда нечётное число N и случайно выбранное число $0 < x < N$ взаимно просты. При этом, если N окажется степенью простого числа, то известен классический алгоритм, позволяющий за полиномиальное время распознать данное обстоятельство и найти это простое число. А вот если N состоит из несовпадающих простых со-множителей, то можно использовать классический алгоритм разложения числа N на основе определения порядка числа по модулю.

Такой алгоритм можно обосновать следующими рассуждениями. Пусть порядок r числа x по модулю N есть чётное число. Если окажется, что порядок r числа x по модулю N нечётен, то необходимо выбрать иное случайное число x так, чтобы r был чётным числом. Это всегда возможно, так как в соответствии с алгоритмом выбор числа x случаен. Так как порядок r – чётное число, вместо x можно определить новую переменную $y \equiv x^{r/2}$. На основании (6.102) для y выполняется равенство $y^2 \bmod N = 1$, которое можно переписать тождественно в виде

$$(y^2 - 1) \bmod N = 0, \quad \text{или} \quad [(y + 1)(y - 1)] \bmod N = 0. \quad (6.103)$$

Покажем, что равенство нулю в данном соотношении означает, что произведение сомножителей $(y + 1)(y - 1)$ делится на N без остатка. Перепишем выражение (6.103) тождественно с учетом ассоциативности произведения

чисел по модулю:

$$\left[(y+1) \bmod N \right] \cdot \left[(y-1) \bmod N \right] \bmod N = (y_+ \cdot y_-) \bmod N = 0. \quad (6.104)$$

Здесь $y_{\pm} \equiv (y \pm 1) \bmod N$. Равенство (6.104) выполняется в следующих трёх случаях:

1. $y_+ = 0$. Это означает, что $y + 1 = N$ в силу того, что $N \bmod N = 0$ и, следовательно,

$$(y-1) \bmod N = (N-2) \bmod N,$$

а $\gcd(y_-, N) = 1$, так как N и $N - 2$ — два соседних нечётных числа, которые всегда являются взаимно простыми. Таким образом, имеем тривиальные множители числа N , равные N и 1, так как $\gcd(y_+, N) = N$ и $\gcd(y_-, N) = 1$.

2. $y_- = 0$. В этом случае $y - 1 = N$, следовательно,

$$(y+1) \bmod N = (N+2) \bmod N, \quad N = 2 \bmod N = 2,$$

так как $N \bmod N = 0$. Отсюда ясно, что $\gcd(y_+, N) = \gcd(2, N) = 1$, поскольку N нечётно. И аналогично предыдущему случаю также возникают только тривиальные сомножители числа N , равные N и 1.

3. Равенство (6.104) выполняется, если $y_+ \cdot y_- = kN$, где $0 < k < N$. Другими словами, произведение сомножителей $y_+ \cdot y_-$ должно иметь общий (или общие) множитель (или множители) с N . Таким образом, нетривиальные множители числа N есть $\gcd(y_+, N) = c_1$ и $\gcd(y_-, N) = c_2$.

Окончательно в простейшем случае классический алгоритм нахождения сомножителей простого числа N с использованием чётного порядка произвольного x , удовлетворяющего условиям $x < N$ и $\gcd(x, N) = 1$, приводит к следующим правилам вычисления сомножителей данного числа: $N = c_1 \cdot c_2$;

$$c_1 = x^{r/2} + 1; \quad c_2 = x^{r/2} - 1.$$

Пусть, например, $N = 15$ [3]. Выберем значение x равным 2. Очевидно, что числа $x = 2$ и $N = 15$ взаимно простые, $\gcd(2, 15) = 1$. В этом случае последовательность чисел x^n по модулю 15 формируется следующим образом:

n	0	1	2	3	4	5	6	7	8	...
x^n	2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	...
Десятичное число	1	2	4	8	16	32	64	128	256	...
$x^n \bmod 15$	1	2	4	8	1	2	4	8	1	...

Таким образом, последовательность чисел $x^n \equiv 2^n$ по модулю 15 имеет период по n , равный $r = 4$. Если известен период r , множители числа N определяются с помощью классического алгоритма Евклида как наибольшие общие делители чисел $2^{r/2} \pm 1$ и N . В рассматриваемом примере $2^{4/2} \pm 1 = (5, 3)$. В данном тривиальном случае эти числа сами являются наибольшими общими делителями числа 15. Другими словами, на основе найденного порядка $r = 4$ установлено, что число $15 = 5 \cdot 3$ состоит из двух сомножителей (5 и 3).

Можно продемонстрировать, что при заданном N выбор числа x относительно произведен. Например, при $N = 39$ можно случайно выбрать $x = 5$. В этом случае последовательность $5^n \bmod 39$, $n \in 1, 2, 3, \dots$ определяется значениями 5, 25, 8, 1, 5, 25, 8, 1, ... и имеет период, равный $r = 4$. Следовательно, для определения множителей N надо найти наибольшие общие делители $\gcd(5^2 + 1, 39) = 13$ и $\gcd(5^2 - 1, 39) = 3$. Отсюда вытекает, что $N = 13 \cdot 3$, т. е. найдены два множителя числа 39.

Соответственно, если случайно было выбрано число $x = 29$ (вместо 5), то последовательность значений функции $29^n \bmod 39$ есть

$$29, 22, 14, 16, 35, 1, 29, 22, 14, 16, 36, 1, \dots,$$

а период такой последовательности равен 6. Отсюда

$$y = x^{r/2} \bmod 39 = (29^3) \bmod 39 = 14,$$

$\gcd(y + 1, 39) = \gcd(15, 39) = 3$, $\gcd(y - 1, 39) = \gcd(13, 39) = 13$, и, таким образом, получим, что $39 = 3 \cdot 13$.

Для справки отметим, что в общем случае классический алгоритм Евклида поиска наибольшего общего делителя $\gcd(n_0, n_1)$ для пары чисел $n_0 \geq n_1$ состоит в выполнении указанных ниже последовательных делений:

$$\begin{aligned} n_0 &= d_1 \times n_1 + n_2, \\ n_1 &= d_2 \times n_2 + n_3, \\ &\dots \\ n_{m-2} &= d_{m-1} \times n_{m-1} + n_m, \\ n_{m-1} &= d_m \times n_m + 0, \end{aligned}$$

где d_m — целая часть от деления $n_{m-1} \geq n_m$ на каждом шаге. Последний ненулевой сомножитель n_m является искомым наибольшим общим делителем. Например, нахождение $\gcd(91, 28)$ определяется последовательно-

стью вычислений:

$$\begin{aligned} 91 &= 3 \cdot 28 + 7, \\ 28 &= 4 \cdot 7 + 0, \end{aligned}$$

которая показывает, что наибольший общий делитель пары чисел (91, 28) равен 7. Как видно, для определения наибольшего общего делителя в данном примере потребовалось два шага. В общем случае число шагов порядка $\sim \log \log n_1$.

В настоящее время известно много различных классических алгоритмов разложения числа на простые множители. Однако даже наилучшие классические алгоритмы требуют экспоненциального по $\log_2^{1/3}(N)$ числа шагов, которые оцениваются по формуле

$$O\left(\exp\left[c \cdot \log_2^{1/3} \log_2^{2/3}(\log_2(N))\right]\right),$$

где c — некоторая постоянная, а N — большое число.

Квантовый алгоритм факторизации чисел, предложенный Шором, состоит из двух частей (квантовой и классической). Квантовая часть алгоритма представляет собой квантовое решение задачи нахождения порядка. Квантовая цепь алгоритма позволяет факторизовать большое число N за полиномиальное $O(\log_2^3(N))$ число шагов в отличие от экспоненциального числа шагов для классических алгоритмов.

Квантовый алгоритм Шора [19] использует два квантовых регистра X и Y , первоначально находящихся в нулевом булевском состоянии $|0\rangle_n$. В регистре X размещаются аргументы функции $f(x)$. Например, при использовании 2^n чисел в качестве аргументов функции $f(x)$ потребуется регистр $|x\rangle_n = |x_{n-1}, x_{n-2}, \dots, x_0\rangle \equiv |x_{n-1}\rangle \otimes |x_{n-2}\rangle \otimes \dots \otimes |x_0\rangle$. Регистр Y используется для размещения значений самой функции $f(x)$ с подлежащим определению периодом r . В общем случае число кубит данного регистра также равно n .

Первый шаг квантового алгоритма состоит в переводе начального состояния $|0\rangle_n$ регистра X в равновероятную суперпозицию всех булевых состояний путём применения операции Уолша – Адамара. Регистр Y на данном этапе не меняется. В результате для системы двух регистров X и Y получается состояние

$$|\phi_1\rangle_{n+n} = \sqrt{\frac{1}{2^n}} \sum_{k=0}^{2^n-1} |k\rangle_n \otimes |0\rangle_n.$$

Допустим далее, что имеется некоторый оператор (квантовый гейт) \hat{U} , создающий в регистре Y значение $f(x) = x^k \bmod N$, где x и N – два целых взаимно простых числа $x < N$, для которых $\gcd(x, N) = 1$. Тогда вторым шагом квантовой части алгоритма является преобразование вида $\hat{U} : |\phi_1\rangle_{n+n} \rightarrow |\phi_2\rangle_{n+n}$, формирующее состояние $|\phi_2\rangle_{n+n}$:

$$|\phi_2\rangle_{n+n} = \sqrt{\frac{1}{2^n}} \sum_{k=0}^{2^n-1} |k\rangle_n \otimes |x^k \bmod N\rangle_n. \quad (6.105)$$

Так, например, при $N = 15$ и $x = 2$ состояние $|\phi_2\rangle_{n+n}$ есть

$$\begin{aligned} |\phi_2\rangle_{n+n} &= \sqrt{\frac{1}{2^n}} \sum_{k=0}^{2^n-1} |k\rangle_n \otimes |2^k \bmod 15\rangle_n = \\ &= \frac{1}{\sqrt{2^n}} \left[|0\rangle_n \otimes |1\rangle_n + |1\rangle_n \otimes |2\rangle_n + |2\rangle_n \otimes |4\rangle_n + |3\rangle_n \otimes |8\rangle_n + \right. \\ &\quad + |4\rangle_n \otimes |1\rangle_n + |5\rangle_n \otimes |2\rangle_n + |6\rangle_n \otimes |4\rangle_n + |7\rangle_n \otimes |8\rangle_n + \\ &\quad \left. + \dots + |2^n - 1\rangle_n \otimes |2^{2^n-1} \bmod 15\rangle_n \right]. \end{aligned} \quad (6.106)$$

Выбор числа кубит n в общем случае определяется точностью вычислений. Обычно можно положить $n \approx \log_2(N^2)$. То есть, если в рассматриваемом случае $N = 15$, отсюда $n = \log_2(15^2) \approx 8$ и $2^8 = 256$. Перегруппируем слагаемые в (6.106) следующим очевидным образом:

$$\begin{aligned} |\phi_2\rangle_{8+8} &= \sqrt{\frac{1}{256}} \sum_{k=0}^{255} |k\rangle_8 \otimes |2^k \bmod 15\rangle_8 = \\ &= \frac{1}{\sqrt{256}} [|0\rangle_8 + |4\rangle_8 + |8\rangle_8 + \dots + |248\rangle_8 + |252\rangle_8] \otimes |1 = 2^0 \bmod 15\rangle_8 + \\ &\quad + \frac{1}{\sqrt{256}} [|1\rangle_8 + |5\rangle_8 + |9\rangle_8 + \dots + |249\rangle_8 + |253\rangle_8] \otimes |2 = 2^1 \bmod 15\rangle_8 + \\ &\quad + \frac{1}{\sqrt{256}} [|2\rangle_8 + |6\rangle_8 + |10\rangle_8 + \dots + |250\rangle_8 + |254\rangle_8] \otimes |4 = 2^2 \bmod 15\rangle_8 + \\ &\quad + \frac{1}{\sqrt{256}} [|3\rangle_8 + |7\rangle_8 + |11\rangle_8 + \dots + |251\rangle_8 + |255\rangle_8] \otimes |8 = 2^3 \bmod 15\rangle_8 = \\ &= \sum_{k=0}^3 \left(\frac{1}{\sqrt{256}} \sum_{m=0}^{63} |k + 4 \cdot m\rangle_8 \right) \otimes |2^k \bmod 15\rangle_8. \end{aligned} \quad (6.107)$$

Можно отметить, что число слагаемых при каждом из четырёх состояний регистра функций одинаково, так как период выбранной функции r случайно оказался целой степенью 2, т. е. $r = 4 = 2^2$. В произвольном случае это не так.

