РЕФЕРАТ

30 Октября 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. Обсуждаются квантовые вычисления. 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 построении 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 $|+\rangle$.

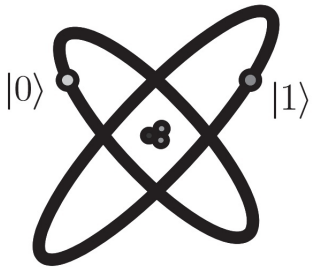

Рисунок 1. Кубит, представленный двумя электронными уровнями в атоме.

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

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

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:

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

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.

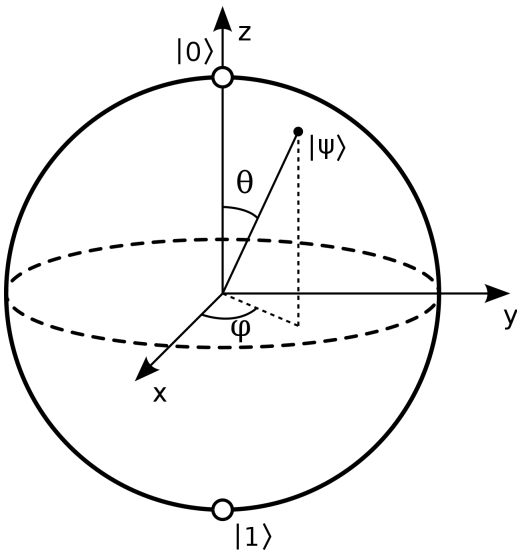

Рисунок 2. Преставление кубита в виде сферы Блоха.

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.

Однокубитные вентили

Классические компьютерные схемы состоят из проводов и логических элементов. Провода используются для передачи информации по схеме, в то время как логические элементы выполняют манипуляции с информацией, преобразуя ее из одной формы в другую. Рассмотрим, например, классические однобитовые логические элементы. Единственным нетривиальным членом этого класса является элемент NOT, работа которого определяется его таблицей истинности, в которой $0 \to 1$ и $1 \to 0$, то есть состояния 0 и 1 меняются местами.

Можно ли определить аналогичный квантовый элемент NOT для кубитов? Представьте, что у нас был какой-то процесс, который перевел состояние $|0\rangle$ в состояние $|1\rangle$, и наоборот. Такой процесс, очевидно, был бы хорошим кандидатом на квантовый аналог элемента NOT. Однако указание действия вентиля на состояния $|0\rangle$ и $|1\rangle$ не говорит нам, что происходит с суперпозициями состояний $|0\rangle$ и $|1\rangle$, без дополнительных знаний о свойствах квантовых вентилей. На самом деле квантовый элемент NOT действует линейно, то есть он переводит состояние

$$\alpha|0\rangle + \beta|1\rangle \tag{5}$$

в соответствующее состояние, в котором роли $|0\rangle$ и $|1\rangle$ поменялись местами,

$$\alpha|1\rangle + \beta|0\rangle. \tag{6}$$

Почему квантовый элемент NOT действует линейно, а не каким-то нелинейным образом — очень интересный вопрос, и ответ на него вовсе не очевиден. Оказывается, что это линейное поведение является общим свойством квантовой механики и очень хорошо мотивировано эмпирически; более того, нелинейное поведение может привести к очевидным парадоксам, таким как

путешествия во времени, связь быстрее света и нарушения вторых законов термодинамики. Существует удобный способ представления квантового элемента NOT в матричной форме, который непосредственно вытекает из линейности квантовых элементов. Предположим, мы определяем матрицу X для представления квантового элемента NOT следующим образом:

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{7}$$

Если квантовое состояние $\alpha|0\rangle + \beta|1\rangle$ записано в векторной записи как

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix}, \tag{8}$$

с верхней записью, соответствующей амплитуде для $\alpha|0\rangle$, а нижней — амплитуде для $\beta|1\rangle$, то соответствующий выходной сигнал квантового элемента NOT равен

$$X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}. \tag{9}$$

Обратите внимание, что действие элемента NOT состоит в том, чтобы взять состояние $\alpha|0\rangle$ и заменить его состоянием , соответствующим первому столбцу матрицы X. Аналогично, состояние $\beta|1\rangle$ заменяется состоянием, соответствующим второму столбцу матрицы X.

Таким образом, квантовые вентили на одном кубите могут быть описаны матрицами два на два. Существуют ли какие-либо ограничения на то, какие матрицы могут использоваться в качестве квантовых вентилей? Оказывается, так оно и есть. Напомним, что условие нормализации требует $|\alpha|^2 + |\beta|^2 = 1$ для квантового состояния $\alpha|0\rangle + \beta|1\rangle$. Это также должно быть верно для квантового состояния $|\psi'\rangle = \alpha'|0\rangle + \beta'|1\rangle$ после срабатывания вентиля. Оказывается, что подходящим условием для матрицы, представляющей элемент, является то, что матрица U, описывающая элемент с одним кубитом, должна быть *унитарной*, то есть $U^\dagger U = I$, где $U^\dagger$ — сопряженное значение U (полученное путем транспонирования и последующего комплексного сопряжения U), а I - единичная матрица два на два. Например, для элемента NOT легко проверить, что $X^\dagger X = I$.

Удивительно, но это ограничение унитарности является единственным ограничением для квантовых вентилей. Любая унитарная матрица определяет допустимый квантовый элемент! Интересным следствием является то, что в в отличие от классического случая, когда существует только один нетривиальный элемент управления — элемент NOT — существует множество нетривиальных элементов управления с одним кубитом. Двумя важными из них являются Z-вентиль:

$$Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \tag{10}$$

который оставляет $|0\rangle$ неизменным и меняет знак с $|1\rangle$ на $-|1\rangle$, и вентиль Адамара,

$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{11}$$

Этот вентиль иногда называют «квадратный корень из NOT» элемента, поскольку он меняет $|0\rangle$ на $(|0\rangle + |1\rangle)/\sqrt{2}$ (первый столбец H), «на полпути» между $|0\rangle$ и $|1\rangle$, и меняет $|1\rangle$ на $(|0\rangle - |1\rangle)/\sqrt{2}$ (второй столбец H), который также находится «на полпути» между $|0\rangle$ и $|1\rangle$. Обратите внимание, что H^2 не является элементом NOT, поскольку простая арифметика показывает, что $H^2 = I$, и , таким образом, двойное применение H к состоянию ничего с ним не делает.

Вентиль Адамара — один из самых полезных квантовых вентилей, и стоит попытаться визуализировать его работу, рассмотрев изображение сферы Блоха. На этом рисунке (рис. 3) оказывается, что одиночные кубитные вентили соответствуют вращениям и отражениям сферы.

