Квантовые вычисления
Глава 2

Сысоев Сергей Сергеевич

Санкт-Петербургский государственный университет
Математико-механический факультет
http://se.math.spbu.ru/

1 Кубит

Разрекламировав в достаточной степени преимущества квантовых вычислений, перейдем, наконец, к математической модели квантового компьютера. Эта модель, описанная в достаточной степени, позволит нам оперировать квантовыми данными и квантовыми алгоритмами без отсылки к физическим процессам, на которых реализованы эти данные и алгоритмы. Понимание материала, представленного в этой главе, критически важно для понимания всего курса, поэтому к ней прилагается наибольшее количество упражнений и тестовых заданий.

Ключевым понятием всей теории квантовых вычислений является "кубит" – сокращение термина "квантовый бит" (**qu**antum **bit**) – минимальная информационная единица квантового мира. Так же, как бит является частичкой информации, содержащейся в простейшем содержательном классическом вычислительном процессе (типа двигателя Сциларда), кубит является описанием простейшей содержательной квантовой системы.

В рассмотренном нами ранее двигателе Сциларда бит информации кодировался камерой, в которой находится частица идеального газа. Например, левая камера – 0, правая – 1 (fig. 1).

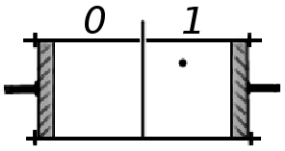

Fig. 1. Двигатель Сциларда.

Точно также, кубит может описывать, например, поляризацию фотона, орбиталь электрона в атоме водорода или любую другую подобную характеристику системы в квантовой физике. Электромагнитные волны являются

поперечными волнами. Это означает, что колебания происходят в плоскости, перпендикулярной линии их распространения. При этом колебания в выбранной системе координат могут быть, например, вертикальными или горизонтальными (это и называется поляризацией волны), и каждой из этих ситуаций мы можем присвоить обозначение – 0 и 1 (fig. 2) и, таким образом, поляризация будет кодировать для нас один бит информации. В атоме водорода, 0 мы можем присвоить первой, базовой орбитали, а 1 – второй, и, аналогичным образом, кодировать 1 бит информации состоянием атома.

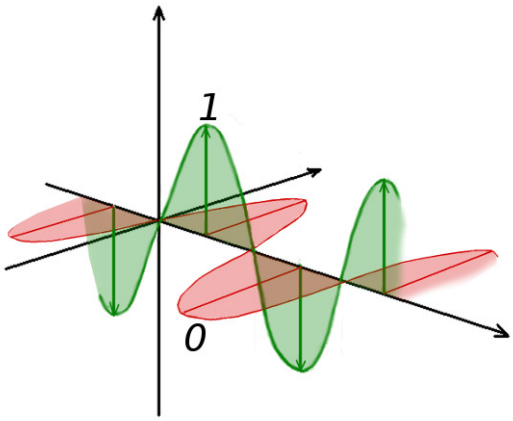

Fig. 2. Информация в квантовой системе.

Вы можете заметить (и будете совершенно правы), что поляризация фотона в выбранной системе координат может оказаться не только вертикальной или горизонтальной, но и вообще какой угодно. Так же как и атом водорода может находится в суперпозиции базового и возбужденного состояний. Это обстоятельство создает затруднения для построения классического компьютера на перечисленных базовых элементах, и именно оно является одним из преимуществ квантового компьютера.

Настало время дать строгое математическое определение термину "квантовый бит" или "кубит".
Кубит – это вектор единичной длинны в двумерном гильбертовом пространстве над полем комплексных чисел.

$$|\phi\rangle \in H, \quad \|\phi\| = 1, \quad \dim H = 2 \tag{1}$$

В гильбертовых пространствах определено скалярное произведение векторов:

$$|x\rangle = \begin{pmatrix} x_1 \\ x_2 \\ \cdots \\ x_n \end{pmatrix} \quad |y\rangle = \begin{pmatrix} y_1 \\ y_2 \\ \cdots \\ y_n \end{pmatrix}$$

$$\langle x|y\rangle = \sum_{i=1}^{n} x_i \cdot y_i^*$$

Скобки "$|\cdots\rangle$" для обозначения векторов были введены Полем Дираком и называются нотацией Дирака.