Равенство (6.107) означает, что если в данной суперпозиции произвести измерение регистра Y , то результатом будет одно из четырёх возможных состояний данного регистра: $|1\rangle_8$, $|2\rangle_8$, $|4\rangle_8$ или $|8\rangle_8$. Пусть, например, результат измерения оказался совпадающим с состоянием $|4\rangle_8$. Это означает, что общее состояние редуцируется до нормированного на единицу состояния вида, в котором в регистре аргумента остаётся суперпозиция регистров, нумерация которых образует последовательность чисел с периодом $r = 4$:

$$\begin{aligned} |\phi_2\rangle_{8+8} &\Rightarrow \overline{|\varphi_2\rangle_{8+8}} = \\ &= \frac{1}{\sqrt{64}} \left[|2\rangle_8 + |6\rangle_8 + |10\rangle_8 + \dots + |250\rangle_8 + |254\rangle_8 \right] \otimes |4 = 2^2 \bmod 15\rangle_8. \end{aligned}$$

Для произвольного (одного из четырёх возможных) результата измерения регистра Y можно записать следующее общее редуцированное состояние:

$$\overline{|\varphi_{2,k}\rangle_{8+8}} = \frac{1}{\sqrt{64}} \sum_{m=0}^{63} |k + 4 \cdot m\rangle_8 \otimes |2^k \bmod 15\rangle_8, \quad k \in 0, 1, 2, 3. \quad (6.108)$$

Измерение состояния регистра Y является третьим шагом алгоритма Шора, в результате выполнения которого в регистре X сформируется суперпозиция регистров, определяемых набором десятичных чисел, имеющих период, равный периоду заданной функции.

На четвёртом шаге алгоритма выполняется обратное квантовое преобразование Фурье (6.41) с регистром данных $X = |k + 4 \cdot m\rangle_8$ из (6.108):

$$F^{-1} : |k + r \cdot m\rangle_8 = \frac{1}{\sqrt{256}} \sum_{j=0}^{255} \exp \left[-i \frac{2\pi}{256} (k + r \cdot m) j \right] |j\rangle_8.$$

В целом, для состояния $\overline{|\varphi_{2,k}\rangle_{8+8}}$ с учётом обратного преобразования Фурье с регистром X получим

$$\overline{|\varphi_{2,k}\rangle_{8+8}} = \frac{1}{\sqrt{256 \cdot 64}} \sum_{j=0}^{255} \sum_{m=0}^{63} \exp \left[-i \frac{2\pi}{256} (k + r \cdot m) j \right] |j\rangle_8 \otimes |2^k \bmod 15\rangle_8. \quad (6.109)$$

Если после выполненного преобразования Фурье измерить состояние регистра X , то с вероятностью $p_j = |a_j|^2$ будет получено какое-то восьмикубитовое состояние $|j\rangle_8$, где амплитуда вероятности a_j равна

$$\begin{aligned} a_j &= \frac{1}{\sqrt{256 \cdot 64}} \exp\left(-i \frac{2\pi}{256} k \cdot j\right) \sum_{m=0}^{63} \left[\exp\left(-i \frac{2\pi}{256} r \cdot j\right) \right]^m = \\ &= \frac{1}{\sqrt{256 \cdot 64}} \exp\left(-i \frac{2\pi}{256} k \cdot j\right) \frac{1 - \exp\left(-i \frac{2\pi}{256} r \cdot j \cdot m'\right)}{1 - \exp\left(-i \frac{2\pi}{256} r \cdot j\right)}, \quad m' = 64. \end{aligned} \quad (6.110)$$

Соответственно, вероятность измерения p_j состояния j в регистре данных X с учётом равенства $|1 - \exp(i 2\alpha)|^2 = 4 \sin^2(\alpha)$ можно переписать в виде

$$p_j = |a_j|^2 = \frac{1}{256 \cdot 64} \frac{\sin^2\left(\pi r \cdot j \cdot m'/256\right)}{\sin^2\left(\pi r \cdot j/256\right)}. \quad (6.111)$$

График функции p_j , как функции j , при $r = 4$, представлен на рис. 6.20.

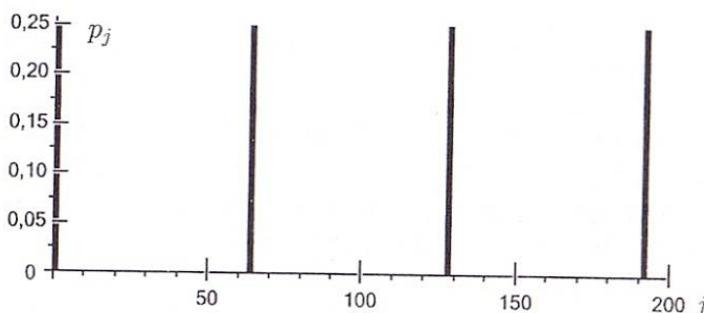


Рис. 6.20. Сингулярное поведение вероятности измерения состояния j

Из рисунка видно, что значение вероятности (6.111) периодически принимает отличное от нуля значение. То есть результатом измерения состояния $|j\rangle_8$ может быть только какое-то число из последовательности 0, 64, 128, 192. Как следует из (6.111), ненулевое значение p_j достигается при условии $r j / 256 = k$, где $k \in 1, 2, 3, \dots$. Поэтому, если результатом измерения явилось значение, равное j , то должно выполняться такое равенство $k/r = j/256$, где k – некоторое целое число. Данное заключение позволяет классическим вычислением определить период r по результатам измерения регистра данных после обратного квантового Фурье-преобразования.

Действительно, пусть результат измерения, например, оказался равным 64. Тогда на основании этого измерения можно заключить, что так как должно выполняться равенство $k/r = 64/256$ или $k/r = 1/4$, то, следовательно, $r = 4$, а k в этом случае равно 1. Если бы результат измерения оказался равным, например, 192, то мы пришли бы к выводу, что $k/r = 192/256 = 3/4$ или $r = 4$, а k в этом случае равно 3. Простая классическая проверка показывает, что найденный результат $r = 4$ удовлетворяет необходимому условию $2^4 \bmod 15 = 1$, следовательно, множителями числа 15 являются два числа, равные $2^{4/2} + 1 = 5$ и $2^{4/2} - 1 = 3$. Этими классическими вычислениями и заканчивается алгоритм Шора.

Конечно, в общем случае r необязательно является числом, совпадающим с целой степенью двойки, как это было в приведённом выше примере. Однако изложенный выше алгоритм позволяет найти множители числа и в этом произвольном случае, так как при произвольных параметрах x, N для нахождения r в сравнении $x^r \bmod N = 1$ алгоритм Шора приведёт к обобщению выражения (6.111) и будет иметь вид

$$p_j = |a_j|^2 = \frac{1}{2^n \cdot m'} \frac{\sin^2(\pi r \cdot j \cdot m'/2^n)}{\sin^2(\pi r \cdot j/2^n)}, \quad (6.112)$$

где, как и раньше, n — число кубит в регистре данных, которое определяется как ближайшее целое от $\log_2(N^2)$, но m' зависит от того, какое конкретно состояние из состояний $|x^r \bmod N\rangle_n$ будет получено на третьем шаге алгоритма при измерении регистра функций. Квантовая цепь алгоритма Шора схематично представлена на рис. 6.21.

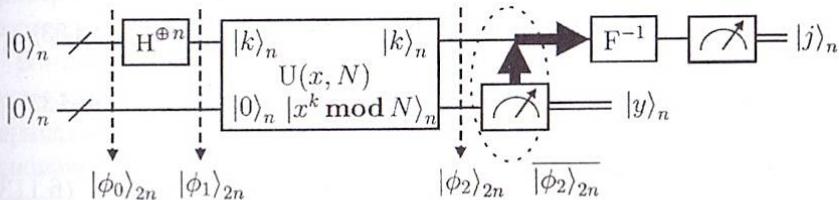


Рис. 6.21. Логическая диаграмма алгоритма Шора

Рассмотренный алгоритм факторизации является определённым стимулом для проведения экспериментальных измерений с квантовыми системами. Принципиальным в этих экспериментах является вопрос о возможности реализации алгоритма на квантовых системах для целых чисел, представляющих коммерческий интерес в криптографии. В работе [16] показано, что реализация операторов поворота на угол $\pi/64$ позволяет факторизовать целые числа длиной до тысячи бит.

Пример 6.4. Пример использования алгоритма Шора

В качестве менее тривиального примера рассмотрим случай выбора исходных данных, когда $x = 5$, а $N = 33$. При данном выборе условий задачи $n = \log_2(33^2) \approx 11$ и $2^{11} = 2048$. Соответственно, после второго шага квантового алгоритма получим перегруппированную суперпозицию вида

$$\begin{aligned}
 |\phi_2\rangle_{11+11} &= \sqrt{\frac{1}{2048}} \sum_{k=0}^{2047} |k\rangle_{11} \otimes |5^k \bmod 33\rangle_{11} = \\
 &= \frac{1}{\sqrt{2048}} [|0\rangle_{11} + |10\rangle_{11} + |20\rangle_{11} + \dots + |2030\rangle_{11} + |2040\rangle_{11}] \otimes |1 = 5^0 \bmod 33\rangle_{11} + \\
 &+ \frac{1}{\sqrt{2048}} [|1\rangle_{11} + |11\rangle_{11} + |21\rangle_{11} + \dots + |2031\rangle_{11} + |2041\rangle_{11}] \otimes |5 = 5^1 \bmod 33\rangle_{11} + \\
 &+ \frac{1}{\sqrt{2048}} [|2\rangle_{11} + |12\rangle_{11} + |22\rangle_{11} + \dots + |2032\rangle_{11} + |2042\rangle_{11}] \otimes |25 = 5^2 \bmod 33\rangle_{11} + \\
 &+ \frac{1}{\sqrt{2048}} [|3\rangle_{11} + |13\rangle_{11} + |23\rangle_{11} + \dots + |2033\rangle_{11} + |2043\rangle_{11}] \otimes |26 = 5^3 \bmod 33\rangle_{11} + \\
 &+ \frac{1}{\sqrt{2048}} [|4\rangle_{11} + |14\rangle_{11} + |24\rangle_{11} + \dots + |2034\rangle_{11} + |2044\rangle_{11}] \otimes |31 = 5^4 \bmod 33\rangle_{11} + \\
 &+ \frac{1}{\sqrt{2048}} [|5\rangle_{11} + |15\rangle_{11} + |25\rangle_{11} + \dots + |2035\rangle_{11} + |2045\rangle_{11}] \otimes |23 = 5^5 \bmod 33\rangle_{11} + \\
 &+ \frac{1}{\sqrt{2048}} [|6\rangle_{11} + |16\rangle_{11} + |26\rangle_{11} + \dots + |2036\rangle_{11} + |2046\rangle_{11}] \otimes |16 = 5^6 \bmod 33\rangle_{11} + \\
 &+ \frac{1}{\sqrt{2048}} [|7\rangle_{11} + |17\rangle_{11} + |27\rangle_{11} + \dots + |2037\rangle_{11} + |2047\rangle_{11}] \otimes |14 = 5^7 \bmod 33\rangle_{11} + \\
 &+ \frac{1}{\sqrt{2048}} [|8\rangle_{11} + |18\rangle_{11} + |28\rangle_{11} + \dots + |2028\rangle_{11} + |2038\rangle_{11}] \otimes |4 = 5^8 \bmod 33\rangle_{11} + \\
 &+ \frac{1}{\sqrt{2048}} [|9\rangle_{11} + |19\rangle_{11} + |29\rangle_{11} + \dots + |2029\rangle_{11} + |2039\rangle_{11}] \otimes |20 = 5^9 \bmod 33\rangle_{11} = \\
 &= \sum_{k=0}^9 \left(\frac{1}{\sqrt{2048}} \sum_{m=0}^{m'-1} |k + 10 \cdot m\rangle_{11} \right) \otimes |5^k \bmod 33\rangle_{11}. \tag{6.113}
 \end{aligned}$$

Как видно из (6.113), в двух частных случаях, когда в регистре Y образуются состояния вида $|4 = 5^8 \bmod 33\rangle_{11}$ и $|20 = 5^9 \bmod 33\rangle_{11}$, число соответствующих состояний в регистре X равно 203, т. е. $m' = 204$, а во всех остальных случаях число состояний $m' = 205$. Это различие состояний является источником неточности вычислений для случая, когда период числа по модулю не является числом, совпадающим с целой степенью 2.