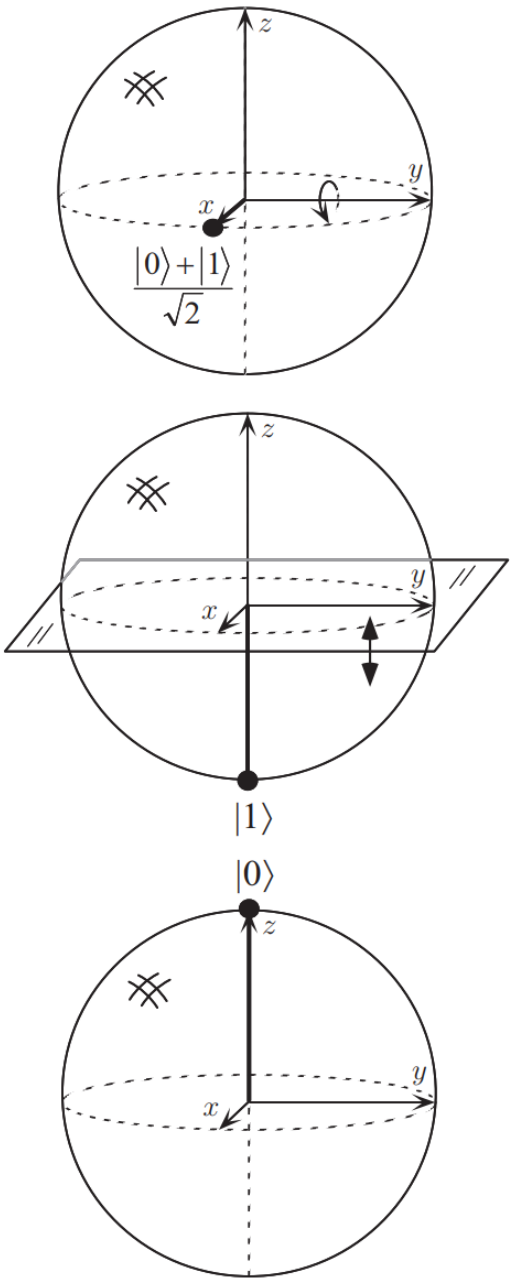

Рисунок 3 Визуализация вентиля Адамара на сфере Блоха, воздействующего на входное состояние $(|0\rangle + |1\rangle)/\sqrt{2}$.

Операция Адамара — это просто поворот сферы вокруг оси $\hat{y}$ на 90°, за которым следует поворот вокруг оси $\hat{x}$ на 180°, как показано на рис. 3. Некоторые важные однокубитные вентили показаны на рис. 4.

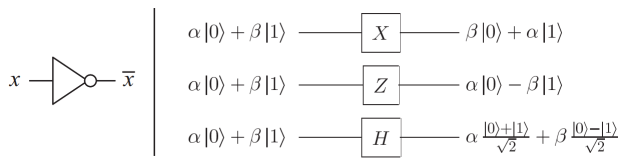

Рисунок 4 Логические элементы с одним битом (слева) и кубитом (справа)

Существует бесконечно много унитарных матриц два на два и, следовательно, бесконечно много однокубитных вентилей. Однако оказывается, что свойства полного набора можно понять из свойств гораздо меньшего набора. Например, произвольный унитарный элемент с одним кубитом может быть разложен как произведение вращений

$$\begin{bmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{bmatrix}, \tag{12}$$

и вентиль, который понимается как вращение вокруг оси $\hat{z}$,

$$\begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix}, \tag{13}$$

вместе с (глобальным) фазовым сдвигом — постоянным множителем формы $e^{i\alpha}$. Эти вентили могут быть разбиты дальше — нам не нужно уметь создавать эти вентили для произвольных α, β и γ, но можно строить сколь угодно хорошие аппроксимации для таких вентилей, используя только определенные специальные фиксированные значения α, β и γ. Таким образом, можно создать произвольный однокубитный вентиль, использующий конечный набор квантовых вентилей. В более общем плане, произвольное квантовое вычисление на любом количестве кубитов может быть сгенерировано конечным набором элементов, который, как говорят, универсален для квантовых вычислений. Чтобы получить такой универсальный набор, нам сначала нужно ввести некоторые квантовые вентили, включающие несколько кубитов.

Многокубитные вентили

Теперь давайте обобщим от одного до нескольких кубитов. На рисунке 5 показаны пять примечательных многоразрядных классических элементов управления: элементы AND, OR, XOR, NAND и NOR. Важным теоретическим результатом является то, что любая функция на битах может быть вычислена только из состава элементов NAND, которые, таким образом, известны как универсальные элементы. Напротив, XOR сам по себе или даже

вместе с NOT не является универсальным. Один из способов увидеть это — отметить, что применение элемента XOR не изменяет общую четность битов. В результате любая схема, включающая только элементы NOT и XOR, если два входа x и y имеют одинаковую четность, будет выдавать выходные данные одинаковой четности, ограничивая класс функций, которые могут быть вычислены, и, таким образом, исключая универсальность.

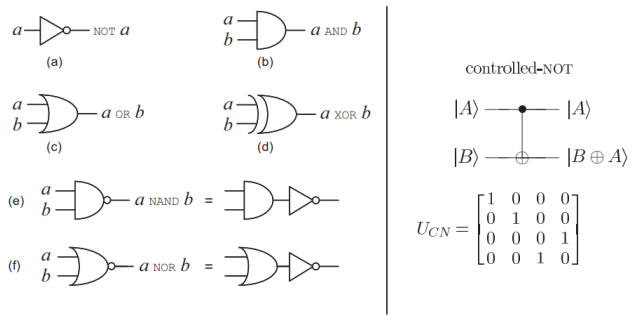

Рисунок 5 Слева расположены некоторые стандартные одно- и многоразрядные вентили, в то время как справа находится прототип многоразрядного кубитного вентиля, управляемый-NOT. Матричное представление управляемого-NOT, U_{CN} , записывается относительно амплитуд для $|00\rangle$, $|01\rangle$, $|10\rangle$ и $|11\rangle$, в таком порядке.

Прототипным многокубитным квантовым логическим элементом является элемент controlled-NOT или CNOT. Этот элемент управления имеет два входных кубита, известных как *управляющий* кубит и *целевой* кубит соответственно. Схемное представление CNOT показано в правом верхнем углу рисунка 5; верхняя строка представляет управляющий кубит, в то время как нижняя строка представляет целевой кубит. Действие вентиля может быть описано следующим образом. Если управляющий кубит установлен в 0, то целевой кубит остается в покое. Если управляющий кубит установлен в 1, то целевой кубит изменяется. В уравнениях:

$$\begin{aligned} &|00\rangle \to |00\rangle;\ |01\rangle \to |01\rangle; \\ &|10\rangle \to |11\rangle;\ |11\rangle \to |10\rangle. \end{aligned} \tag{14}$$

Другой способ описания CNOT — это обобщение классического элемента XOR, поскольку действие элемента может быть представлено как $|A,\ B\rangle \to |A,\ B \oplus A\rangle$, где $\oplus$ — сложение по модулю 2, что именно и делает XOR, то есть над контрольным и целевым кубитами проводится XOR, и результат сохраняется в целевой кубит.