В пространстве со скалярным произведением можно определить понятие угла θ между векторами:

$$\begin{aligned} \cos\theta &= \frac{|\langle x|y\rangle|}{\|x\| \cdot \|y\|} \\ \theta &= \arccos \frac{|\langle x|y\rangle|}{\|x\| \cdot \|y\|}, \quad \theta \in [0, \frac{\pi}{2}] \end{aligned} \tag{2}$$

Поскольку мы имеем дело с комплексными числами, а комплексные косинусы нам не к чему, в выражении (2) мы берем модуль и, таким образом ограничиваем диапазон возможных углов. В евклидовом пространстве над вещественными числами модуль в этом выражении не стоит, и поэтому там возможны углы от 0 до π.

На протяжении всего курса мы будем иметь дело с единичными векторами (векторами единичной длины), поэтому нормы векторов из этого выражения можно убрать:

$$\begin{aligned} \cos\theta &= |\langle x|y\rangle| \\ \theta &= \arccos|\langle x|y\rangle| \end{aligned} \tag{3}$$

Получается, что косинус угла между двумя векторами равен модулю их скалярного произведения. Ортогональными векторами мы будем называть такие вектора, скалярное произведение которых равно 0.

$$|x\rangle \perp |y\rangle \Leftrightarrow \langle x|y\rangle = 0$$

Сонаправленными векторами мы будем называть такие вектора, скалярное произведение которых равно единице. Заметим, что в отличие от евклидового пространства, сонаправленные единичные вектора не обязаны быть идентичными. Например, единичные вектора

$$|x\rangle, \quad e^{i\phi}|x\rangle$$

$$|e^{i\phi}| \cdot |\langle x|x\rangle| = 1$$

сонаправлены, но, как мы видим, это разные вектора.

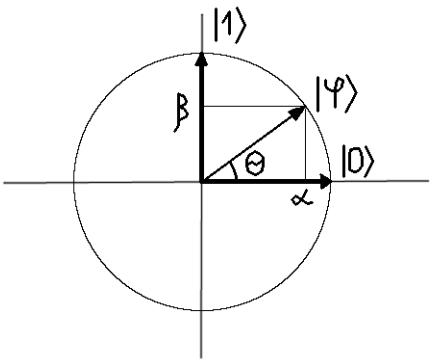

Fig. 3. Кубит.

Кубит – это единичный вектор в двумерном гильбертовом пространстве (fig. 3).

Каждая из осей на рисунке является проекцией комплексной плоскости на плоскость страницы. Вообще говоря, нарисовать две ортогональных комплексных плоскости без проекции нам не удалось бы даже на трехмерной бумаге. Окружность здесь представляет все вектора единичной длины в этом пространстве – все возможные значения одного кубита. Как видите, их намного больше, чем значений классического бита (которых всего два). Кубит может принимать любое из бесконечного множества значений. Так же как фотон (fig. 2) может быть поляризован не только вертикально или горизонтально, но, вообще говоря под любым углом. Получается, что простейшая квантовая система не ограничивается двумя состояниями.

На самом деле, классические системы (тот же двигатель Сциларда) тоже содержат огромное множество возможных состояний. Молекула газа в камерах двигателя Сциларда может находится во множестве разных точек, но наши особенности интерпретации (измерения) этой системы позволяют нам определить ее положение только с точностью до номера камеры.

В классических системах такое сокращение количества потенциально доступной информации называется "оцифровка". В квантовых системах есть похожий процесс, называемый "измерением" (measurement).

2 Измерение кубита

Выделим в пространстве системы ортонормированный базис (fig. 3). Выбор такого базиса, вообще говоря, произволен и определяется так называемой наблюдаемой, которая в свою очередь определяется процессом измерения. Вектора базиса назовем $|0\rangle$ и $|1\rangle$, по аналогии со значениями классического бита. Дело в том, что для получения информации о состоянии его нужно

измерить (совсем как с двигателем Сциларда!). А для измерения нужно выбрать базис (наблюдаемую). И после измерения квантовой системы в выбранном нами базисе мы получим не что иное, как один из векторов этого базиса.