После измерения регистра Y получим какую-то одну из десяти возможных суперпозиций в регистре X , которые в общем виде могут быть записаны следующим образом:

$$\overline{|\varphi_{2,k}\rangle_{11+11}} = \frac{1}{\sqrt{m'}} \sum_{m=0}^{m'-1} |k + 10 \cdot m\rangle_{11} \otimes |5^k \bmod 33\rangle_{11}, \quad (6.114)$$

где $k \in 0, 1, 2, \dots, 8, 9$. Если теперь выполнить обратное квантовое преобразование Фурье с регистром X полученного состояния и измерить регистр данных X , то вероятность измерения значения j в регистре X определяется выражением

$$p_j = \frac{1}{2048 \cdot m'} \frac{\sin^2(\pi 10 \cdot j \cdot m'/2048)}{\sin^2(\pi 10 \cdot j/2048)}. \quad (6.115)$$

График функции $p(j)$ имеет максимумы при $j = 0, 205, 410, 615, 820, 1025, 1230, 1435, 1640, 1845$. То есть результатом измерения окажется какое-то число из этой последовательности или (с учётом ошибок измерения) близкое к этим целым числам. Например, если результатом измерения окажется число, равное 820, то из классических вычислений находим:

$$820/2048 = 0,400390625 \approx 4/10.$$

Следовательно, можно заключить, что $k/r = 4/10$, т. е. период $r = 10$ или $k/r' = 2/5$, тогда нужно сделать вывод, что $r' = 5$. Однако прямая проверка показывает, что $5^5 \bmod 33 = 23 \neq 1$ и, следовательно, $r' = 5$ не является искомым периодом.

В то же время $5^{10} \bmod 33 = 1$ и, следовательно, $r = 10$ есть искомый период. В свою очередь, $r' = 5$ показывает, что это множитель искомого периода $r = r' \cdot 2$, но не сам период. После того как период определён на основании квантовой части алгоритма, множители числа $33 = p \cdot q$ находятся на основании классического алгоритма путём вычисления

$$d_1 = 5^{10/2} + 1 = 24, \quad d_2 = 5^{10/2} - 1 = 22$$

и $p = \gcd(d_1, N) = \gcd(24, 33) = 3$, $q = \gcd(d_2, N) = \gcd(22, 33) = 11$. Окончательный ответ настоящего примера: $33 = 3 \cdot 11$.

Упражнение 6.7. Используя квантовый алгоритм Шора, показать, что 21 является произведением двух простых чисел 3 и 7.

Упражнение 6.8. Используя классические алгоритмы для чётных чисел и квантовые для нечётных, найти множители числа 360.

6.10 Алгоритм Гровера (поиск в базе данных)

Данный алгоритм решает задачу поиска заданного элемента в неупорядоченной базе данных с использованием свойства усиления амплитуды вероятности квантового состояния при выполнении определённой процедуры с квантовым регистром.

Прежде чем рассматривать квантовый алгоритм Гровера, рассмотрим простой пример классических вычислений, из которого будет ясна идеология квантового алгоритма. Пусть есть неупорядоченная база данных, содержащая N элементов: $x_1, x_2, x_3, \dots, x_N$. Этими элементами могут быть любые сущности: номера телефонов, фотографии, идентифицирующие людей, детали какого-то производства и т. д. Если требуется найти в этой базе конкретный элемент, который обозначим через z , то процедура отыскания этого элемента будет состоять в случайному переборе элементов базы x_i и "сравнении" их с образцом для поиска z . Когда окажется, что $x_i = z$, можно утверждать, что искомый элемент найден. Очевидно, что если размер базы N , то может потребоваться $\mathcal{O}(N)$ испытаний для отыскания конкретного элемента. Обозначим амплитуду вероятности извлечения x_i -го элемента через a_i и допустим, что вероятности $p_i = |a_i|^2$ извлечения из базы всех элементов одинаковы, тогда $a_i = 1/\sqrt{N}$.

Выполним циклически три операции, определённые следующими тремя шагами, и проследим за изменением величины амплитуд извлечения элементов из базы:

1-й шаг: вычисление среднего значения амплитуды $\langle a \rangle$ для всех элементов базы данных:

$$\langle a \rangle = \frac{1}{N} \sum_{i=1}^N a_i.$$

2-й шаг: преобразование амплитуд в соответствии с выражением

$$a_i = 2 \langle a \rangle - a_i, \quad i \in 1, 2, \dots, N.$$

3-й шаг: изменение знака амплитуды искомого элемента в базе данных на противоположный: $a_p \rightarrow -a_p$.

Пусть, например, число элементов базы $N = 32$, а искомым элементом является третий элемент x_3 . Исходное равновероятное значение амплитуд $a_i = 1/\sqrt{N} \approx 0,17678\dots$. Тогда после первой итерации выполнения указанных выше операций получим $\langle a \rangle = 0,17678\dots, a_3 = -0,17678\dots$, а остальные амплитуды $a_i = 0,17678\dots$. Выполняя далее указанные выше шаги циклически, получим результаты, представленные в табл. 6.1.

Таблица 6.1

Результаты пошаговой итерации

Номер итерации	a_3	$a_i, i \neq 3$	$\langle a \rangle$
1	-0,17678 ...	0,17678 ...	0,17678 ...
2	-0,50823 ...	0,15468 ...	0,16728 ...
3	-0,77616 ...	0,11325 ...	0,13396 ...
4	-0,94707 ...	0,05766 ...	0,08545 ...
5	-0,99959 ...	-0,00513 ...	0,02626 ...
6	-0,92717 ...	-0,06729 ...	-0,03621 ...
7	-0,73884 ...	-0,12103 ...	-0,09416 ...
8	-0,45817 ...	-0,15964 ...	-0,14034 ...
9	-0,12022 ...	-0,17830 ...	-0,16897 ...
10	0,23275 ...	-0,17467 ...	-0,17649 ...
14	0,99632 ...	0,01539 ...	-0,01622 ...
23	-0,98979 ...	-0,02559 ...	-0,00613 ...

Из данной таблицы видно, что на пятой итерации амплитуда искомого состояния достигает максимума, равного $a_3 = -0,99959\dots$. То есть после пятой итерации (отметим, что $5 \approx \sqrt{N}$) практически с вероятностью, равной единице, из базы данных будет извлечён искомый элемент. К сожалению, представленная процедура не имеет практического смысла, так как мы заранее знаем, с каким элементом надо провести специальное преобразование на третьем шаге. Однако нужно отметить, что рассмотренная математическая процедура привела к усилению амплитуды вероятности извлечения искомого элемента из базы практически до единицы.

Именно это обстоятельство позволяет сформулировать эффективный квантовый алгоритм на принципе усиления амплитуды искомого состояния. В квантовом устройстве вычисление функции от всех элементов базы и их сравнение с образцом осуществляются за один шаг. Однако использовать это обстоятельство непосредственно не удается, так как в результате измерения регистра функций, осуществляющей сравнение, с равной вероятностью может быть получен и результат, не относящийся к искомому элементу. Но если выполнить порядка \sqrt{N} указанных выше итераций с вероятностью, близкой к единице, измерение регистра функций укажет именно на искомый элемент. В этом и состоит идеология квантового алгоритма Гровера. Терминологически элементы базы данных, которые являются искомыми объектами, называются маркованными, а остальные — немаркованными.

На первом шаге реализации квантового алгоритма Гровера формируется квантовый регистр, содержащий n штук кубит, что соответствует размеру базы данных $N = 2^n$. Данный начальный регистр инициализируется в состоянии $|\varphi_0\rangle_n = |0\rangle_n$. В результате действия гейта Уолша – Адамара регистр переводится в равновероятную суперпозицию всех состояний:

$$|\varphi_1\rangle_n = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle_n. \quad (6.116)$$

На втором шаге алгоритма для обеспечения различия между маркированным и немаркованными состояниями вводится специальный гейт \hat{O}_{x_0} , получивший в литературе наименование Оракул. Данный гейт умножает амплитуду маркированного состояния $|x_0\rangle_n$ на -1 , оставляя амплитуды остальных состояний неизменными:

$$\hat{O}_{x_0} : |x\rangle_n = (-1)^{f(x)} |x\rangle_n, \quad f(x_0) = 1, \quad f(x \neq x_0) = 0. \quad (6.117)$$

Определение функции $f(x)$ несёт на себе кажущееся противоречие: она "знает" ответ задачи, и, следовательно, в поиске нет смысла. Однако надо иметь в виду, что равенство $x = x_0$ устанавливается во время операции сравнения всех элементов с образцом за один ход квантового вычисления и знание "номера" маркированного элемента исходно не требуется.

Техническое построение Оракула возможно, например, путём добавления к регистру $|x\rangle_n$ дополнительного кубита $|q\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ и выполнения следующей операции:

$$\hat{O}_{x_0} : |x\rangle_n \otimes |q\rangle = |x\rangle_n \otimes \hat{X}^{f(x)} : |q\rangle,$$

где $\hat{X}^{f(x)}$ совпадает с квантовым оператором отрицания X кубита $|q\rangle$ при $f(x_0) = 1$ и является тождественным оператором при $f(x \neq x_0) = 0$, так как $\hat{X}^0 \equiv I$. Соответственно, при $x = x_0$ имеем

$$\hat{X} : |q\rangle = (-|0\rangle + |1\rangle)/\sqrt{2} = -|q\rangle.$$

Таким образом, $\hat{O}_{x_0} : |x\rangle_n \otimes |q\rangle = (-1)^{f(x)} |x\rangle_n \otimes |q\rangle$, что и преобразует состояние $|x\rangle_n \rightarrow (-1)^{f(x)} |x\rangle_n$. Другими словами, амплитуда маркированного состояния поменяет знак.

Гейт \hat{O}_{x_0} можно представить и в операторном виде:

$$\hat{O}_{x_0} = I - 2 |x_0\rangle_n \langle x_0|_n, \quad (6.118)$$

так как прямое произведение векторов вычислительного базиса $|k\rangle_n \langle k|_n$ приводит к матрице размерности $N \times N$. При этом все матричные элементы $a_{i,j}$ такой матрицы равны 0, кроме одного матричного элемента $a_{k,k}$.

Соответственно, вычитая удвоенную матрицу такого прямого произведения из единичной матрицы, получим матрицу, отличающуюся от единичной тем, что матричный элемент $a_{k,k} = 1$ заменяется на $a_{k,k} = -1$.