Еще одним способом описания действия CNOT является предоставление матричного представления, как показано в правом нижнем углу рисунка 5. Вы можете легко убедиться, что первый столбец U_{CN} описывает преобразование, которое происходит с $|00\rangle$, и аналогично для других вычислительных базовых состояний, $|01\rangle$, $|10\rangle$, и $|11\rangle$. Что касается случая с одним кубитом, то требование сохранения вероятности выражается в том факте, что U_{CN} является унитарной матрицей, то есть $U_{CN}^{\dagger} U_{CN} = I$.

Мы заметили, что CNOT можно рассматривать как тип обобщенного элемента XOR. Могут ли другие классические элементы, такие как NAND или обычный элемент XOR пониматься как унитарные элементы в смысле, аналогичном тому, как квантовый элемент NOT представляет классический элемент NOT? Оказывается, это невозможно. Причина в том, что элементы XOR и NAND по существу необратимы. Например, учитывая выходные данные $A \oplus B$ из элемента XOR, невозможно определить, какими были входные данные A и B; существует безвозвратная потеря информации, связанная с необратимым действием элемента XOR. С другой стороны, унитарные квантовые вентили всегда обратимы, поскольку инверсия унитарной матрицы также является унитарной матрицей, и, таким образом, квантовый вентиль всегда может быть инвертирован другим квантовым вентилем. Понимание того, как использовать классическую логику в этом обратимом смысле, станет решающим шагом в понимании того, как использовать мощь квантовой механики для вычислений.

Конечно, есть много интересных квантовых вентилей, отличных от контролируемых-NOT. Однако в некотором смысле элементы с управляемым-NOT и однокубитным вентилем являются прототипами для всех других элементов из-за

следующего замечательного результата универсальности: любой логический элемент с несколькими кубитами может быть составлен из элементов CNOT и одиночных кубитов.

Измерения в базах, отличных от расчетной базы

Мы описали квантовые измерения одного кубита в состоянии $\alpha|0\rangle + \beta|1\rangle$ как дающие результат 0 или 1 и оставляющие кубит в соответствующем состоянии $|0\rangle$ или $|1\rangle$ с соответствующими вероятностями $|\alpha|^2$ и $|\beta|^2$. На самом деле, квантовая механика допускает несколько большую универсальность в классе измерений, которые могут быть выполнены, хотя, конечно, далеко не настолько, чтобы восстановить α и β из одного измерения!

Обратите внимание, что состояния $|0\rangle$ и $|1\rangle$ представляют собой лишь один из многих возможных вариантов базовых состояний для кубита. Другим возможным выбором является набор $|+\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}$ и $|-\rangle \equiv (|0\rangle - |1\rangle)/\sqrt{2}$. Произвольное состояние $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ может быть повторно выражено в терминах состояний $|+\rangle$ и $vert-\rangle$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha\frac{|+\rangle + |-\rangle}{\sqrt{2}} + \beta\frac{|+\rangle - |-\rangle}{\sqrt{2}} = \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle. \quad (15)$$

Оказывается, что можно рассматривать состояния $|+\rangle$ и $|-\rangle$ так, как если бы они были вычислительными базисными состояниями, и измерять относительно этого нового базиса. Естественно, измерение по отношению к базису $|+\rangle$, $|-\rangle$ приводит к результату «+» с вероятностью $|\alpha+\beta|^2/2$ и к результату «−» с вероятностью $|\alpha-\beta|^2/2$, с соответствующими состояниями $|+\rangle$ и $|-\rangle$ после измерения.

В более общем плане, учитывая любые базисные состояния $|a\rangle$ и $|b\rangle$ для кубита, можно выразить произвольное состояние как линейную комбинацию $\alpha|a\rangle + \beta|b\rangle$ этих состояний. Кроме того, при условии, что состояния *ортонормированы*, можно выполнить измерение относительно базиса $|a\rangle$, $|b\rangle$, получая результат a с вероятностью α^2 и b с вероятностью β^2. Ограничение ортонормированности необходимо для того, чтобы $|\alpha|^2 + |\beta|^2 = 1$, как мы и ожидаем для вероятностей. Аналогичным образом в принципе возможно измерить квантовую систему из многих кубитов относительно произвольного ортонормированного базиса.

Квантовые схемы

Давайте рассмотрим чуть более подробно элементы квантовой схемы. Простая квантовая схема, содержащая три квантовых элемента, показана на рис. 6. Схема должна считываться слева направо. Каждая линия в схеме представляет собой провод в квантовой схеме. Этот провод не обязательно соответствует физическому проводу; вместо этого он может соответствовать течению времени или, возможно, физической частице, такой как фотон — частица света, перемещающаяся из одного места в другое в пространстве. Принято считать, что состояние, входящее в схему является базовым вычислительным состоянием, обычно состоянием, состоящим из всех $|0\rangle$. Это правило часто нарушается в литературе по квантовым вычислениям и квантовой информации, но считается вежливым информировать читателя, что это имеет место.

Схема на рис. 6 выполняет простую, но полезную задачу — она меняет местами состояния двух кубитов. Чтобы увидеть, что эта схема выполняет операцию *swap*, обратите внимание, что последовательность элементов имеет следующую последовательность воздействий на вычислительное базовое состояние $|a, b\rangle$,

$$\begin{aligned} |a,b\rangle &\longrightarrow |a, a\oplus b\rangle \\ &\longrightarrow |a\oplus(a\oplus b), a\oplus b\rangle = |b, a\oplus b\rangle \\ &\longrightarrow |b, (a\oplus b)\oplus b\rangle = |b, a\rangle, \end{aligned} \quad (16)$$

где все сложения производятся по модулю

2. Таким образом, эффект схемы заключается в обмене состояниями двух кубитов.

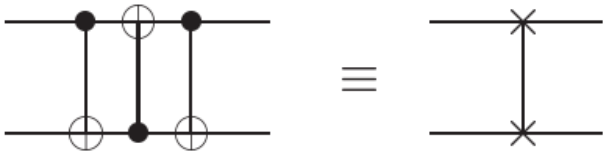

Рисунок 6 Схема, заменяющая два кубита, и эквивалентное схематическое обозначение для этой распространенной и полезной схемы.

В классических схемах разрешено несколько функций, которые обычно не присутствуют в квантовых схемах. Прежде всего, мы не допускаем «петель», то есть обратной связи от одной части квантовой схемы к другой; мы говорим, что схема ациклическая. Во-вторых, классические схемы позволяют «соединять» провода вместе, операция, известная как FANIN, при этом результирующий одиночный провод содержит побитовое OR входов. Очевидно, что эта операция необратима и , следовательно, не является унитарной, поэтому мы не допускаем FANIN в наших квантовых схемах. В-третьих, обратное операция FANOUT, при которой создается несколько копий бита, также не допускается в квантовых схемах. Фактически, оказывается, что квантовая механика запрещает копирование кубита, что делает операцию FANOUT невозможной!