Например, если система находится в состоянии $|0\rangle$, то при измерении ее в этом базисе мы получим результат $|0\rangle$. Если система находится в состоянии $|1\rangle$, мы получим результат $|1\rangle$. А для состояния $|\phi\rangle$:

$$\begin{aligned} |\phi\rangle &= \alpha\,|0\rangle + \beta\,|1\rangle \\ \alpha,\ \beta &\in \mathbb{C} \\ |\alpha|^2 + |\beta|^2 &= 1 \end{aligned} \tag{4}$$

мы получим вектор $|0\rangle$ с вероятностью $|\alpha|^2$, а вектор $|1\rangle$ – с вероятностью $|\beta|^2$.

$$\begin{aligned} P(|0\rangle) &= |\alpha|^2 \\ P(|1\rangle) &= |\beta|^2 \end{aligned} \tag{5}$$

Обратите внимание, что:

$$\begin{aligned} \alpha &= \langle\phi|0\rangle \\ |\alpha| &= \cos\theta \\ \beta &= \langle\phi|1\rangle \\ |\beta| &= \sin\theta \end{aligned} \tag{6}$$

Итак, при измерении квантовой системы несущей один кубит информации, мы:

1. Выбираем ортонормированный базис.
2. Проводим измерение и получаем один из векторов этого базиса с вероятностями, равными квадратам модулей скалярного произведения вектора системы на вектора базиса.
3. Из квантового бита мы получаем один классический бит информации – 0 или 1.
4. При измерении сама система переходит в тот вектор выбранного нами базиса, который мы получили в результате измерения.
5. Поэтому, повторное измерение всегда дает нам тот же результат, который мы получили при первом измерении.

Получается, что процесс измерения в некотором смысле аналогичен классическому процессу оцифровки – вместо континуума возможных состояний мы всегда получаем 1 бит.

Узнать коэффициенты α и β с помощью процесса измерения мы не можем. Повторное измерение той же самой системы мы провести так же

не можем, поскольку процесс измерения разрушает изначальное состояние. И, в добавок ко всему, мы не можем копировать неизвестные нам состояния, для того, чтобы провести серию измерений на копиях и оценить коэффициенты. Это нам запрещает **Теорема о запрете клонирования**, сформулированная Вуттерсом, Зуреком и Диэксом в 1982 году.

Таким образом, если мы хотим получить максимально достоверную информацию о состоянии системы, нам для ее измерения нужно выбирать базис, один из векторов которого очень близок (в идеале – совпадает) с измеряемым нами кубитом.

Допустим, например, мы знаем, что система находится в одном из следующих состояний:

$$\begin{aligned} |\phi\rangle &= \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \\ |\psi\rangle &= \frac{1}{\sqrt{2}}|1\rangle - \frac{1}{\sqrt{2}}|0\rangle \end{aligned} \tag{7}$$

Нам нужно узнать, какая из ситуаций имеет место на самом деле. В базисе $|0\rangle, |1\rangle$ измерять этот кубит бесполезно, поскольку при таком измерении мы получим $|0\rangle$ или $|1\rangle$ с одинаковыми вероятностями:

$$\begin{aligned} P(|0\rangle|\phi) = |\langle\phi|0\rangle|^2 = \frac{1}{2} = |\langle\psi|0\rangle|^2 = P(|0\rangle|\psi) \\ P(|1\rangle|\phi) = \frac{1}{2} = P(|1\rangle|\psi) \end{aligned} \tag{8}$$

Мы, правда, можем это сделать, если нам нужен абсолютно случайный бит информации. В остальных же случаях, если нам правда нужно что-то узнать о состоянии кубита, мы можем выбрать базис $|+\rangle, |-\rangle$:

$$\begin{aligned} |+\rangle &= \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \\ |-\rangle &= \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle, \end{aligned} \tag{9}$$

который называется базисом Адамара (англ. Hadamard).

Измерив систему в базисе Адамара мы получим достоверную информацию о состоянии кубита, потому что модуль его скалярного произведения на один из векторов этого базиса равен 1, что соответствует вероятности достоверного события.

$$\begin{aligned} P(|+\rangle|\phi) = |\langle\phi|+\rangle|^2 = 1 \\ P(|+\rangle|\psi) = |\langle\psi|+\rangle|^2 = 0 \end{aligned} \tag{10}$$

Проиллюстрируем процесс измерения на примере. Мы помним, что носителем информации может быть, например, поляризация фотонов – направление их колебаний. Предположим, что у нас есть фотон, или поток фотонов, поляризованный определенным образом, например – вертикально или горизонтально. Как мы можем узнать, какая из этих ситуаций имеет место на самом деле?