В качестве примера рассмотрим случай маркированного состояния под номером 1 в базе данных с $N = 4$. В этом случае маркированное состояние $|x_0\rangle$ совпадает с базисным состоянием $|1\rangle_2 = |0, 1\rangle$. В результате

$$\hat{O}_1 = I - 2 |1\rangle_2 \langle 1|_2 = I - 2 |1\rangle_2 \left(|1\rangle_2 \right)^\dagger = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \quad (6.119)$$

Продолжая общее рассмотрение квантового алгоритма Гровера, можно сказать, что в результате действия Оракула (выполнение второго шага алгоритма) в регистре базы данных возникает состояние $|\varphi_2\rangle_n$, равное

$$|\varphi_2\rangle_n = \hat{O}_{x_0} : |\varphi_1\rangle_n = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} (-1)^{f(x)} |x\rangle_n = \sum_{x=0}^{N-1} \alpha_x |x\rangle_n. \quad (6.120)$$

На третьем шаге алгоритма Гровера выполняется операция инверсии относительно среднего, которая, как показано в классическом случае, приводит к усилению маркированной (распознанной в результате сравнения) амплитуды. Так как среднее значение амплитуд в произвольном состоянии регистра базы данных равно по определению

$$\langle \alpha \rangle = \frac{1}{N} \sum_{x=0}^{N-1} \alpha_x, \quad (6.121)$$

то операция инверсии амплитуд относительно среднего в регистре базы данных приводит к состоянию $|\varphi_3\rangle_n$:

$$\begin{aligned} |\varphi_3\rangle_n &= \sum_{x=0}^{N-1} (2 \langle \alpha \rangle - \alpha_x) |x\rangle_n = \\ &= 2 \langle \alpha \rangle \sum_{x=0}^{N-1} |x\rangle_n - |\varphi_2\rangle_n = 2 \langle \alpha \rangle \sqrt{N} |\varphi_1\rangle_n - |\varphi_2\rangle_n. \end{aligned} \quad (6.122)$$

Для дальнейших преобразований рассмотрим вспомогательное выражение $\langle \varphi_1 | \varphi_2 \rangle_n$. В соответствии с определением состояний $|\varphi_1\rangle_n$ и $|\varphi_2\rangle_n$ получим

$$\langle \varphi_1 | \varphi_2 \rangle_n = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \langle x |_n \sum_{x'=0}^{N-1} \alpha_{x'} |x'\rangle_n = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \alpha_x = \sqrt{N} \langle \alpha \rangle.$$

Таким образом, с учётом найденного равенства $\langle \varphi_1 | \varphi_2 \rangle = \sqrt{N} < \alpha >$ состояние $|\varphi_3\rangle_n$ в (6.122) можно переписать в виде

$$|\varphi_3\rangle_n = 2 |\varphi_1\rangle_n \langle \varphi_1 | \varphi_2 \rangle_n - |\varphi_2\rangle_n$$

или с использованием операторного равенства $|\varphi_3\rangle_n = \hat{U} |\varphi_2\rangle_n$, где оператор \hat{U} определён соотношением

$$\hat{U} = 2 |\varphi_1\rangle_n \langle \varphi_1| - I.$$

Наконец, если учесть, что $|\varphi_1\rangle_n = \hat{W} |0\rangle_n$, где \hat{W} – оператор Уолша – Адамара, а также что $\hat{W} = \hat{W}^\dagger$ и $\hat{W} I \hat{W} = I$, оператор \hat{U} можно переписать тождественно:

$$\hat{U} = 2 \hat{W} |0\rangle_n \langle 0|_n \hat{W} - \hat{W} I \hat{W} = 2 \hat{W} |0\rangle_n \langle 0|_n \hat{W} - I.$$

Таким образом оператор Гровера суммарно может быть представлен в виде

$$G = \left(2 \hat{W} |0\rangle_n \langle 0|_n \hat{W} - I \right) \hat{O}_{x_0} = \left(2 |\varphi_1\rangle_n \langle \varphi_1|_n - I \right) \left(I - 2 |x_0\rangle_n \langle x_0|_n \right). \quad (6.123)$$

Амплитудное усиление, приводящее амплитуду маркированного состояния к 1, в результате применения алгоритма Гровера за один проход может быть достигнуто только в специальном случае. По этой причине для достижения значения амплитуды искомого состояния, близкого к единице, нужно выполнить повторение алгоритма порядка \sqrt{N} раз, что быстрее любого классического алгоритма, требующего порядка N вычислений.

Пример 6.5. Оператор Гровера для базы данных из 4 элементов

В качестве элементарного примера рассмотрим базу данных с $N = 4$ с маркированным элементом $|1\rangle_2 = |0, 1\rangle$. В соответствии с (6.123) оператор Гровера в этом случае имеет вид

$$\begin{aligned} G_1 &= (2 |\varphi_1\rangle_2 \langle \varphi_1|_2 - I) \hat{O}_1 = \frac{1}{2} \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix} \hat{O}_1 = \\ &= \frac{1}{2} \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} -1 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{pmatrix}. \end{aligned} \quad (6.124)$$

В результате при действии G_1 на равновероятную суперпозицию двухкубитовых состояний $|\varphi_1\rangle_2$ получим чистое двухкубитовое состояние $|1\rangle_2$:

$$G_1 : |\varphi_1\rangle_2 = \frac{1}{2} \begin{pmatrix} -1 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{pmatrix} \frac{1}{2} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = |1\rangle_2.$$

Таким образом, при измерении регистра данных базы с вероятностью, равной единице, будет получено именно маркированное (т. е. искомое) состояние.

Пример 6.6. Квантовое Фурье-преобразование и алгоритм поиска в базе данных

Рассмотренный выше алгоритм поиска в неупорядоченной базе данных можно переписать и с использованием преобразования Фурье. В этом случае необходимо выполнить следующую последовательность шагов.

1. Создание регистра данных $|x\rangle_n = \hat{W}|0\rangle_n$.
2. Применение Оракула к состоянию $|x\rangle_n$: $|x'\rangle_n = \hat{O}_{x_0}|x\rangle_n$.
3. Применение операции квантового Фурье-преобразования к состоянию $|x'\rangle_n$.
4. Изменение знаков амплитуд у всех состояний $|x'\rangle_n$, кроме состояния $|0'\rangle_n$.
5. Применение операции обратного квантового Фурье-преобразования к полученным состояниям.
6. Возврат к шагу 2 и повтор алгоритма.

В соответствии с изложенной процедурой можно получить результат, представленный в предыдущем примере и при использовании квантового Фурье-преобразования. Для этого выполним последовательно предусмотренные алгоритмом шаги.

1. Создание регистра данных:

$$|x\rangle_2 = \frac{1}{2}(|0\rangle_2 + |1\rangle_2 + |2\rangle_2 + |3\rangle_2).$$

2. Применение Оракула \hat{O}_1 к $|x\rangle_2$:

$$|x'\rangle_2 = \hat{O}_1 : |x\rangle_2 = \frac{1}{2}(|0\rangle_2 - |1\rangle_2 + |2\rangle_2 + |3\rangle_2).$$

3. Квантовое Фурье-преобразование состояния $|x'\rangle_2$:

$$\begin{aligned} |x''\rangle_2 &= \frac{1}{4} \sum_{k=0}^3 \left[|k\rangle_2 - \exp(i\frac{\pi}{2}k) |k\rangle_2 + \exp(i\frac{\pi}{2}2k) |k\rangle_2 + \exp(i\frac{\pi}{2}3k) |k\rangle_2 \right] = \\ &= \frac{1}{4} \left[\left(|0\rangle_2 + |1\rangle_2 + |2\rangle_2 + |3\rangle_2 \right) - \left(|0\rangle_2 + i|1\rangle_2 - |2\rangle_2 - i|3\rangle_2 \right) + \right. \\ &\quad \left. + \left(|0\rangle_2 - |1\rangle_2 + |2\rangle_2 - |3\rangle_2 \right) + + \left(|0\rangle_2 - i|1\rangle_2 - |2\rangle_2 + i|3\rangle_2 \right) \right] = \\ &= \frac{1}{2} \left[|0\rangle_2 - i|1\rangle_2 + |2\rangle_2 + i|3\rangle_2 \right]. \end{aligned}$$

4. Замена знаков у всех состояний на противоположные, кроме состояния $|0\rangle_2$. В результате возникает состояние $|x'''\rangle_2$:

$$|x'''\rangle_2 = \frac{1}{2} \left[|0\rangle_2 + i|1\rangle_2 - |2\rangle_2 - i|3\rangle_2 \right].$$

5. Обратное квантовое Фурье-преобразование $|y\rangle_2 = F^{-1} : |x'''\rangle_2$:

$$\begin{aligned} |y\rangle_2 &= \frac{1}{4} \left[\left(|0\rangle_2 + |1\rangle_2 + |2\rangle_2 + |3\rangle_2 \right) + i \left(|0\rangle_2 - i|1\rangle_2 - |2\rangle_2 + i|3\rangle_2 \right) - \right. \\ &\quad \left. - \left(|0\rangle_2 - |1\rangle_2 + |2\rangle_2 - |3\rangle_2 \right) - -i \left(|0\rangle_2 + i|1\rangle_2 - |2\rangle_2 - i|3\rangle_2 \right) \right] = \\ &= \frac{1}{4} \left[2|1\rangle_2 + 2|3\rangle_2 + 2|1\rangle_2 - 2|3\rangle_2 \right] = |1\rangle_2, \end{aligned} \tag{6.125}$$

т. е. тот же результат, что и найденный операторным методом за один цикл применения оператора Гровера.

Важным является вопрос о том, сколько раз надо применять оператор Гровера для того, чтобы получить амплитуду маркированного состояния, максимально близкую к единице, а это при измерении регистра данных позволит определить искомый элемент базы данных. Детальный анализ рассмотренного алгоритма даёт следующий результат для оптимального числа итераций в базе из N элементов: $N_0 \approx \pi\sqrt{N}/4$.

Упражнение 6.9. Для 128 элементов базы с искомым пятым элементом выполнить последовательно итерации, обеспечивающие усиление амплитуды вероятности извлечения пятого элемента.

Упражнение 6.10. Построить оператор Гровера для базы данных из 8 элементов с пятым маркированным состоянием.

Упражнение 6.11. Определить результат последовательного трёхкратного действия оператора Гровера, построенного в предыдущем примере, на равновероятную суперпозицию исходного трёхбитового состояния.

ЗАЩИТА ОТ ПОДСЛЫПОВ

САМОУДАР

Часть IV

Телепортация и связь

Глава 7

Телепортация и сверхплотное кодирование

7.1 Квантовая телепортация

Квантовая телепортация — это передача квантового состояния из одного места в другое даже при отсутствии квантового канала связи между отправителем и получателем.

Для объяснения смысла телепортации положим, что два человека А и Б находились в одном месте и подготовили на некотором квантовом устройстве EPR-пару

$$|\text{EPR}\rangle_2 = (|0,0\rangle + |1,1\rangle)/\sqrt{2}$$

из двух отдельных кубитов $|\varphi_1\rangle$ и $|\varphi_2\rangle$. Затем они разъехались в разные места, но каждый из них взял с собой один кубит из данной EPR-пары, заботясь о том, чтобы их кубиты были изолированы от окружающего пространства. По истечении некоторого времени одному из них (далее А) потребовалось передать Б третий кубит $|q\rangle$, не связанный с их EPR-парой :

$$|q\rangle = \alpha |0\rangle + \beta |1\rangle, \quad (7.1)$$

не используя квантовый канал связи. При этом А не владеет информацией о состоянии кубита $|q\rangle$, т. е. не знает величины комплексных коэффициентов α и β и имеет возможность связаться с Б только по классическому каналу связи.

В соответствии с общими принципами квантовой теории и теоремой о неклонируемости квантового состояния А не может без разрушения кубита $|q\rangle$ определить коэффициенты α и β и просто передать их значения Б, чтобы тот изготовил соответствующий кубит $|q\rangle$ у себя на квантовом устройстве. Однако А может осуществить специальное взаимодействие кубита $|q\rangle$ со своим кубитом $|\phi_1\rangle$, который входит в $|\text{EPR}\rangle_2$ -пару, а затем

произвести измерение образовавшегося двухкубитового состояния. Оказывается, что по информации, полученной А в результате измерения созданного А двухкубитового состояния $|x\rangle_2$, А может сообщить Б такие данные, на основании которых Б "сконструирует" кубит $|q\rangle$ из имеющегося у него кубита EPR-пары.

Таким образом, без физической передачи кубита $|q\rangle$ у Б образуется кубит именно в том состоянии, которое требовалось передать от абонента А абоненту Б. Очевидно при этом, что процесс измерения двухкубитового состояния, выполненный абонентом А, приведёт к разрушению состояния кубита $|q\rangle$ и кубита из EPR-пары абонента А.

Так как в общем случае произвольное двухкубитовое состояние $|x\rangle_2$, сформированное абонентом А, является суперпозицией базисных двухкубитовых состояний вида

$$|x\rangle_2 = \sum_{k=0}^3 c_k |k\rangle_2 = c_0 |0,0\rangle + c_1 |0,1\rangle + c_2 |1,0\rangle + c_3 |1,1\rangle,$$

то в результате измерения состояния $|x\rangle_2$ может быть получен только один из четырёх возможных результатов измерения: (0, 0), (0, 1), (1, 0) или (1, 1).

Ниже будет показано, что если абонент А по классическому каналу связи передаст информацию о полученном им результате измерения абоненту Б, то Б выполнит одну из четырёх операций со своим кубитом $|\varphi_2\rangle$ из его $|\text{EPR}\rangle_2$ -пары, которая и приведёт к формированию у абонента Б кубита, находящегося точно в состоянии кубита $|q\rangle$. Такой процесс передачи кубита без его физического перемещения и есть *квантовая телепортация*.