По мере продвижения мы будем вводить новые квантовые элементы по мере необходимости. На этом этапе удобно ввести еще одно соглашение о квантовых схемах. Это соглашение проиллюстрировано на рис. 7. Предположим, что U — любая унитарная матрица, действующая на некоторое число n кубитов, поэтому U можно рассматривать как квантовый вентиль на этих кубитах. Затем мы можем определить элемент controlled-U, который является естественным продолжением элемента controlled-NOT. Такой вентиль имеет один контрольный кубит, обозначенный линией с черной точкой, и n целевых кубитов, обозначается буквой U в рамке. Если контрольный кубит установлен в 0, то с целевыми кубитами ничего не происходит. Если контрольный кубит установлен в 1, то элемент U применяется к целевым кубитам. Прототипическим примером элемента controlled-U является элемент controlled-NOT, который представляет собой элемент controlled-U с $U = X$, как показано на рисунке 8.

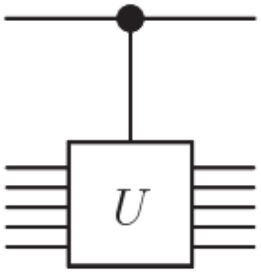

Рисунок 7 controlled-U вентиль.

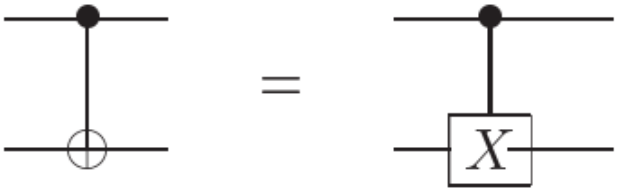

Рисунок 8 Два разных представления controlled-NOT вентиля

Другой важной операцией является измерение, которое мы обозначаем символом «M», как показано на рисунке 9. Как описано ранее, эта операция преобразует состояние одиночного кубита $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ в вероятностный классический бит M (отличающийся от кубита тем, что он представлен в виде двухлинейного провода), который равен 0 с вероятностью $|\alpha|^2$ и 1 с вероятностью $|\beta|^2$.

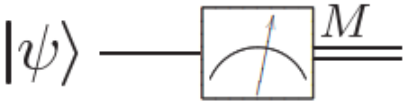

Рисунок 9 Символ квантовой схемы для измерения.

Квантовые схемы полезны в качестве моделей всех квантовых процессов, включая коммуникацию и даже квантовый шум. Ниже приведены несколько простых примеров, иллюстрирующих это.

Кубит копирует схему?

Элемент CNOT полезен для демонстрации одного особенно фундаментального свойства квантовой информации. Рассмотрим задачу копирования классического бита. Это может быть сделано с помощью классического элемента CNOT, который принимает бит для копирования (в некотором неизвестном состоянии x) и бит «блокнота», инициализированный нулем, как показано на рисунке 10. На выходе получается два бита, находящиеся в одном и том же состоянии x.

Предположим, мы пытаемся скопировать кубит в неизвестном состоянии $|\psi\rangle = a|0\rangle + b|1\rangle$ таким же образом, используя элемент CNOT. Входное состояние двух кубитов может быть записано как

$$\big[a|0\rangle + b|1\rangle\big]|0\rangle = a|00\rangle + b|10\rangle, \qquad (17)$$

Функция CNOT состоит в том, чтобы применить отрицание ко второму кубиту, когда первый равен 1, и, таким образом, на выходе получается просто $a|00\rangle + b|11\rangle$. Успешно ли мы скопировали $|\psi\rangle$? То есть, создали ли мы состояние $|\psi\rangle|\psi\rangle$? В случае, когда $|\psi\rangle = |0\rangle$ или $|\psi\rangle = |1\rangle$, это действительно то, что делает схема; можно использовать квантовые схемы для копирования классической информации, закодированной как $|0\rangle$ или $|1\rangle$. Однако для общего состояния $|\psi\rangle$ мы видим, что

$$|\psi\rangle|\psi\rangle = a^2|00\rangle + ab|01\rangle + ab|10\rangle + b^2|11\rangle. \quad (18)$$

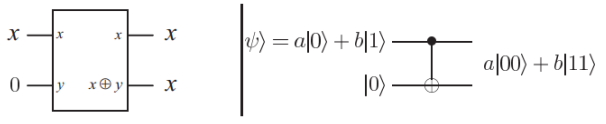

Рисунок 10 Классические и квантовые схемы для «копирования» неизвестного бита или кубита.

Сравнивая с $a|00\rangle + b|11\rangle$, мы видим, что, если $ab = 0$, описанная выше «схема копирования» *не* копирует входное квантовое состояние. На самом деле, оказывается невозможным создать копию неизвестного квантового состояния. Это свойство, заключающееся в том, что кубиты не могут быть скопированы, известно как теорема о недопустимости клонирования, и это одно из главных отличий квантовой информации от классической.

Существует другой способ взглянуть на сбой схемы на рис. 10, основанный на интуиции, что кубит каким-то образом содержит «скрытую» информацию, недоступную непосредственно измерению. Рассмотрим, что происходит, когда мы измеряем один из кубитов состояния $a|00\rangle + b|11\rangle$. Как описано ранее, мы получаем либо 0, либо 1 с вероятностями $|a|^2$ и $|b|^2$. Однако, как только один кубит измерен, состояние другого кубита полностью определено, и никакой дополнительной информации об a и b получить невозможно. В этом смысле, дополнительная скрытая информация, содержащаяся в исходном кубите $|\psi\rangle$, была потеряна при первом измерении и не может быть восстановлена. Однако если кубит был скопирован, то состояние другого кубита все равно должно содержать часть этой скрытой информации. Следовательно, копия не могла быть создана.

Пример: Состояния Белла

Давайте рассмотрим немного более сложную схему, показанную на рис. 11, которая имеет элемент Адамара, за которым следует CNOT, преобразующую четыре вычислительных базовых состояния в соответствии с приведенной таблицей. В качестве явного примера, элемент Адамара принимает входные данные от $|00\rangle$ до $(|0\rangle + |1\rangle)|0\rangle/\sqrt{2}$, и затем CNOT выдает выходное состояние $(|00\rangle + |11\rangle)/\sqrt{2}$. Обратите внимание, как это работает: во-первых, преобразование Адамара помещает верхний кубит в суперпозицию; затем это действует как управляющий вход для CNOT, и цель инвертируется только тогда, когда значение элемента управления равно 1. Выходные состояния

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}; \qquad (19)$$

$$|\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}; \qquad (20)$$

$$|\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}; \tag{21}$$

$$|\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \tag{22}$$

известны как *состояния Белла*, или иногда *состояния* EPR или *пары* EPR, в честь некоторых людей — Белла, Эйнштейна, Подольского и Розена, — которые первыми указали на странные свойства подобных состояний. Мнемоническое обозначение $|\beta_{00}\rangle$, $|\beta_{01}\rangle$, $|\beta_{10}\rangle$, $|\beta_{11}\rangle$ может пониматься из равенств

$$|\beta_{\mathrm{xy}}\rangle \equiv \frac{|0, \mathrm{y}\rangle + (-1)^{\mathrm{x}}|1, \bar{\mathrm{y}}\rangle}{\sqrt{2}}, \tag{23}$$

где $\bar{y}$ — отрицание y.

