РЕФЕРАТ

30 Апреля 2023

Автор: *Д. И. Дружкин*

Федеральное государственное бюджетное образовательное учреждение высшего образования «Саратовский национальный исследовательский государственный университет имени Н. Г. Чернышевского»

КВАНТОВЫЕ КОМПЬЮТЕРЫ, КВАНТОВЫЕ ЭЛЕМЕНТЫ КОМПЬЮТЕРНЫХ СИСТЕМ

Реферат посвящен изложению принципов работы квантовых компьютеров и их элементов. Обозначаются цели, для которых могут использоваться квантовые компьютеры. Вводится понятие кубита, перечисляются некоторые способы реализации кубитов. Представлена теория идеальных компьютеров, не взаимодействубщих с окружением и не подверженных процессам квантовой декогерентизации. Реферат завершается оценкой ситуации на сегодняшний день, перечисляются уже существующие квантовые компьютеры и обсуждается будущее квантовой теории информации.

Введение

Современные компьютеры, несмотря на все их чудеса, работают по тому же фундаментальному принципу, что и механические устройства, придуманные Чарльзом Бэббиджем в 19 веке и позже формализованные Аланом Тьюрингом: одно стабильное состояние машины представляет одно число. Даже, казалось бы, нестандартные вычислительные модели, такие как модель, основанная на ДНК, разделяют этот основной принцип. Тем не менее физики показали, что законы, описывающие мир природы, — это не простые законы классической механики, а более тонкие законы квантовой физики, и они побуждают нас по-другому думать о вычислениях ...

Цифровые электронные компьютеры, широко используемые в настоящее время, созданы с помощью полупроводниковых технологий. Такие компьютеры обычно представляют собой совокупность элементов только с двумя возможными логическими состояниями «0» и «1» — так называемых битов (binary digits = bits), вентильных элементов, и соединений между ними. Такие компьютеры, в которых логические операции производятся с этими классическими, с точки зрения физики, состояниями, в настоящее время принято называть *классическими.*

Однако уже достаточно давно было обнаружено, что эти классические компьютеры не могут справиться с некоторыми очень важными задачами. Примерами таких задач являются поиск в неструктурированной базе данных, моделирование эволюции квантовых систем (например, ядерные реакции) и, наконец, факторизация больших чисел.

Интерес к последней задаче связан с тем, что практически все современные шифры для секретной переписки основаны на этой математической процедуре.

Для взлома уже существующего кода необходима работа классического компьютера в течении нескольких лет. Предполагаемое экспоненциальное увеличение счёта в случае возникновения квантового компьютера сильно встревожило «секретное» мировое сообщество, и оно стала вкладывать немалые средства в исследования и разработки в области квантового компьютера и квантовых вычислений.

Квантовые биты

Бит — это фундаментальное понятие классических вычислений и классической информации. Квантовые вычисления и квантовая информация построены на аналогичной концепции — квантовом бите, или сокращенно кубите. В этом разделе мы познакомимся со свойствами одиночных кубитов, сравнивая и противопоставляя их свойства свойствам классических битов.

Что такое кубит? Мы собираемся описать кубиты как математические объекты с определенными специфическими свойствами. «Но подождите, — скажете вы, — я думал, кубиты — это физические объекты». Это верно, что кубиты, как и биты, реализуются как реальные физические системы, между абстрактной математической точкой зрения и реальными системами существует связь. Однако по большей части мы рассматриваем кубиты как абстрактные математические объекты. Прелесть рассмотрения кубитов как абстрактных сущностей заключается в том, что это дает нам свободу в по-

строении общей теории квантовых вычислений и квантовой информации, реализация которой не зависит от конкретной системы. Что же тогда такое кубит? Точно так же, как классический бит имеет состояние — либо 0, либо 1, — кубит также имеет состояние. Двумя возможными состояниями для кубита являются состояния $|0\rangle$ и $|1\rangle$, которые, как вы могли догадаться, соответствуют *состояниям* 0 и 1 для классического бита. Обозначение типа «$|\ \rangle$» называется *обозначением Дирака*, и мы будем часто его видеть, поскольку это стандартное обозначение состояний в квантовой механике. Разница между битами и кубитами заключается в том, что кубит может находиться в *состоянии*, отличном от $|0\rangle$ или $|1\rangle$. Также возможно формировать *линейные комбинации* состояний, часто называемые *суперпозициями*:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1}$$

где α и β — комплексные числа. Способность кубита находиться в состоянии суперпозиции противоречит нашему пониманию окружающего нас физического мира, основанному на «здравом смысле». Классический бит подобен монете: либо орлом, либо решкой вверх. Для несовершенных монет могут существовать промежуточные состояния, такие как балансирование на ребре, но в идеальном случае ими можно пренебречь. Напротив, кубит может существовать в континууме состояний между $|0\rangle$ и $|1\rangle$ — до тех пор, пока его не будут наблюдать. Давайте еще раз подчеркнем, что когда измеряется кубит, он всегда выдает только «0» или «1» в качестве результата измерения. Например, кубит может находиться в состоянии

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \tag{2}$$

что при измерении дает результат 0 в половине случаев ($|1/\sqrt{2}|^2$) и результат 1 в половине случаев. Несмотря на эту странность, кубиты определенно реальны, их существование и поведение полностью подтверждены экспериментами (Опыт Штерна–Герлаха), и для реализации кубитов можно использовать множество различных физических систем.