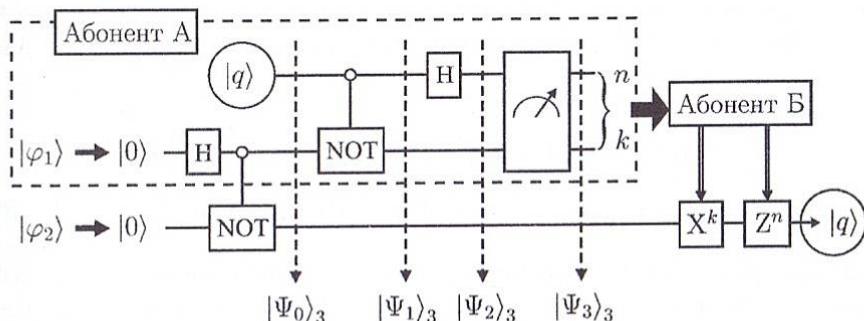


Рис. 7.1. Логическая диаграмма квантовой телепортации

Квантовая цепь, изображённая на рис. 7.1, даёт описание процесса телепортации в результате преобразований трёхкубитового состояния (два ку-

бита EPR-пары и кубит $|q\rangle$). Состояние кубита, которое должно быть передано Б, определяется выражением (7.1), где α и β неизвестны.

Начальное состояние всей трёхкубитовой цепи определяется прямым произведением кубита $|q\rangle$ (7.1) и двухкубитового состояния EPR-пары:

$$\begin{aligned} |\Psi_0\rangle_3 &= |q\rangle \otimes |\text{EPR}\rangle_2 = \\ &= \frac{1}{\sqrt{2}} \left[\alpha |0\rangle \otimes (|0,0\rangle + |1,1\rangle) + \beta |1\rangle \otimes (|0,0\rangle + |1,1\rangle) \right]. \end{aligned} \quad (7.2)$$

Здесь и ниже использовано соглашение о том, что в формулах первые два (слева направо) кубита находятся у абонента А, а третий кубит – у абонента Б. На рис. 7.1 формирование EPR-пары осуществляется последовательным действием оператора Адамара Н на кубит $|\varphi_1\rangle$ и оператора контролируемого отрицания CNOT на кубиты $|\varphi_1\rangle$ и $|\varphi_2\rangle$. В результате образуется исходное трёхкубитовое состояние $|\Psi_0\rangle_3$. В соответствии с квантовой цепью телепортации на первом шаге абонент А пропускает свои два кубита ($|q\rangle$ и $|\varphi_1\rangle$) через CNOT-гейт. В результате получается трёхкубитовое состояние $|\Psi_1\rangle_3$:

$$|\Psi_1\rangle_3 = \frac{1}{\sqrt{2}} \left[\alpha |0\rangle \otimes (|0,0\rangle + |1,1\rangle) + \beta |1\rangle \otimes (|1,0\rangle + |0,1\rangle) \right]. \quad (7.3)$$

На следующем шаге абонент А пропускает кубит $|q\rangle$ через гейт Адамара. В результате возникает трёхкубитовое состояние $|\Psi_2\rangle_3$ вида

$$|\Psi_2\rangle_3 = \frac{1}{2} \left[\alpha (|0\rangle + |1\rangle) \otimes (|0,0\rangle + |1,1\rangle) + \beta (|0\rangle - |1\rangle) \otimes (|1,0\rangle + |0,1\rangle) \right]. \quad (7.4)$$

Перегруппировав члены в (7.4) путём выделения пары кубит, находящихся у А, соблюдая выбранную последовательность принадлежности кубит А и Б, получим

$$\begin{aligned} |\Psi_2\rangle_3 &= \frac{1}{2} \left[|0,0\rangle \otimes (\alpha |0\rangle + \beta |1\rangle) + |0,1\rangle \otimes (\alpha |1\rangle + \beta |0\rangle) + \right. \\ &\quad \left. + |1,0\rangle \otimes (\alpha |0\rangle - \beta |1\rangle) + |1,1\rangle \otimes (\alpha |1\rangle - \beta |0\rangle) \right]. \end{aligned} \quad (7.5)$$

Отсюда видно, что если результат измерения, выполненного А, окажется равным $(0,0)$, т. е. при измерении первых двух кубит состояния $|\Psi_2\rangle_3$ ре-дуцировалось до состояния $|0,0\rangle \otimes (\alpha |0\rangle + \beta |1\rangle)$, а показания приборов оказались равными $n = 0, k = 0$, то кубит Б находится точно в состоянии, совпадающем с $|q\rangle$ (именно в том состоянии, которое абонент А должен по условию процесса передать абоненту Б).

В общем случае в зависимости от результата измерения $|\Psi_2\rangle_3$, полученного абонентом А, абоненту Б со своим кубитом Б нужно выполнить одно из четырёх преобразований, которые приведены в табл. 7.1, чтобы его кубит оказался совпадающим с исходным кубитом $|q\rangle$.

Таблица 7.1

Действия абонента Б в зависимости от результатов измерения абонента А

Результат измерения А	Состояние кубита Б после измерения А	Действия Б	Окончательное состояние
00	$\alpha 0\rangle + \beta 1\rangle$	1	$\alpha 0\rangle + \beta 1\rangle$
01	$\alpha 1\rangle + \beta 0\rangle$	X	$\alpha 0\rangle + \beta 1\rangle$
10	$\alpha 0\rangle - \beta 1\rangle$	Z	$\alpha 0\rangle + \beta 1\rangle$
11	$\alpha 1\rangle - \beta 0\rangle$	XZ	$\alpha 0\rangle + \beta 1\rangle$

X и Z в табл. 7.1 – однокубитовые операторы, являющиеся известными матрицами Паули $X = \sigma_x$, $Z = \sigma_z$. Как видно из таблицы, после выполнения указанных преобразований из кубита, принадлежащего абоненту Б, получится кубит, точно совпадающий с $|q\rangle$.

Однако для того чтобы узнать, в каком из четырёх состояний находится его кубит, абонент Б должен получить классическую информацию о результате измерения, выполненного абонентом А. Как только Б узнает результат измерения А, он может получить состояние кубита $|q\rangle$, выполняя соответствующие табл. 7.1 квантовые операции.

Так, если результат сообщённого измерения А равен (0, 0), то Б ничего не нужно делать с его кубитом – он находится именно в состоянии $|q\rangle$. Если же измерение А даёт результат (0, 1), то Б должен подействовать на свой кубит гейтом квантового отрицания X (матрица Паули σ_x). В результате у него образуется именно тот кубит $|q\rangle$, который требуется ему передать. Если измерение А даёт результат, равный (1, 0), то Б должен подействовать на свой кубит гейтом Z (матрица Паули σ_z), и его кубит в этом случае перейдет в состояние $|q\rangle$. Наконец, если результат измерения А оказался равным (1, 1), то Б должен подействовать гейтами $X \cdot Z$ на свой кубит, чтобы получить передаваемое состояние $|q\rangle$.

Имеется ряд обстоятельств в явлении квантовой телепортации, которые должны быть объяснены с учётом общефизических принципов. Например, может создаться впечатление, что телепортация позволяет передавать квантовое состояние мгновенно и, следовательно, быстрее скорости распространения электромагнитного поля в пространстве. Это утверждение находится в прямом противоречии с фундаментальным принципом теории относительности. Однако в рассмотренном явлении квантовой телепортации нет противоречия с теорией относительности, потому что для осуществления телепортации абонент А должен передать результат своего измерения по классическому каналу связи, а следовательно, со скоростью не больше скорости света.

Напомним, что до проведения измерений абонентом А квантовое состояние трёх кубит определяется выражением (7.5). Измерения, выполняемые А, дают вероятность, равную $1/4$ для любого из четырёх представленных состояний $|i, j\rangle_2 \otimes (\alpha|0\rangle \pm \beta|1\rangle)$, где $i, j \in 0, 1$. Таким образом, оператор плотности всей системы имеет вид

$$\begin{aligned} \varrho = \frac{1}{4} & \left[|0, 0\rangle \langle 0, 0| (\alpha|0\rangle + \beta|1\rangle)(\alpha^* \langle 0| + \beta^* \langle 1|) + \right. \\ & + |01\rangle \langle 01| (\alpha|1\rangle + \beta|0\rangle)(\alpha^* \langle 1| + \beta^* \langle 0|) + \\ & + |10\rangle \langle 10| (\alpha|0\rangle - \beta|1\rangle)(\alpha^* \langle 0| - \beta^* \langle 1|) + \\ & \left. + |11\rangle \langle 11| (\alpha|1\rangle - \beta|0\rangle)(\alpha^* \langle 1| - \beta^* \langle 0|) \right]. \end{aligned} \quad (7.6)$$

Вычисляя штурм от ϱ по переменным системы кубит, находящихся у абонента А, можно получить приведённую матрицу плотности кубита абонента Б. Результат в этом случае есть

$$\begin{aligned} \varrho^B &= \frac{1}{4} \left[(\alpha|0\rangle + \beta|1\rangle)(\alpha^* \langle 0| + \beta^* \langle 1|) + (\alpha|1\rangle + \beta|0\rangle)(\alpha^* \langle 1| + \beta^* \langle 0|) + \right. \\ & + (\alpha|0\rangle - \beta|1\rangle)(\alpha^* \langle 0| - \beta^* \langle 1|) + (\alpha|1\rangle - \beta|0\rangle)(\alpha^* \langle 1| - \beta^* \langle 0|) \Big] = \\ &= \frac{1}{2} \left((|\alpha|^2 + |\beta|^2) |0\rangle \langle 0| + (|\alpha|^2 + |\beta|^2) |1\rangle \langle 1| \right) = \\ &= \frac{1}{2} (|\alpha|^2 + |\beta|^2) \left[|0\rangle \langle 0| + |1\rangle \langle 1| \right] = \frac{1}{2}. \end{aligned} \quad (7.7)$$

Следовательно, состояние кубита у Б после измерения, выполненного абонентом А, но до того, как Б узнал результат, определяется матрицей плотности, равной $\varrho^B \equiv 1/2$, и не зависит от состояния кубита $|q\rangle$. Значит, любое измерение, выполненное абонентом Б, не будет содержать информации о $|q\rangle$. Таким образом, без передачи классической информации нельзя

получить состояние $|q\rangle$, и нет нарушения принципов теории относительности.

Следующим нетривиальным и удивительным результатом является возможность создания копии квантового состояния, что противоречит теореме о невозможности клонирования (копирования) квантового состояния, которая обсуждалась ранее. В этом утверждении также не содержится противоречий основным физическим принципам, так как после осуществления явления телепортации только кубит у Б находится в состоянии $|q\rangle$, а исходный кубит (в результате измерения) – уже в одном из базисных состояний $|0\rangle$ или $|1\rangle$. То есть нет двух тождественных кубит $|q\rangle$.

В практическом смысле телепортация показывает, что EPR-пара совместно с двумя классическими битами информации образуют ресурс по передаче одного кубита информации. В целом, квантовая телепортация иллюстрирует возможность использования запутанных состояний в качестве метода передачи квантовой информации на удалённые расстояния без непосредственной передачи кубит по квантовым каналам связи.

Квантовую телепортацию можно эффективно использовать в квантовых цепях с целью контроля появления возможных ошибок при выполнении многокубитовых операций. Это связано с тем, что в квантовых цепях нельзя дублировать кубит при вычислении. В классических системах копирование исходных данных используется для реакции вычислительного элемента при обнаружении ошибки в данном элементе. Реакция состоит в повторении попытки выполнения операции с копией исходных данных при обнаружении ошибки. В квантовых системах приходится выстраивать достаточно сложные цепи квантовых операторов, позволяющие с использованием явления телепортации исправлять верифицированные ошибки. Подробное описание таких цепей можно найти в [8].

Упражнение 7.1. Описать процесс телепортации, если передаваемый кубит находится в базисном однокубитовом состоянии $|0\rangle$.

Упражнение 7.2. Описать процессы телепортации при выполнении следующих начальных условий:

$$|\varphi\rangle_1 = |i\rangle \quad \text{и} \quad |\varphi\rangle_2 = |j\rangle, \quad i, j \in \{0, 1\}.$$

Упражнение 7.3. Установить возможность телепортации макроскопических предметов.

Упражнение 7.4. Перечислить фундаментальные идеи, которые лежат в основе квантовой телепортации?