In	Out
$\|00\rangle$	$(\|00\rangle + \|11\rangle)/\sqrt{2} \equiv \|\beta_{00}\rangle$
$\|01\rangle$	$(\|01\rangle + \|10\rangle)/\sqrt{2} \equiv \|\beta_{01}\rangle$
$\|10\rangle$	$(\|00\rangle - \|11\rangle)/\sqrt{2} \equiv \|\beta_{10}\rangle$
$\|11\rangle$	$(\|01\rangle - \|10\rangle)/\sqrt{2} \equiv \|\beta_{11}\rangle$

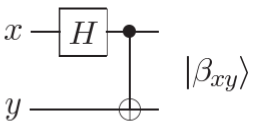

Рисунок 11 Квантовая схема для создания состояний Белла и ее входно–выходная квантовая «таблица истинности».

Пример: квантовая телепортация

Теперь мы применим методы, описанные на последних нескольких страницах, чтобы понять нечто нетривиальное, удивительное и очень забавное — квантовую телепортацию! Квантовая телепортация — это метод перемещения квантовых состояний даже при отсутствии квантового канала связи, связывающего отправителя квантового состояния с получателем. Вот как работает квантовая телепортация. Алиса и Боб познакомились давным-давно, но сейчас живут далеко друг от друга. Находясь вместе, они генерировали EPR-пару, каждый из них брал по одному кубиту из EPR-пары, когда они разделялись. Много лет спустя Боб скрывается, и миссия Алисы — доставить кубит $|\psi\rangle$ Бобу. Она не знает состояния кубита и, более того, может отправлять Бобу только *классическую* информацию. Должна ли Алиса взяться за эту миссию?

Интуитивно, для Алисы все выглядит довольно плохо. Она не знает состояния $|\psi\rangle$ кубита, который она должна отправить Бобу, и законы квантовой механики не позволяют ей определить состояние, когда в ее распоряжении есть только одна копия $|\psi\rangle$. Что еще хуже, даже если бы она знала состояние $|\psi\rangle$, для его точного описания требуется бесконечное количество классической информации, поскольку $|\psi\rangle$ принимает значения в непрерывном пространстве. Так что даже если бы она знала $|\psi\rangle$, Алисе потребовалась бы вечность, чтобы описать Бобу это состояние. К счастью для Алисы, квантовая телепортация — это способ использования запутанной пары EPR для отправки $|\psi\rangle$ Бобу с небольшими накладными расходами по сравнению с *классической* коммуникацией.

В общих чертах этапы решения следующие: Алиса взаимодействует с кубитом $|\psi\rangle$ со своей половиной EPR пары, а затем измеряет два имеющихся в ее распоряжении кубита, получая один из четырех возможных классических результатов: 00, 01, 10 и 11. Она отправляет эту информацию Бобу. В зависимости от классического сообщения Алисы Боб выполняет одну из четырех операций со своей половиной EPR пары. Удивительно, но, сделав это, он может восстановить исходное состояние $|\psi\rangle$!

Квантовая схема, показанная на рис. 12, дает более точное описание квантовой телепортации. Состояние, подлежащее телепортации — $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ где α и β — неизвестные амплитуды. Состояние $|\psi_0\rangle$, которое схема получает на вход, равно

$$|\psi 0\rangle = |\psi\rangle|\beta_{00}\rangle = \tag{24}$$

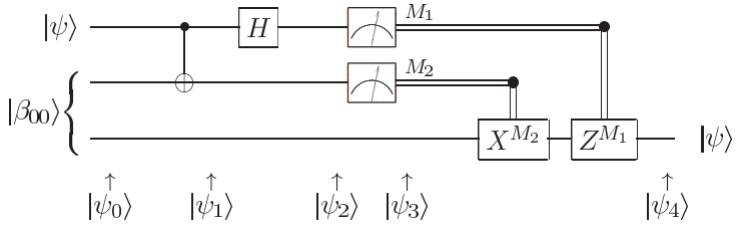

Рисунок 12 Квантовая схема для телепортации кубита. Две верхние строки представляют систему

Алисы, в то время как нижняя строка — систему Боба. Счетчики представляют собой измерение, а двойные линии, выходящие из них, несут классические биты (напомним, что одиночные линии обозначают кубиты).

$$= \frac{1}{\sqrt{2}}\big[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)\big], \tag{25}$$

где мы используем соглашение о том, что первые два кубита (слева) принадлежат Алисе, а третий кубит — Бобу. Как мы объясняли ранее, второй кубит Алисы и кубит Боба начинаются в состоянии EPR. Алиса отправляет свои кубиты через CNOT, получая

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\big[\alpha|0\rangle(|00\rangle+|11\rangle)+\beta|1\rangle(|10\rangle+|01\rangle)\big]. \tag{26}$$

Затем она отправляет первый кубит через вентиль Адамара, получая

$$\begin{aligned}|\psi_2\rangle = \frac{1}{2}\big[&\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle)+\\ &\beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)\big].\end{aligned} \tag{27}$$

Это состояние может быть переписано следующим образом, просто перегруппировав элементы:

$$\begin{aligned}|\psi_2\rangle = \frac{1}{2}\big[&|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle)\\ &+|10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)\big].\end{aligned} \tag{28}$$

Это выражение, естественно, распадается на четыре члена. Первый член содержит кубиты Алисы в состоянии $|00\rangle$, а кубит Боба — в состоянии $\alpha|0\rangle + \beta|1\rangle$, которое является исходным состоянием $|\psi\rangle$. Аналогично, из предыдущего выражения мы можем считать состояние Боба после измерения, учитывая результат измерения Алисы:

$$00 \longmapsto |\psi_3(00)\rangle \equiv \big[\alpha|0\rangle + \beta|1\rangle\big] \tag{29}$$

$$01 \longmapsto |\psi_3(01)\rangle \equiv \big[\alpha|1\rangle + \beta|0\rangle\big] \tag{30}$$

$$10 \longmapsto |\psi_3(10)\rangle \equiv \big[\alpha|0\rangle - \beta|1\rangle\big] \tag{31}$$

$$11 \longmapsto |\psi_3(11)\rangle \equiv \big[\alpha|1\rangle - \beta|0\rangle\big]. \tag{32}$$

В зависимости от результата измерения Алисы кубит Боба окажется в одном из этих четырех возможных состояний. Конечно, чтобы узнать, в каком состоянии он находится, Бобу необходимо сообщить результат измерения Алисы — позже мы покажем, что именно этот факт не позволяет использовать телепортацию для передачи информации быстрее света. Как только Боб узнает результат измерения, он может «исправить» свое состояние, восстановив $|\psi\rangle$, применив соответствующий квантовый вентиль. Например, в случае, когда измерение дает результат 00, Бобу ничего не нужно делать. Если значение равно 01, то Боб может исправить свое состояние, применив элемент X. Если значение равно 10, то Боб может исправить свое состояние, применив элемент Z. Если значение равно 11, то Боб может исправить свое состояние, применив сначала элемент X, а затем Z. В итоге Бобу придется применить $Z^{M_1}X^{M_2}$ (обратите внимание, как на схемах время идет слева направо, но в матричных произведениях термины справа появляются первыми) к своему кубиту, и он восстановит состояние $|\psi\rangle$.