Чтобы получить конкретное представление о том, как может быть реализован кубит, полезно перечислить некоторые из способов, которыми эта реализация может произойти: две разные поляризации фотона; выравнивание ядерного спина в однородном магнитном поле; два состояния электрона, вращающегося вокруг одного атома, как показано на рис. 1. В модели атома электрон может существовать либо в так называемом «основном», либо в «возбужденном» состояниях, которые мы будем называть $|0\rangle$ и $|1\rangle$ соответственно. Направляя свет на атом с соответствующей энергией и в течение соответствующего промежутка времени, можно перевести электрон из состояния $|0\rangle$ в состояние $|1\rangle$ и наоборот. Но что еще более интересно, сокращая время, в течение которого мы излучаем свет, электрон, изначально находящийся в состоянии $|0\rangle$, может быть перемещен «на полпути» между $|0\rangle$ и $|1\rangle$, в состояние $|+\rangle$.

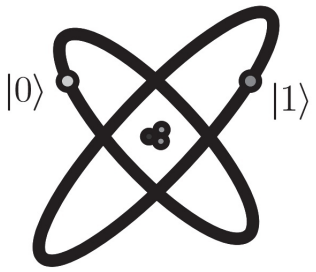

Рисунок 1. Кубит, представленный двумя электронными уровнями в атоме.

Так как $|\alpha^2| + |\beta^2| = 1$, мы можем записать равенство (1) следующим образом:

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right), \tag{3}$$

где θ, ϕ и γ — действительные числа. На самом деле мы можем не учитывать влияние $e^{i\gamma}$ из-за отсутствия *заметных эффектов*, что позволит нам записать это выражение в следующем виде:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle. \tag{4}$$

Числа θ и ϕ определяют точку на единичной трехмерной сфере, как показано на рис. 2. Эту сферу часто называют сферой Блоха (названной в честь Феликса Блоха). Она обеспечивает хорошую визуализацию состояния отдельного кубита и часто служит отличным испытательным стендом для идей о квантовых вычислениях и квантовой информации. Многие операции над одним кубитом четко описаны в рамках сферы Блоха. Однако следует иметь в виду, что не существует обобщения сферы Блоха на множество кубитов.

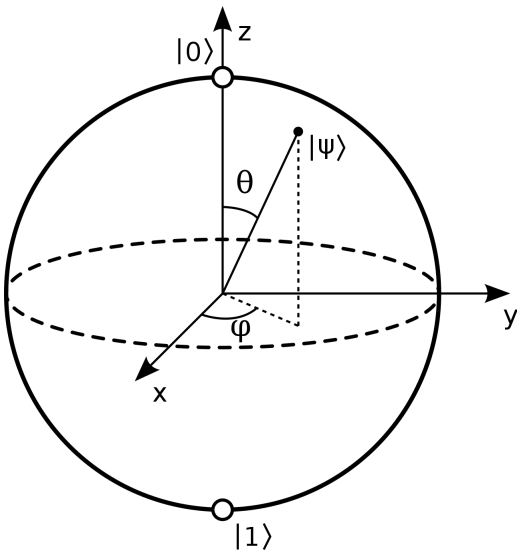

Рисунок 2. Преставление кубита в виде сферы Блоха.