7.2 Сверхплотное кодирование

Рассмотренные выше EPR-пары могут использоваться и для передачи классических бит информации по квантовым каналам связи путём прямой передачи кубита от абонента А абоненту Б. Пусть, например, кубиты абонентов А и Б находятся в состоянии Белла вида

$$|\text{EPR}\rangle_2 = \frac{|0,0\rangle + |1,1\rangle}{\sqrt{2}}, \quad (7.8)$$

а сами абоненты располагаются со своими кубитами в различных местах. Если абонент А желает передать два бита информации (x_1, x_2) , $x_i \in \{0, 1\}$ абоненту Б, он может путём некоторого преобразования изменить состояние своего кубита и в дальнейшем передать его абоненту Б. Абонент Б, измерив специальной процедурой состояние двух кубитов (своего и полученного от А), может понять, какие значения битов (x_1, x_2) были ему переданы посредством одного кубита. При этом квантовая цепь, соответствующая измерению, выполняемому абонентом Б, всегда одна (рис. 7.2).

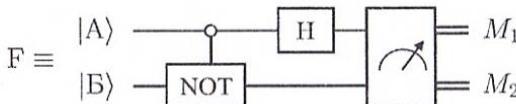


Рис. 7.2. Логическая диаграмма измерения кубит при сверхплотном кодировании

Для того чтобы продемонстрировать технологию реализации передачи информации в соответствии с изложенной выше процедурой, рассмотрим некоторые варианты преобразований, которые может выполнить со своим кубитом абонент А.

1. Если абонент А ничего не будет делать со своим кубитом и перешлёт его абоненту Б в исходном виде, тогда результат измерения пары кубитов, выполненного абонентом Б, определяется выражением

$$\hat{F} : \frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{1}{2}(|00\rangle + |10\rangle + |00\rangle - |10\rangle) = |00\rangle. \quad (7.9)$$

Другими словами, абонент Б прочтёт в результате измерения два бинарных значения: $x_1 = 0$ и $x_2 = 0$.

2. Если абонент А перед отправкой своего кубита подействует на него однокубитовым гейтом отрицания X , то исходная EPR-пара перейдёт в состояние вида $|\text{EPR}'\rangle_2 = (|1,0\rangle + |0,1\rangle)/\sqrt{2}$. Отправленный далее кубит абонент Б прочтает по схеме, представленной на рис. 7.2, и получит сле-

дующий результат:

$$\hat{F} : \frac{|10\rangle + |01\rangle}{\sqrt{2}} = \frac{1}{2}(|01\rangle - |11\rangle + |01\rangle + |11\rangle) = |01\rangle. \quad (7.10)$$

В этом случае двухбитовое сообщение для абонента Б имеет следующий вид: $x_1 = 0$ и $x_2 = 1$.

3. Если абонент А перед отправкой своего кубита по квантовому каналу связи подействует на него однокубитовым гейтом Z , то исходная EPR-пара перейдёт в состояние вида $|EPR\rangle''_2 = (|0,0\rangle - |1,1\rangle)/\sqrt{2}$. Результат измерения, выполненного абонентом Б, в этом случае определяется выражением

$$\hat{F} : \frac{|00\rangle - |11\rangle}{\sqrt{2}} = \frac{1}{2}(|00\rangle + |10\rangle - |00\rangle + |10\rangle) = |10\rangle. \quad (7.11)$$

То есть абонент Б получит следующее двухбитовое сообщение: $x_1 = 1$ и $x_2 = 0$.

4. Наконец, если абонент А перед отправкой своего кубита по квантовому каналу связи подействует на него произведением однокубитовых операторов $Z \cdot X$, то исходная EPR-пара перейдёт в суперпозицию состояний вида $|EPR\rangle'''_2 = (-|1,0\rangle + |0,1\rangle)/\sqrt{2}$. Результат измерения, выполненного абонентом Б, в этом случае определяется выражением

$$\hat{F} : \frac{-|10\rangle + |01\rangle}{\sqrt{2}} = \frac{1}{2}(-|01\rangle + |11\rangle + |01\rangle + |11\rangle) = |11\rangle. \quad (7.12)$$

И абонент Б получит двухбитовое сообщение $x_1 = 1$ и $x_2 = 1$.

Представленный анализ позволяет сделать следующее заключение. Для передачи абонентом А абоненту Б двухбитового сообщения (00) ему просто нужно отправить свой кубит Б. Соответственно, для передачи двухбитового сообщения (01) абонент А перед отправкой своего кубита Б должен обработать его гейтом X . Если А хочет посредством своего кубита передать двухбитовую информацию (10), то перед отправкой кубит А должен быть обработан гейтом Z . И последний вариант двухбитовой информации (11) передаётся после обработки кубита абонента А последовательным действием на кубит двух однокубитовых операций $Z \cdot X$.

Естественно, что для пересылки целого текста от А к Б сначала абонент А кодирует его последовательностью битовых нулей и единиц, затем каждой паре битовых значений абонент А формирует кубит из EPR-пар, имеющихся у А и Б, и посыпает его абоненту Б. Абонент Б измеряет каждый полученный кубит и получает последовательность двухбитовых значений, которая и составляет передаваемый текст. Описанный выше протокол передачи кубит из EPR-пар от одного абонента другому называется

сверхплотным кодированием, при этом имеется в виду, что пара битовых значений передаётся одним объектом — кубитом.

Упражнение 7.5. Сформулировать протокол передачи текстовой информации на основе технологии сверхплотного кодирования.

Упражнение 7.6. Показать, что рассмотренный выше протокол кодирования не может привести к передаче более чем одного бита классической информации, если исходное двухкубитовое состояние незапутанное.

Часть V

Защита информации

Глава 8

Элементарные основы квантовой криптографии

8.1 Классическое шифрование

Создание необходимых условий для защищённого от постороннего вмешательства хранения информации или её передачи играет огромную роль в жизни человечества и особенно в условиях существования информационного общества.

Наука, имеющая дело с секретной информацией, называется *криптологией*. В свою очередь, криптология подразделяется на *криптографию* и *криptoанализ*. Криптография включает в себя создание (шифрование) и передачу секретной информации, а также её восстановление (расшифрование). А криptoанализ рассматривает методы раскрытия (взлома) зашифрованной информации.

Кратко такие процессы могут быть описаны по следующей схеме. Пусть, например, абонент А имеет задачу передать абоненту Б некоторую открытую информацию (набор символов из алфавита общения), которую обозначим через T . Для сохранения тайны текста T абонент А преобразует исходный текст T по некоторому правилу f_K в скрытое или шифрованное сообщение

$$E = f_K(T).$$

Здесь K – называемый “ключом” набор символов, определяющих операцию преобразования. Абонент Б, получая сообщение E по какому-то каналу связи, применяет к этому сообщению преобразование ψ_N , где N – ключ преобразования абонента Б, и получает исходный текст $T = \psi_N(E)$, т. е. осуществляет расшифрование. Криптография с использованием одинаковых ключей называется *криптографией с симметричными ключами*. Криптография с использованием различных ключей у абонентов называется *криптографией с открытыми ключами*.

При использовании криптографии с симметричными ключами абоненты должны встретиться и договориться об общем алфавите L , состоящем из N символов, и о секретном ключе $K = k_1k_2\dots k_n$, $k_i \in L$, где n — длина ключа. В результате, если у абонента А имеется открытый текст $T = t_1t_2\dots t_k$, $t_i \in L$, k — число символов в открытом тексте, то он составляет шифрованное сообщение $E = e_1e_2\dots e_k$ по правилу

$$e_i = [t_i + k_i \bmod n] \bmod N, \quad i \in 1, 2, \dots, k.$$

Соответственно, абонент Б, получив сообщение, восстанавливает исходный текст по формуле

$$t_i = [e_i - k_i \bmod n] \bmod N, \quad i \in 1, 2, \dots, k.$$

Такая система шифрования неудобна в случае большого числа абонентов, например, в сетях сотовой связи или Интернете, так как организация обмена ключами в этом случае становится чрезвычайно сложной. Для решения этой проблемы в сетях сотовой связи используются предварительно запрограммированные статические ключи, которые хранятся на SIM-карте пользователя, и его точная копия в регистре абонентов у оператора сотовой связи. Естественно, что число таких ключей довольно ограничено, так что невозможно обеспечить действительно безопасную передачу информации.

В сети Интернет отсутствует субъект, отвечающий за присвоение секретного ключа пользователю и хранение базы данных ключей. В этом случае реализуется криптография с открытым ключом. Наиболее употребительная схема такой криптографии основана на использовании алгоритма RSA. Этот алгоритм требует выполнения процедуры создания ключей, один из которых является открытым ключом абонента, а другой — его секретным ключом. Генерация ключей происходит по следующей схеме.

1. Выбираются два случайных простых числа p, q ($p \neq q$).
2. Вычисляется число $n = p \cdot q$, которое называется модулем.
3. Вычисляется значение функции Эйлера $\varphi(n) = (p - 1)(q - 1)$.
4. Выбирается взаимно простое со значением $\varphi(n)$ целое число e , удовлетворяющее условию $1 \leq e \leq \varphi(n)$. Взаимная простота означает, что $\gcd(e, \varphi(n)) = 1$.
5. Выбирается число d , удовлетворяющее сравнению $d \cdot e \equiv 1 \pmod{\varphi(n)}$.
6. Пара чисел $P = (e, n)$ образуют открытый ключ, доступный любым абонентам, а пара чисел $S = (d, n)$ называется секретным ключом, который сохраняется в тайне каждым абонентом, сгенерировавшим P и S .

Например, абонент А выбирает два простых числа: $p_a = 7, q_a = 23$. В этом случае $n = p_a \cdot q_a = 161$. Функция Эйлера $\varphi(161) = 132$. Далее абонент А выбирает целое число e , взаимно простое с 132, например $e = 7$, и решает сравнение $d \cdot 7 \equiv 1 \pmod{132}$. Решение сравнения даёт секретное число $d = 19$. Таким образом абонент А определяет два числа, которые формируют открытый ключ $P_a = (7, 161)$, и два числа секретного ключа $S_a = (19, 161)$.

Аналогично другие абоненты генерируют свои ключи P_i, S_i . В результате формируется "телефонная" книга, в которой приведены имена абонентов и их открытые ключи. Свои секретные ключи они хранят в тайне. Для примера осуществления секретной переписки в табл. 8.1 приведены секретные и открытые ключи ряда абонентов.

Таблица 8.1

Примеры открытых и секретных ключей абонентов

Абонент	Открытые ключи	Секретные ключи
А	$P_a = (e_a, n_a) = (7, 161)$	$S_a = (d_a, n_a) = (19, 161)$
Б	$P_b = (e_b, n_b) = (41, 368659)$	$S_b = (d_b, n_b) = (268841, 368659)$
С	$P_c = (e_c, n_c) = (23, 42827)$	$S_c = (d_c, n_c) = (18407, 42827)$
...

Допустим, абонент А имеет необходимость отправить секретное сообщение $T = 5648$ абоненту С. Для этого он должен взять открытый ключ абонента С и зашифровать своё сообщение с использованием выражения

$$E = T^{e_c} \pmod{n_c} = 5648^{23} \pmod{42827} = 10908,$$

отослать это сообщение абоненту С, который расшифрует его своим секретным ключом

$$T = E^{d_c} \pmod{n_c} = 10908^{18407} \pmod{42827} = 5648.$$

Аналогично осуществляется защищённая связь между любыми абонентами. В данных цифровых примерах величина сообщения не должна превышать величины n – абонента-получателя.

Алгоритм RSA может быть использован для подтверждения подлинности сообщения или авторства, что получило наименование цифровая подпись. Смысл данного протокола состоит в выполнении следующей процедуры. Если абоненту А необходимо отправить сообщение абоненту С, подтверждённое цифровой подписью абонента А, то данный абонент сначала

создаёт так называемую цифровую подпись Q с помощью собственного секретного ключа $d_a = 19$ и случайно выбранного числа (например, 89):

$$Q = T^{d_a} \bmod n_a = 89^{19} \bmod 161 = 40.$$

Далее абонент А передаёт абоненту С некоторое сообщение и пару чисел $(T, Q) = (89, 40)$ для собственной идентификации. Получив данную пару, абонент С должен проверить подлинность подписи абонента А. Для этого абонент С с помощью открытого ключа абонента А e_a выполняет преобразование

$$T' = Q^{e_a} \bmod n_a = 40^7 \bmod 161 = 89.$$

Если $T' = 89$ оказывается равной $T = 89$, то подпись подлинная.