Во-первых, разве телепортация не позволяет передавать квантовые состояния быстрее света? Это было бы довольно странно, поскольку теория относительности подразумевает, что передача информации со скоростью, превышающей скорость света, может быть использована для отправки информации назад во времени. К счастью, квантовая телепортация не обеспечивает связь быстрее света, потому что для завершения телепортации Алиса должна передать результат своего измерения в Боб по классическому каналу связи. Без классической коммуникации телепортация вообще не передает никакой информации. Классический канал ограничен скоростью света, из чего следует, что квантовая телепортация не может быть осуществлена быстрее скорости света, разрешая кажущийся парадокс.

Вторая загадка, связанная с телепортацией, заключается в том, что она, по-видимому, создает копию телепортируемого квантового состояния, что явно нару-

шает теорему о недопустимости клонирования, обсуждаемую ранее. Это нарушение является лишь иллюзорным, поскольку после процесса телепортации только целевой кубит остается в состоянии $|\psi\rangle$, а исходный кубит данных оказывается в одном из базовых вычислительных состояний $|0\rangle$ или $|1\rangle$, в зависимости от результата измерения в первом кубите.

Чему мы можем научиться из квантовой телепортации? Довольно многому! Это гораздо больше, чем просто изящный трюк, который можно проделать с квантовыми состояниями. Квантовая телепортация подчеркивает взаимозаменяемость различных ресурсов в квантовой механике, показывая, что общая пара EPR вместе с двумя классическими битами связи представляет собой ресурс, по меньшей мере равный одному кубиту связи. Квантовые вычисления и квантовая информация выявили множество методов обмена ресурсами, многие из которых основаны на квантовой телепортации.

Телепортация может быть использована для создания квантовых вентилей, устойчивых к воздействию шума, также телепортация тесно связана со свойствами квантовых кодов, исправляющих ошибки.

Оптический фотонный квантовый компьютер

Привлекательной физической системой для представления квантового бита является оптический фотон. Фотоны — это частицы без заряда, и они не очень сильно взаимодействуют друг с другом или даже с большей частью материи. Их можно направлять на большие расстояния с малыми потерями в оптических волокнах, эффективно задерживать с помощью фазовращателей и легко комбинировать с помощью светоделителей. Фотоны демонстрируют характерные квантовые явления, такие как интерференция, возникающая в экспериментах с двумя щелями. Более того, в принципе, фотоны можно заставить взаимодействовать друг с другом. С этим идеальным сценарием связаны проблемы; тем не менее, как мы увидим в этом разделе, из изучения компонентов, архитектуры и недостатков оптического фотонного квантового информационного процессора можно многому научиться.

Давайте начнем с рассмотрения того, что такое одиночные фотоны, как они могут представлять квантовые состояния и экспериментальные компоненты, полезные для манипулирования фотонами. Описано классическое поведение фазовращателей, расщепителей луча и нелинейно-оптических сред Керра.нергия в электромагнитном резонаторе квантуется в единицах $\hbar\omega$. Каждый такой квант называется фотоном. Полость может содержать суперпозицию нуля или одного фотона, состояние которого можно было бы выразить как кубит $c_0|0\rangle + c_1|1\rangle$, но мы сделаем кое-что другое. Давайте рассмотрим две полости, суммарная энергия которых равна $\hbar\omega$, и примем два состояния кубита за то, находится ли фотон в одной полости ($|01\rangle$) или в другой ($|10\rangle$). Таким образом, физическое состояние суперпозиции было бы записано как $c_0|01\rangle + c_1|10\rangle$; мы будем называть это представление *двойным рельсовым (dual-rail)*. Обратите внимание, что мы сосредоточимся на одиночных фотонах, распространяющихся в виде волнового пакета в свободном пространстве, а не внутри полости; можно представить это как наличие полости, движущейся вместе с волновым пакетом. Таким образом, каждая полость в нашем состоянии кубита будет соответствовать другому пространственному режиму.

Одна из схем генерации одиночных фотонов в лаборатории заключается в ослаблении мощности лазера. Лазер выводит состояние, известное как когерентное состояние, $|\alpha\rangle$, определяемое как

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle, \qquad (33)$$

где $|n\rangle$ — собственное состояние энергии n-фотонов. Это состояние, которое было

предметом тщательного изучения в области квантовой оптики, обладает многими прекрасными свойствами, которые мы не будем здесь описывать. Достаточно просто понять, что когерентные состояния естественным образом излучаются управляемыми генераторами, такими как лазер, при накачке выше порога генерации. Обратите внимание, что средняя энергия равна

$$\langle\alpha|n|\alpha\rangle = |\alpha|^2. \tag{34}$$

При ослаблении когерентное состояние просто становится более слабым когерентным состоянием, и с высокой вероятностью можно сделать так, чтобы в слабом когерентном состоянии был только один фотон.

Например, для $\alpha = \sqrt{0.1}$, мы получаем состояние $\sqrt{0.90}|0\rangle + \sqrt{0.09}|1\rangle + \sqrt{0.002}|2\rangle + \ldots$. Таким образом, если свет когда-либо проходит через аттенюатор, человек знает, что это одиночный фотон с вероятностью более 95%; таким образом, вероятность отказа составляет 5%. Обратите также внимание, что в 90% случаев фотоны вообще не проходят; таким образом, этот источник имеет скорость 0,1 фотона в единицу времени. Наконец, этот источник не указывает (посредством некоторого классического считывания), был ли выведен фотон или нет; два из этих источников не могут быть синхронизированы.

Лучшей синхронности можно достичь с помощью параметрического понижающего преобразования. Это включает в себя отправку фотонов частоты ω_0 в нелинейно-оптическую среду, такую как KH_2PO_4, для генерации пар фотонов на частотах $\omega_1 + \omega_2 = \omega_0$. Импульс также сохраняется, так что $\vec{k_1} + \vec{k_2} = \vec{k_3}$, так что когда (деструктивно) обнаруживается один фотон ω_2, то известно, что фотон ω_1 существует (рис. 13). Связывая это с вентилем, который открывается только при обнаружении одного фотона (в отличие от двух или более), и соответствующим образом задерживая выходные сигналы нескольких источников понижающего преобразования, можно, в принципе, получить множество одиночных фотонов, распространяющихся во времени синхронно, в пределах временного разрешения детектора и вентиля.

Одиночные фотоны могут быть обнаружены с высокой квантовой эффективностью в широком диапазоне длин волн с использованием различных технологий. Для наших целей наиболее важной характеристикой детектора является его способность с высокой вероятностью определять, существует ли ноль или один фотон в определенном пространственном режиме. Для представления с двумя рельсами это приводит к проективному измерению в вычислительном базисе. На практике несовершенства снижают вероятность обнаружения одиночного фотона; *квантовая эффективность* $\eta (0 \leq \eta \leq 1)$ фотоприемника — это вероятность того, что одиночный фотон, падающий на детектор, генерирует пару фотоносителей, которые вносят вклад в ток детектора. Другими важными характеристиками детектора являются его полоса пропускания (чувствительность ко времени), шум и «количество темных пятен», которые являются фотоносителями, генерируемыми даже при отсутствии падающих фотонов.