Какой объем информации представлен кубитом? Парадоксально, но на единичной сфере существует бесконечное число точек, так что в принципе можно было бы сохранить весь текст Шекспира в бесконечном двоичном разложении θ. Однако этот вывод является заблуждением из-за поведения кубита при наблюдении. Напомним, что измерение кубита даст *только* либо 0, либо 1. Кроме того, измерение *изменяет* состояние кубита, переводя его из суперпозиций $|0\rangle$ и $|1\rangle$ в конкретное состояние, соответствующее результату измерения. Например, если измерение $|+\rangle$ дает 0, то состояние кубита после измерения будет равно $|0\rangle$. Почему такое происходит? Никто не знает. Такое поведение является одним из *фундаментальных постулатов* квантовой механики. Что важно для наших целей, так это то, что в результате одного измерения можно получить только один бит информации о состоянии кубита, разрешая таким образом кажущийся парадокс. Оказывается, что только в том случае, если было измерено бесконечно много одинаковых подготовленных кубитов, можно было бы определить α и β для кубита в состоянии, заданном в уравнении (1). Но еще более интересным является вопрос: какой объем информации представлен кубитом, если *мы его не измеряем*? Это вопрос с подвохом, потому что как можно количественно оценить информацию, если ее нельзя измерить? Тем не менее, здесь есть нечто концептуально важное, потому что, когда Природа развивает замкнутую квантовую систему кубитов, не выполняя никаких «измерений», она, по-видимому, отслеживает все непрерывные переменные, описывающие состояние, такие как α и β. В некотором смысле, в состоянии кубита Природа скрывает огромное количество «скрытой информации». И что еще более интересно, потенциальный объем этой дополнительной «информации» растет экспоненциально с увеличением количества кубитов. Понимание этой скрытой квантовой информации — это вопрос, который лежит в основе того, что делает квантовая механика — мощный инструмент для обработки информации.

Множества кубитов

Рассмотрим систему из n кубитов. Вычислительные базовые состояния этой системы имеют вид $|x_1 x_2 \dots x_n\rangle$, и поэтому квантовое состояние такой системы задается 2^n амплитудами. Для $n = 500$ это число больше, чем предполагаемое количество атомов во Вселенной! Попытка сохранить все эти комплексные числа была бы невозможна ни на одном классическом компьютере. Гильбертово пространство действительно большое. Однако Природа манипулирует такими огромными объемами данных даже для систем, содержащих всего несколько сотен атомов. Это похоже на то, как если бы Природа хранила 2^{500} бумажек, на которых она выполняет свои вычисления по мере развития системы. Эта огромная потенциальная вычислительная мощность — то, чем мы бы очень хотели воспользоваться. Но как мы можем думать о квантовой механике как о вычислении?

Изменения, происходящие в квантовом состоянии, могут быть описаны с помощью языка квантовых вычислений. Аналогично тому, как классический компьютер строится из электрической схемы, содержащей провода и логические элементы, квантовый компьютер строится из *квантовой схемы*, содержащей провода и элементарные квантовые элементы для переноса квантовой информации и манипулирования ею.

Физическая реализация

Каковы *экспериментальные требования* для создания квантового компьютера? Элементарными единицами теории являются квантовые биты — двухуровневые квантовые системы. Чтобы реализовать квантовый компьютер, мы должны не только дать кубитам некоторое надежное физическое представление (в котором они сохраняют свои квантовые свойства), но и выбрать *систему*, в которой их можно заставить эволюционировать по желанию. Кроме того, мы должны уметь подготавливать кубиты в некотором *заданном* наборе начальных состояний и измерять конечное выходное состояние системы.

Проблема экспериментальной реализации заключается в том, что эти основные требования часто могут быть выполнены лишь частично. Монета имеет два состояния и является хорошим битом, но плохим кубитом, потому что она не может оставаться в состоянии суперпозиции («орла» и «решки») очень долго. Одиночный ядерный спин может быть очень хорошим кубитом, потому что суперпозиции выравнивания с внешним магнитным полем или против него могут сохраняться долгое время — даже в течение нескольких дней. Но построить квантовый компьютер из ядерных спинов может быть трудно из-за проблемы в измерии ориентации отдельных ядер.

Требования весьма противоречивы: квантовый компьютер должен быть хорошо *изолирован*, чтобы сохранить свои квантовые свойства, но в то же время его кубиты должны быть *доступны*, чтобы ими можно было манипулировать для выполнения вычислений и считывания результатов. Реализация должна обеспечивать тонкий баланс между этими ограничениями, так что актуальный вопрос заключается не в том, как построить квантовый компьютер, а скорее в том, насколько хороший квантовый компьютер может быть построен.

Квантовый компьютер

Схема квантового компьютера представлена на

рис. 3. По существу квантовый компьютер представляет собой *регистр* из n кубитов, управляемых внешними (классическими) сигналами. Квантовый компьютер встроен в классическое окружение, состоящее из управляющего классического компьютера и генераторов импульсов, управляющих эволюцией кубитов, а также средствами измерений состояния кубитов. В ходе вычислений к регистру n можно добавить другие регистры, играющие вспомогательную роль (*ancillas*).

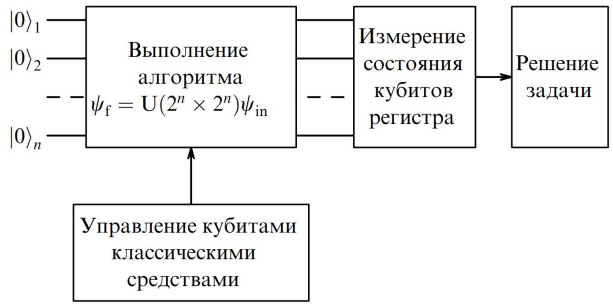

Рисунок 3. Схема квантового компьютера.