Описанная выше асимметричная криптосистема подвержена взлому, если злоумышленнику удаётся факторизовать число $n = p \cdot q$, объявленное в открытом ключе абонента. Например, мы хотим установить секретный ключ абонента Б, зная только его открытый ключ. Так как в его открытом ключе $n = 368\,659$, то можно перебором или иным алгоритмом разложения n на простые множители установить, что $368\,659 = 487 \cdot 757$. Таким образом, становится известным значение функции Эйлера:

$$\varphi(n) = \varphi(368\,659) = (487 - 1)(757 - 1) = 367\,416.$$

А так как открытый ключ абонента Б известен ($e_b = 41$), то необходимо решить сравнение

$$x \cdot 41 = 1 \bmod 367\,416,$$

из которого находится секретный ключ x абонента Б, равный в данном примере $x = 268\,841$.

В настоящее время считается, что RSA-ключи длиной в 1024 бит и более обеспечивают достаточную криптостойкость RSA-системы, так как даже лучшие известные алгоритмы факторизации (например, решето числового поля) не позволяют разложить большое целое число за приемлемое время. Рассмотренные ранее квантовые алгоритмы Шора и Гровера в теории позволяют решить задачу о факторизации целого числа как раз за приемлемое время. И это значит, что в случае их реализации на реальных системах потребуется существенно увеличить длину RSA-ключей для обеспечения надежности такой классической системы, что приведёт к возрастанию ресурсов, необходимых для их обеспечения. Можно сказать, что квантовые системы угрожают криптографическим системам с открытым ключом. Однако выяснилось, что квантовые системы сами предлагают эффективное решение проблемы защиты передаваемой информации на основе симметричного криптографического ключа.

Упражнение 8.1. Установить секретный ключ абонента С из приведённой выше телефонной книги на основании его известного открытого ключа.

8.2 Квантовый протокол BB84

Квантовая теория информации не вносит радикальных изменений в идеологию построения криптографических систем, однако открывает новые возможности в повышении их криптографической стойкости. Известно, что в симметричных криптографических системах их стойкость существенно зависит от ключа, выбор которого желательно осуществлять на основе генерации случайных последовательностей. Более того, желательно менять ключевую последовательность при каждом акте передачи зашифрованной информации между абонентами. Однако систематическая генерация новых ключей в симметричных криптографических системах сопряжена с трудностью распространения ключа между заинтересованными абонентами.

Квантовая теория позволяет безопасными (контролируемыми) процедурами с кубитами обеспечить генерацию случайного ключа и его распространение между участниками обмена информацией для дальнейшего использования. Простейший вариант такой процедуры называется квантовым протоколом BB84 генерации и распространения случайного ключа. Название протокола происходит от фамилий авторов, предложивших данную квантовую схему (Bennett, Brassard) в 1984 г.

Для объяснения данного протокола рассмотрим очень простой идеальный пример. Пусть абонент А должен скрытно передать некоторую информацию абоненту Б по некоторому каналу связи. Предполагается, что у абонентов имеется оборудование для работы с кубитами (они могут создавать кубиты, измерять кубиты и т. п.). Кроме того, в их распоряжении есть и квантовый, и классический каналы связи. До момента осуществления передачи информации абоненты не имеют общего секретного ключа. Поэтому на первом этапе они должны сначала сформировать уникальный случайный ключ для зашифрования данного сообщения у абонента А и его расшифрования у абонента Б.

Протокол BB84 позволяет решить задачу создания секретного ключа у обоих абонентов с использованием квантовых объектов. Для этой цели абонент А генерирует случайную битовую последовательность, на основании которой и будет сформирован секретный ключ. Допустим, сге-

нерированная битовая последовательность состоит из 8 бит и имеет вид $a = (10110101)$. В соответствии с данной последовательностью абонент А на своём специальном квантовом устройстве создаёт восьмикубитовый регистр вида

$$|\psi\rangle_8 = |1, 0, 1, 1, 0, 1, 0, 1\rangle_8 = |1\rangle \otimes |0\rangle \otimes |1\rangle \otimes |1\rangle \otimes |0\rangle \otimes |1\rangle \otimes |0\rangle \otimes |1\rangle. \quad (8.1)$$

Кубиты находятся в регистре из восьми базисных однокубитовых состояний, совпадающих со случайно сгенерированной битовой последовательностью.

Далее с каждым из этих 8 кубит абонент А выполняет последовательность случайных преобразований. Для простоты будем считать, что у А и Б имеется только по два устройства (вентиля, гейта), которыми они могут воспользоваться для преобразования кубита. Один вентиль – это гейт Адамара \hat{H} , а второй – тождественное преобразование \hat{I} . Применяя эти вентили к кубитам регистра (8.1), например в указанном, случайно выбранном порядке $\hat{H}_1 \hat{I}_2 \hat{H}_3 \hat{I}_4 \hat{H}_5 \hat{I}_6 \hat{H}_7 \hat{I}_8$, где индексы определяют номер кубита в регистре слева направо, абонент А получает квантовый регистр вида

$$\begin{aligned} |y\rangle_8 &= \hat{H}_1 \hat{I}_2 \hat{H}_3 \hat{I}_4 \hat{H}_5 \hat{I}_6 \hat{H}_7 \hat{I}_8 |1, 0, 1, 1, 0, 1, 0, 1\rangle_8 = \\ &= \hat{H}_1 |1\rangle \otimes \hat{I}_2 |0\rangle \otimes \hat{H}_3 |1\rangle \otimes \hat{I}_4 |1\rangle \otimes \hat{H}_5 |0\rangle \otimes \hat{I}_6 |1\rangle \otimes \hat{H}_7 |0\rangle \otimes \hat{I}_8 |1\rangle = \\ &= |q_-\rangle \otimes |0\rangle \otimes |q_-\rangle \otimes |1\rangle \otimes |q_+\rangle \otimes |1\rangle \otimes |q_+\rangle \otimes |1\rangle = \\ &= |q_-, 0, q_-, 1, q_+, 1, q_+, 1\rangle_8. \end{aligned} \quad (8.2)$$

Здесь кубиты $|q_{\pm}\rangle \equiv (|0\rangle \pm |1\rangle)/\sqrt{2}$ возникают в результате действия гейта Адамара $|q_+\rangle \equiv \hat{H}|0\rangle$, $|q_-\rangle \equiv \hat{H}|1\rangle$.

Кубиты из регистра $|y\rangle_8$ абонент А по квантовому каналу связи последовательно (первый, второй, третий и т.д.) передаёт абоненту Б. При этом абонент Б не знает ни исходной последовательности, ни порядок вентиляй, которые использовал абонент А. В соответствии с рассматриваемым протоколом абонент Б случайным образом действует на получаемые кубиты своими вентилями \hat{H} и \hat{I} и после этого производит “измерение” полученного кубита. Пусть, например, случайная последовательность действия вентилями на получаемые кубиты у абонента Б оказалась следующая: $\hat{H}_1 \hat{H}_2 \hat{I}_3 \hat{I}_4 \hat{H}_5 \hat{H}_6 \hat{I}_7 \hat{I}_8$. Здесь индексы у операторов указывают на номер кубита из последовательности их поступления абоненту Б.

Так, при действии гейтом Адамара \hat{H}_1 на первый поступивший кубит $|q_-\rangle$ Б переводит его в состояние $|1\rangle$, так как $\hat{H}_1 |q_-\rangle = |1\rangle$, и при измерении получает точно 1. Однако при действии гейтом Адамара на второй

полученный кубит $|0\rangle$ Б переводит этот кубит в суперпозицию базисных состояний $|q_+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ и при измерении может получить с равной вероятностью значение, равное 0 или 1. Обозначим полученный им результат буквой x_2 , $x_2 \in 0, 1$. При продолжении обработки поступающих кубит в соответствии с выбранной им схемой действия вентилей результат измерения абонента Б образует последовательность

$$b = (1, x_2, x_3, 1, 0, x_6, x_7, 1), \quad x_i \in 0, 1. \quad (8.3)$$

Здесь буквами x_i отмечены такие значения, которые в измерении могли оказаться и 0, и 1. Например, могла образоваться такая последовательность $b' = (1, 1, 1, 1, 0, 0, 0, 1)$ и т. п.

После этого абоненты А и Б по открытому каналу связи обмениваются информацией о применённых ими последовательностях вентилей.

Последовательность абонента А есть $\hat{H}_1\hat{I}_2\hat{H}_3\hat{I}_4\hat{H}_5\hat{I}_6\hat{H}_7\hat{I}_8$; соответственно, последовательность абонента Б есть $\hat{H}_1\hat{H}_2\hat{I}_3\hat{I}_4\hat{H}_5\hat{H}_6\hat{I}_7\hat{I}_8$.

Получив такую информацию, они отмечают для себя только те кубиты, для которых использовали одинаковые вентили, так как дважды применённый вентиль даёт исходное состояние кубита. Этими кубитами в рассматриваемом примере являются первый, четвёртый, пятый и восьмой.

Далее абонент А по открытому каналу связи сообщает абоненту Б, что значение четвёртого и пятого бит в исходно случайно выбранной последовательности $a = (10110101)$ есть 1 и 0 соответственно. Абонент Б сравнивает эти значения с полученными им значениями при измерении четвёртого и пятого кубит, и, в случае если они оказываются совпадающими с объявленными абонентом А, он сообщает об этом абоненту А. В результате они могут рассматривать последовательность значений первого и восьмого кубит (1,1) в качестве секретного ключа шифрования, который они сгенерировали случайным образом. Если значения не совпали, сеанс связи прерывается.

В этом и состоит протокол BB84, который позволил абонентам сформировать общий секретный случайный ключ, находясь на удалении друг от друга. То есть выполнено секретное распространение случайного ключа, что обеспечивает защиту передаваемой информации в симметричной криптографической системе.

Конечно, приведённый пример чрезвычайно примитивен и изложен лишь в учебных целях. В реальном случае длина сгенерированной случайной исходной битовой последовательности значительно больше и получаемый ключ несравненно сложнее.

Рассмотренный выше протокол обеспечивает определения факта “прослушивания” квантового канала связи. Покажем это на изложенном выше примере. Пусть абонент А передаёт последовательность кубит (8.2). Если между абонентами А и Б в квантовом канале связи появляется “ злоумышленник” X, пытающийся перехватить сообщение, он должен будет применять к кубитам свои вентили с последующим измерением (чтением) кубит. Пусть, например, последовательность вентилей, которые использовал X, есть $\hat{H}_1\hat{H}_2\hat{H}_3\hat{H}_4\hat{I}_5\hat{I}_6\hat{I}_7\hat{I}_8$. В результате расшифровка, полученная X, даст последовательность кубит:

$$\begin{aligned} |X\rangle_8 &= \hat{H}_1\hat{H}_2\hat{H}_3\hat{H}_4\hat{I}_5\hat{I}_6\hat{I}_7\hat{I}_8 |q_-, 0, q_-, 1, q_+, 1, q_+, 1\rangle_8 = \\ &= |1, q_+, 1, q_-, q_+, 1, q_+, 1\rangle_8, \end{aligned} \quad (8.4)$$

а результат их измерения равен

$$X' = (1, x_2, 1, x_4, x_5, 1, x_7, 1), \quad x_i \in 0, 1. \quad (8.5)$$

Здесь через x_i обозначены результаты измерений кубита, которые могли оказаться равными 0 или 1. Пусть, например, данная последовательность оказалась вида $X' = (1, 0, 1, 0, 0, 1, 1, 1)$. Пытаясь скрыть факт прослушивания, злоумышленник к последовательности измеренных им кубит $|X'\rangle = |1, 0, 1, 0, 0, 1, 1, 1\rangle_8$ повторно применяет использованную им последовательность вентилей $\hat{H}_1\hat{H}_2\hat{H}_3\hat{H}_4\hat{I}_5\hat{I}_6\hat{I}_7\hat{I}_8$ в надежде восстановить полученные кубиты от абонента А. Результат у X получится в виде

$$|X\rangle_8 = \hat{H}_1\hat{H}_2\hat{H}_3\hat{H}_4\hat{I}_5\hat{I}_6\hat{I}_7\hat{I}_8 |X'\rangle = |q_-, q_+, q_-, q_+, 0, 1, 1, 1\rangle_8.$$

Последовательность кубит $|X\rangle_8$ X передаёт абоненту Б, который применяет к данной последовательности свои вентили $\hat{H}_1\hat{H}_2\hat{I}_3\hat{I}_4\hat{H}_5\hat{H}_6\hat{I}_7\hat{I}_8$ и после измерения получает результат в виде битовой последовательности $b_x = (1, 0, x_3, x_4, x_5, x_6, 1, 1)$, $x_i \in 0, 1$. Пусть, например, эта последовательность имела вид $b_x = (1, 0, 1, 1, 1, 0, 1, 1)$. И когда в соответствии с протоколом BB84 абонент А сообщает абоненту Б, что его значение четвёртого и пятого кубита есть (1,0), абонент Б видит по своему результату, что его четвёртый и пятый кубит дают (1,1), т. е. результат его измерений не совпадает с последовательностью, объявленной абонентом А по открытому каналу. Таким образом, абонент Б получает информацию о “прослушивании” квантового канала связи, о чём сообщает абоненту А, и связь прекращается.