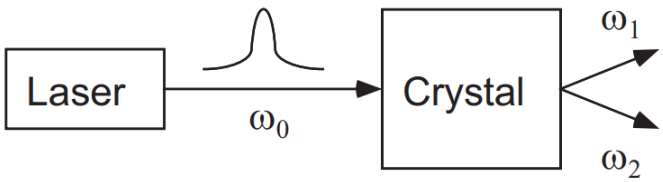

Рисунок 13 Параметрическая схема понижающего преобразования для генерации одиночных фотонов.

Тремя наиболее доступными в экспериментальном плане устройствами для манипулирования состояниями фотонов являются зеркала, фазовращатели и расщепители луча. Зеркала с высокой отражательной способностью отражают фотоны и изменяют направление их распространения в пространстве. Зеркала с потерями в 0,01% не являются чем-то необычным. Мы будем считать это само собой разумеющимся в нашем сценарии. Фазовращатель — это не что иное, как пластинка прозрачной среды с показателем преломления n, отличным от

показателя преломления свободного пространства n_0; например, обычное боросиликатное стекло имеет $n \approx 1,5n_0$ на оптических длинах волн. Распространение в такой среде на расстояние L изменяет фазу фотона на величину e^{ikL}, где $k = n\omega/c_0$, а c_0 — скорость света в вакууме. Таким образом, фотон, распространяющийся через фазовращатель, будет испытывать фазовый сдвиг $e^{i(n-n_0)L\omega/c_0}$ по сравнению с фотоном, проходящим то же расстояние через свободное пространство.

Другой полезный компонент, светоделитель, представляет собой не что иное, как частично посеребренный кусок стекла, который отражает долю R падающего света и пропускает $1 - R$. В лабораторных условиях светоделитель обычно изготавливается из двух призм, между которыми помещен тонкий металлический слой, схематически изображенный, как показано на рисунке 14. Удобно определить *угол* θ светоделителя как $\cos\theta = R$; обратите внимание, что угол параметризует величину частичного отражения и не обязательно имеет какое-либо отношение к физической ориентации светоделителя. Два входа и два выхода этого устройства связаны между собой как

$$a_{out} = a_{in}\cos\theta + b_{in}\sin\theta \tag{35}$$

$$b_{out} = -a_{in}\sin\theta + b_{in}\cos\theta, \tag{36}$$

где классически мы рассматриваем a и b как электромагнитные поля излучения на двух портах. Обратите внимание, что в этом определении мы выбрали нестандартное соглашение о фазе, удобное для наших целей. В частном случае светоделителя (50/50), $\theta = 45°$.

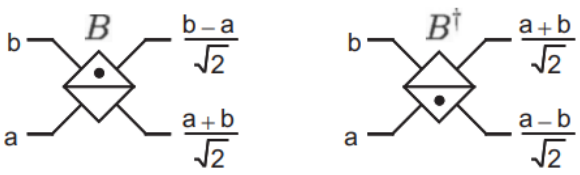

Рисунок 14 Схема оптического светоделителя, показывающая два входных порта, два выходных порта и фазовые соотношения для светоделителя 50/50 ($\theta = \frac{\pi}{4}$). Светоделитель справа является обратным по отношению к светоделителю слева (они различаются точкой, нарисованной внутри).

Нелинейная оптика обеспечивает полезный компонент для этого: материал, показатель преломления которого n пропорционален общей интенсивности I проходящего через него света:

$$n(I) = n + n_2 I. \tag{37}$$

Произвольные унитарные преобразования могут быть применены к квантовой информации, закодированной одиночными фотонами в двухканальном представлении $c_0|01\rangle + c_1|10\rangle$, с использованием фазовращателей, расщепителей луча и нелинейно-оптических сред Керра. Как это работает, можно понять следующим образом, дав квантово-механическое гамильтоново описание каждого из этих устройств.

Временная эволюция резонаторного режима электромагнитного излучения моделируется квантово-механически с помощью гармонического генератора. $|0\rangle$ — состояние вакуума, $|1\rangle = a^\dagger|0\rangle$ — состояние одиночного фотона, и в целом, $|n\rangle = \frac{a^{\dagger n}}{\sqrt{n!}}|0\rangle$ — это n-фотонное состояние,где $a^\dagger$ — оператор создания режима. Эволюция свободного пространства описывается Гамильтонианом:

$$H = \hbar\omega a^\dagger a, \tag{38}$$

и учитывая, что $|\psi(t)\rangle = e^{-iHt/\hbar}|\psi(0)\rangle = \sum_n c_n e^{-in\omega t}|n\rangle$, мы находим, что состояние $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$ со временем изменяется к $|\psi(t)\rangle = c_0|0\rangle + c_1 e^{-i\omega t}|1\rangle$. Обратите внимание, что представление с двумя рельсами удобно, поскольку свободная эволюция изменяет $|\phi\rangle = c_0|01\rangle + c_1|10\rangle$ только на общую фазу, которую невозможно обнаружить. Таким образом, для этого многообразия состояний эволюционный гамильтониан равен нулю.

Фазовращатель. Фазовращатель P действует точно так же, как обычная временная эволюция, но с другой скоростью и локализован только для режимов, проходящих через него. Это происходит потому, что свет замедляется в среде с большим

показателем преломления; в частности, для прохождения расстояния L в среде с показателем преломления n требуется на $\Delta \equiv (n - n_0)L/c_0$ больше времени, чем в вакууме. Например, действие P на вакуумное состояние состоит в том, чтобы ничего не делать: $P|0\rangle = |0\rangle$, но в однофотонном состоянии получается $P|1\rangle = e^{i\Delta}|1\rangle$.

P выполняет полезную логическую операцию в состоянии с двумя рельсами. Перевод фазовращателя в один режим замедляет его фазовую эволюцию по отношению к другому режиму, который проходит то же расстояние, но без прохождения через фазовращатель. Для состояний с двумя рельсами это преобразует $c_0|01\rangle + c_1|10\rangle$ в $c_0 e^{-i\Delta/2}|01\rangle + c_1 e^{i\Delta/2}|10\rangle$, вплоть до несущественной общей фазы. Эта операция является не чем иным, как вращением,

$$R_z(\Delta) = e^{-iZ\Delta/2}, \tag{39}$$

где мы принимаем за логический ноль $|0_L\rangle = |01\rangle$ и единицу $|1_L\rangle = |10\rangle$, а Z — оператор Паули. Таким образом, можно думать о P как о результате эволюции во времени в соответствии с Гамильтонианом

$$H = (n_0 - n)Z, \tag{40}$$

где $P = exp(-iHL/c_0)$.