Назовем *идеальным* квантовый компьютер, состояния которого всегда когерентны. Это означает, во-первых, отсутствие взаимодействия компьютера с окружением, создающим шумы и нарушающим когерентность вектора состояния компьютера (декогерентизация); во-вторых, в идеальном квантовом компьютере внешние сигналы осуществляют точное управление.

Вектор состояния $|\psi\rangle$ квантового регистра из n кубитов представляет собой *разложение* по 2^n базисным состояниям регистра $|i_1 \dots i_n\rangle, i_1, \dots, i_n = \{0, 1\}$:

$$|\psi\rangle = \sum_{i_1,\dots,i_n} a_{i_1,\dots,i_n} |i_1 \dots i_n\rangle. \qquad (5)$$

Здесь суперпозиция $|\psi\rangle$ является вектором в 2^n-мерном векторном пространстве, $|i_1 \dots i_n\rangle$ — 2^n базисных векторов (ортов) этого пространства, $a_{i_1,\dots,i_n}$ — проекции вектора $|\psi\rangle$ на направления ортов $|i_1 \dots i_n\rangle$. Все, что можно сделать с системой, — это преобразовать ее начальный вектор состояния $|\psi_{in}\rangle$ в другой вектор: $|\psi_f\rangle$. Поэтому процесс вычислений на квантовом компьютере рассматривается как преобразование начального вектора состояния компьютера $|\psi_{in}\rangle$ в конечный вектор состояния $|\psi_f\rangle$ путем умножения вектора $|\psi_{in}\rangle$ на унитарную матрицу U размерности $2^n \times 2^n$:

$$|\psi_f\rangle = U(2^n \times 2^n)|\psi_{in}\rangle. \qquad (6)$$

Удобно полагать, что в начальном состоянии компьютера все его кубиты находятся в состоянии $|0\rangle$:

$$|\psi_{in}\rangle = |0_1 \dots 0_n\rangle. \qquad (7)$$

Эту операцию называют инициализацией. Состояние $|0_1 \dots 0_n\rangle$ можно получить или с помощью глубокого охлаждения (до температур порядка миликельвина), или путем применения методов поляризации.

Алгоритм решения задачи заключен в матрице преобразования $U(2^n \times 2^n)$. Классическая информация о решении задачи содержится в конечном векторе состояния $|\psi_f\rangle$; она должна быть получена измерением кубитов.

Для решения задачи на квантовом компьютере необходимо изготовить необходимое количество кубитов, инициализировать их, управлять их квантовой эволюцией, выполнить преобразование $U|\psi_{in}\rangle$ и измерить состояния кубитов, описываемых вектором $|\psi_f\rangle = U|\psi_{in}\rangle$.

Взгляд в будущее

На сегодняшний день квантовые компьютеры производятся, например, в октябре корпорация *Google* заявила, что добилась квантового превосходства — 54-кубитный квантовый процессор *Sycamore* сумел превзойти один из мощнейших в мире суперкомпьютеров *Summit* разработки *IBM* в задаче генерации случайных числовых строк, выполнив ее за 200 секунд, тогда как у классического суперкомпьютера на это ушло бы 10 000 лет.

Кроме того, существует квантовый процессор *D-Wawe Advantage* на 5760 кубитов, однако он может решать лишь ограниченный круг задач.

Допустим, придет время, когда будет освоена квантовая динамика систем на атомном уровне и построена квантовая информационная техника. Что дальше? Какие новые ресурсы природы могут быть использованы для создания новых поколений информационной техники? Степени свободы систем в меньших, чем атом, объемах (атомные ядра, элементарные частицы) связаны с большими энергиями, что затрудняет их использование для кодирования информации. Означает ли это, что на атомном уровне будут исчерпаны информационные ресурсы природы?

Список литературы

· Michael A. Nielsen, Isaac L. Chuang Quantum Computation and Quantum Information. 10th Anniversary Edition. 2010.
· Килин С. Я. Квантовая информация, май 1999 г. — Т. 169. № 5 — С. 507-527.
· Валиев К. А. Квантовые компьютеры: можно ли их сделать «большими»? — 1999. Т. 169. № 6 — С. 691-694.
· Валиев К. А. Квантовые компьютеры и квантовые вычисления. — 2005. — Т. 175. — С. 3-39.
· A. M. Steane, E. G. Rieffel. Beyond Dits: The Future of Quantum Information Processing. — January 2000. — P. 38-45.
· Квантовый компьютер и его полупроводниковая база. 08.04.2003.