Необходимо подчеркнуть, что факт прослушивания квантового канала связи в данном протоколе невозможно скрыть из-за того, что промежуточное измерение кубит злоумышленником неизбежно портит кубиты абонента А, а это регистрируется рассмотренным протоколом.

В заключение подчеркнём, что протокол BB84 не является криптографической системой. Это средство распределения уникальных вероятностных ключей перед сеансом связи в симметричных криптографических системах. Кроме того, в реальных системах число вентилей у абонентов значительно превышает два рассмотренных в приведённом выше простом примере, что, естественно, реально усиливает защищённость схемы распространения ключа.

Упражнение 8.2. Продемонстрировать реализацию протокола BB84 на основе случайно сгенерированной битовой последовательности из 16 бит.

Упражнение 8.3. Продемонстрировать обнаружение злоумышленника по протоколу BB84 на основе случайно сгенерированной битовой последовательности из 16 бит.

8.3 Квантовый протокол B92

Определённая громоздкость протокола BB84, которая проявляется в числе реально используемых вентилей и многоэтапности протокола, была частично преодолена в протоколе, предложенном Беннетом, получившем наименование B92-протокол. В рамках данного протокола последовательность общения абонентов также состоит из нескольких этапов, но последовательность действий абонента А фиксирована единым правилом.

Для объяснения протокола предположим, что абонент А имеет квантовое устройство, которое производит последовательность кубит на основании бинарной последовательности по определённому правилу. Это правило состоит в том, что если бит последовательности равен 0, то ему ставится в соответствие кубит $|0\rangle$. В случае если бинарной последовательности равен 1, то ему квантовая машина ставит в соответствие кубит вида $|q_+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$.

В свою очередь, у абонента Б имеется квантовое устройство, которое преобразует полученный им кубит в соответствии с действием одного из операторов $\hat{P}_1 = |1\rangle\langle 1|$ или $\hat{P}_- = |q_-\rangle\langle q_-|$, где $q_- = (|0\rangle - |1\rangle)/\sqrt{2}$. Фактически операторы \hat{P} являются операторами проектирования.

Таким образом, у абонента А имеется квантовая машина, производящая неортогональные состояния $|0\rangle$ и $|q_+\rangle$, а у абонента Б – квантовое устройство, проектирующее кубиты на пару неортогональных состояний $|1\rangle$ и $|q_-\rangle$.

На первом этапе реализации алгоритма B92 абонент А генерирует слу-

чайную бинарную последовательность, например $a = (10111100)$, которую на квантовом устройстве превращает в последовательность кубит по установленному выше правилу. Таким образом, на данном этапе у абонента А из выбранной им бинарной последовательности $a = (10111100)$ появляется последовательность кубит вида (при этом нумерация кубит, как и в предыдущем разделе, слева направо)

$$|q_a\rangle_8 = |q_+\rangle \otimes |0\rangle \otimes |q_+\rangle \otimes |q_+\rangle \otimes |q_+\rangle \otimes |q_+\rangle \otimes |0\rangle \otimes |0\rangle.$$

Далее абонент А посыпает абоненту Б полученные кубиты последовательно по имеющемуся квантовому каналу связи.

Абонент Б до начала сеанса связи также генерирует случайную битовую последовательность. Пусть его последовательность оказалась равной $b = 00101010$. Эта последовательность ему нужна для того, чтобы в соответствии с ней проводить преобразование получаемых от А кубит. Его правило реализации последовательности состоит в том, что при значении бита из b , равного нулю, абонент Б применяет к полученному кубиту оператор \hat{P}_- и производит измерение результата, а при значении бита, равного 1, применяет оператор \hat{P}_1 с последующим измерением кубита. То есть для выбранной им последовательности порядок применения операторов есть (слева направо) $\hat{P}_-, \hat{P}_-, \hat{P}_1, \hat{P}_-, \hat{P}_1, \hat{P}_-, \hat{P}_-$. Таким образом, получив первый кубит от А, абонент Б применяет к нему оператор \hat{P}_- и производит вычисления:

$$|z_1\rangle = \hat{P}_- : |q_+\rangle = |q_-\rangle \langle q_- | q_+ \rangle = 0,$$

так как $\langle q_- | q_+ \rangle = 0$. Фактически данное равенство означает, что применённый анализатор не зарегистрирует кубит. Данное обстоятельство абонент Б может фиксировать у себя значением 0 или значком N (No).

Для второго кубита абонент Б опять применяет оператор \hat{P}_- . Однако теперь он получит следующий результат:

$$\begin{aligned} |z_2\rangle &= \hat{P}_- : |0\rangle = |q_-\rangle \langle q_- | : |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \frac{1}{\sqrt{2}}(\langle 0| - \langle 1|) |0\rangle = \\ &= \frac{|0\rangle - |1\rangle}{2}. \end{aligned}$$

Измерив данный кубит, Б получит значение 0 или 1 с равной вероятностью. Обозначим для общности результат его измерения через x_2 , где $x_2 \in \{0, 1\}$.

На полученный третий кубит абонент Б действует оператором \hat{P}_1 :

$$\hat{P}_1 : |q_+\rangle \rightarrow |1\rangle / \sqrt{2}.$$

Вся выбранная абонентом Б последовательность операторов представлена в табл. 8.2, в которой указаны случайная последовательность абонента А, посланные абонентом А кубиты, случайная последовательность, выбранная абонентом Б, соответствующая последовательность операторов абонента Б, результат измерения кубит абонентом Б, реальный пример измерения кубит абонентом Б.

Таблица 8.2

Последовательности действий и результатов абонентов А и Б

	1	2	3	4	5	6	7	8
Последовательность a	1	0	1	1	1	1	0	0
Кубиты, посланные от А	$ q_+\rangle$	$ 0\rangle$	$ q_+\rangle$	$ q_+\rangle$	$ q_+\rangle$	$ q_+\rangle$	$ 0\rangle$	$ 0\rangle$
Последовательность b	0	0	1	0	1	0	1	0
Операторы \hat{P}_i абонента Б	\hat{P}_-	\hat{P}_-	\hat{P}_1	\hat{P}_-	\hat{P}_{-1}	\hat{P}_-	\hat{P}_1	\hat{P}_-
Результат действия \hat{P}_i	N	x_2	1	N	1	N	0	x_8
Пример	0	0	1	0	1	0	0	1

Далее абонент Б объявляет (сообщает А по открытому каналу) номера кубит, измерение которых дало значение, равное 1. В приведённом примере это третий, пятый и восьмой кубиты. Тогда абонент А из своей последовательности a выделяет третий, пятый и восьмой биты, а абонент Б те же биты фиксирует в своей последовательности b . Как видно, они одинаковы (1,1,0). Данная битовая последовательность служит секретным случайнym ключом в симметричной криптографической системе во время сеанса связи.

В реальном случае длина выбранных последовательностей существенно больше, а регистрация прослушивания квантового канала связи устанавливается аналогично тому, как это было изложено в протоколе BB84.

Таким образом, в протоколе B92 играют важную роль только те кубиты, которые дают значение, равное 1, в процессе их измерения абонентом Б. Остальные кубиты отбрасываются.

Упражнение 8.4. Продемонстрировать реализацию протокола B92 на основе случайно сгенерированной битовой последовательности из 16 бит.

Упражнение 8.5. Продемонстрировать обнаружение злоумышленника по протоколу B92 на основе случайно сгенерированной битовой последовательности из 16 бит.

Библиографический список

1. Абрамовиц М. Справочник по специальным функциям / М. Абрамовиц, И. Стиган. – М. : Наука, 1979. – 832 с.
2. Бауэр А. Информатика. Вводный курс : в 2 ч. / А. Бауэр ; пер. с нем. под ред. Д. Ершова. – М. : Мир, 1990. – 423 с.
3. Валиев К. А. Квантовые компьютеры : надежды и реальность / К. А. Валиев, А. А. Кокин. – М. ; Ижевск : R&C, 2001. – 351 с.
4. Варшалович Д. А. Квантовая теория углового момента / Д. А. Варшалович, А. Н. Москалёв, В. К. Херсонский. – Л. : Наука, 1975. – 439 с.
5. Давыдов А. С. Квантовая механика / А. С. Давыдов. – М. : Наука, 1973. – 704 с.
6. Дирак П. Принципы квантовой механики / П. Дирак ; пер. с англ. под ред. В. А. Фока. – М. : Наука, 1979. – 480 с.
7. Имре Ш. Квантовые вычисления и связь / Ш. Имре, Ф. Балаж. – М. : Физматлит, 2008. – 319 с.
8. Кайе Ф. Введение в квантовые вычисления / Ф. Кайе, Р. Лафламм, М. Москва. – М. ; Ижевск : R&C, 2009. – 346 с.
9. Нильсен М. Квантовые вычисления и квантовая информация / М. Нильсен, И. Чанг. – М. : Мир, 2006. – 824 с.
10. Ожигов Ю. И. Квантовые вычисления / Ю. И. Ожигов. – М. : Макс Пресс, 2003. – 152 с.
11. Прескил Дж. Квантовая информация и квантовые вычисления / Дж. Прескил. – Ижевск : РХД, 2011. – 312 с.
12. Флюге З. Задачи по квантовой механике : в 2 т. / З. Флюге. – М. : Мир, 1974. – Т. 1. – 341 с. ; Т. 2. – 315 с.
13. Branstein S. L. Quantum Computation / S. L. Branstein // Encyclopedia of Applied Physics. – Update 1. Berlin : Wiley-VCH, 1999. – P. 239–256.
14. Deutsch D. Quantum Theory the Church-Turing Principle and the Universal Quantum Computer / D. Deutsch // Proc. Roy. Soc. – London, 1985. – V. A400, № 1818. – P. 57. Перевод с английского под ред. В. А. Садовничего: Сб. «Квантовый компьютер и квантовые вычисления». – Ижевск : Ред. журн. «Регулярная и хаотическая динамика», 1999. – 268 с.
15. Deutsch D. Rapid Solution of Problems by Quantum Computation / D. Deutsch, R. Jozsa // Proc. Roy. Soc. – London, 1992. –

- V. A439, № 1907. – Р. 553. Перевод с английского под ред. В. А. Садовничего: Сб. «Квантовый компьютер и квантовые вычисления». – Ижевск : Ред. журн. «Регулярная и хаотическая динамика», 1999. – 268 с.
16. *Fowler A. G.* Robustness of Shor's algorithm with finite rotation control / A. G. Fowler, L. C. L. Hollenberg. – 2003. – e-print quant-ph/0306018
17. *Keyes R. W.* Miniaturization of electronics and its limits / R. W. Keyes // IBM Journal of Research and Development. – 1988. – V. 32. – P. 24.
18. *Odiyzko A. M.* The future of integer factorization / A. M. Odiyzko // AT&T Bell Laboratories, preprint (1995).
19. *Shor P.* Polynomial-Time Algorithms for Prime Factorization and Descrete Logarithms on a Quantum Computer / P. Shor // SIAM Your Comp. – 1997. – V. 26, № 5. – P. 1484–1509.
20. *Toffoli T.* Bicontinuous extensions of invertible combinatorial functions / T. Toffoli // Mathematical Systems Theory. – 1981. – V. 14. – P. 13–23.