Светоделитель. Аналогичное гамильтоново описание светоделителя также существует, но вместо того, чтобы мотивировать его феноменологически, давайте начнем с гамильтониана и покажем, как из него вытекает ожидаемое классическое поведение. Напомним, что светоделитель работает в двух режимах, которые мы опишем операторами создания (уничтожения) a ($a^\dagger$) и b ($b^\dagger$). Гамильтониан равен

$$H_{bs} = i\theta(ab^\dagger - a^\dagger b), \tag{41}$$

и светоделитель выполняет единую операцию

$$B = exp\big[\theta(a^\dagger b - ab^\dagger)\big]. \tag{42}$$

Преобразования, произведенные B над a и b, которые позже окажутся полезными, оказались следующими $BaB^\dagger = a\cos\theta + b\sin\theta$ и $BbB^\dagger = -a\sin\theta + b\cos\theta$. Мы проверяем эти соотношения, используя формулу Бейкера–Кэмпбелла–Хаусдорфа

$$e^{\lambda G} A e^{-\lambda G} = \sum_{n=0}^{\infty} \frac{\lambda^n}{n!} C_n, \tag{43}$$

где λ — комплексное число, $A,\ G,\ C_n$ — операторы, и C_n определяется рекурсивно как последовательность коммутаторов $C_0 = A, C_1 = [G, C_0], C_2 = [G, C_1], \ldots, C_n = [G, C_{n-1}]$. Поскольку из $[a, a^\dagger] = 1$ и $[b, b^\dagger] = 1$ следует, что $[G, a] = -b$ и $[G, b] = a$ для $G \equiv a^\dagger b - ab^\dagger$, мы получаем для разложения $BaB^\dagger$ коэффициенты ряда $C_0 = a, C_1 = [G, a] = -b, C_2 = [G, C_1] = -a, C_3 = [G, C_2] = -[G, C_0] = b$, что в общем случае

$$C_{n\ even} = i^n a \tag{44}$$

$$C_{n\ odd} = i^{n+1} b. \tag{45}$$

Из этого прямо вытекает наш желаемый результат:

$$\begin{aligned} BaB^\dagger &= e^{\theta G} a e^{-\theta G} \\ &= \sum_{n=0}^{\infty} \frac{\theta^n}{n!} C_n \\ &= \sum_{n\ even} \frac{(i\theta)^n}{n!} a + i \sum_{n\ odd} \frac{(i\theta)^n}{n!} b \\ &= a\cos\theta - b\sin\theta. \end{aligned} \tag{46}$$

Это известно как оптический эффект Керра, и он проявляется (очень слабо) в таких обыденных материалах, как стекло и сахарная вода. В легированных стеклах n_2 колеблется от 10^{-14} до 10^{-7} см^2/Вт, а в полупроводниках — от 10^{-10} до 10^2. Экспериментально соответствующее поведение заключается в том, что когда два пучка света равной интенсивности почти совместно распространяются через среду Керра, каждый пучок будет испытывать дополнительный фазовый сдвиг $e^{in_2 IL\omega/c_0}$ по сравнению с тем, что происходит в случае с одним пучком. Это было бы идеально, если бы длина L могла быть произвольной долго, но, к сожалению, это не удается, потому что большинство материалов Керра также обладают высокой поглощающей

способностью или рассеивают свет не в желаемом пространственном режиме. Это основная причина, по которой однофотонный квантовый компьютер непрактичен.

Однофотонное представление кубита привлекательно. Одиночные фотоны относительно просты в генерировании и измерении, а в представлении с двумя рельсами возможны произвольные операции с одним кубитом. К сожалению, взаимодействие фотонов затруднено — лучшие доступные нелинейные среды Керра очень слабы и не могут обеспечить перекрестную фазовую модуляцию π между состояниями одиночных фотонов. На самом деле, поскольку нелинейный показатель преломления обычно получается при использовании среды вблизи оптического резонанса, всегда присутствует некоторое поглощение связанное с нелинейностью, и теоретически можно оценить, что при наилучшем таком расположении должно быть поглощено приблизительно 50 фотонов для каждого фотона, который испытывает π-перекрестную фазовую модуляцию. Это означает, что перспективы создания квантовых компьютеров из традиционных компонентов нелинейной оптики в лучшем случае невелики.

Тем не менее, изучая этот оптический квантовый компьютер, мы получили некоторое ценное представление о природе архитектуры и системного проектирования квантового компьютера. Теперь мы можем видеть, как мог бы выглядеть настоящий квантовый компьютер в лаборатории (если бы для его создания были доступны только достаточно качественные компоненты), и поразительной особенностью является то, что он почти полностью построен из оптических интерферометров. В устройстве информация кодируется как в номере фотона, так и в фазе фотона, и для преобразования между этими двумя представлениями используются интерферометры. Хотя возможно сконструировать стабильные оптические интерферометры, если бы было выбрано альтернативное, массивное представление кубита, то быстро стало бы трудно создавать стабильные интерферометры из-за короткости типичных длин волн де Бройля.

Исторически сложилось так, что классические оптические компьютеры когда-то считались многообещающей заменой электронным машинам, но в конечном счете они не оправдали ожиданий, когда не были открыты в достаточной степени нелинейные оптические материалы и когда их преимущества в скорости и параллелизме недостаточно перевешивали недостатки в выравнивании и мощности. С другой стороны, оптическая связь является жизненно важной областью; одной из причин этого является то, что на расстояниях более одного сантиметра энергия, необходимая для передачи бита с использованием фотона по волокну, меньше энергии, необходимой для зарядки обычного электронная линия передачи 50 Ом, покрывающая то же расстояние. Аналогичным образом, возможно, что оптические кубиты могут найти естественное применение при передаче квантовой информации, например, в квантовой криптографии, а не в вычислениях.

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 оста-

ваться 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. 13. 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*).

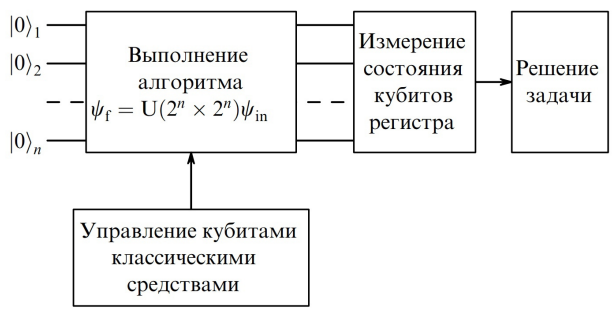

Рисунок 13. Схема квантового компьютера.

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 $|i_1 \dots i_n\rangle, i_1, \dots, i_n = \{0, 1\}$:

$$|\psi\rangle = \sum_{i_1,\dots,i_n} a_{i_1,\dots,i_n} |i_1 \dots i_n\rangle. \qquad (47)$$

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 $2^n \times 2^n$:

$$|\psi_f\rangle = U(2^n \times 2^n)|\psi_{in}\rangle. \qquad (48)$$

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

$$|\psi_{in}\rangle = |0_1 \dots 0_n\rangle. \qquad (49)$$

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.