К нашему счастью, в природе существуют кристаллы, имеющие оптическую ось и пропускающие только свет, поляризованный определенным образом. На микроуровне эти кристаллы состоят из диполей, ориентированных по одной оси (fig. 4).

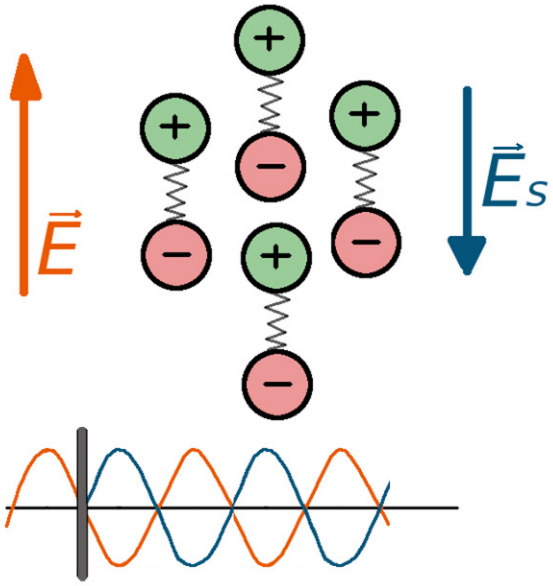

Fig. 4. Линейный поляризатор на молекулярном уровне.

Пружинка между полюсами диполя нарисована потому, что атомы в молекулах не скреплены гвоздями, а находятся в ямах потенциальной энергии кулоновского поля и, следовательно, могут отдаляться и приближаться при наличии внешнего поля. Пропускаемый через кристалл поляризованный вертикально свет, как раз, и создает это поле $\bar{E}$, причем поле переменное (синусоиду). Это поле приводит диполи в колебательное движение, и они, в свою очередь испускают вторичную волну $\bar{E}_s$, смещенную по фазе на π по отношению к падающей волне. Это вторичная волна складывается с прошедшей через кристалл и гасит ее. Зато горизонтально поляризованная

волна никак не влияет на диполи, не создает вторичной волны и, следовательно, легко проходит через кристалл (fig. 5).

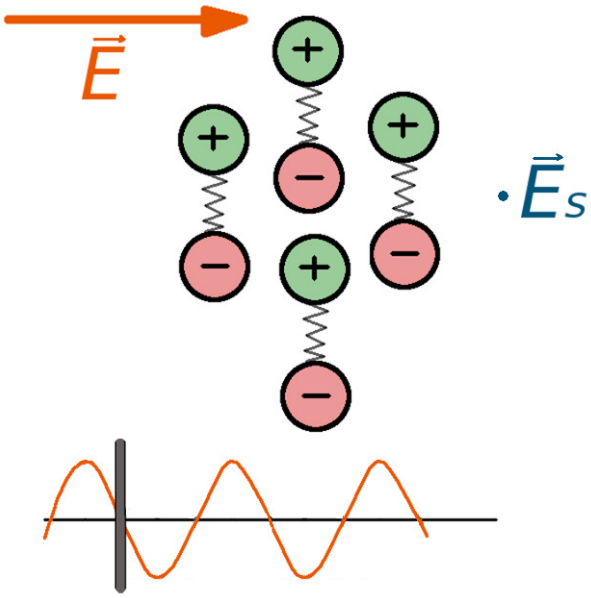

Fig. 5. Линейный поляризатор на молекулярном уровне.

С помощью пластинок из этих кристаллов, называемых линейными поляризаторами, мы можем получать поляризованный свет и измерять его поляризацию.

Обычный свет от лампочки не является поляризованным. Источниками поляризованного света могут быть, например, экраны LCD мониторов, покрытые пленками, имеющими оптическую ось. Частично поляризованным бывает свет, отраженный от некоторых материалов, например, от воды. Иногда фотографы, желая сфотографировать дно неглубокого водоема, используют подобные поляризационные фильтры для отсекания изображения, отраженного поверхностью воды. Так же поляризованный свет можно использовать для анализа дефектов (напряжений) в прозрачных материалах.

3 Система кубитов

В подавляющем большинстве случаев для вычислений нам требуется более одного бита. Система, состоящая из нескольких кубитов, описывается тензорным произведением составляющих ее систем. Поясним на примере.

Допустим, у нас есть два кубита (например, два поляризованных фотона, или два атома водорода, или два электрона с разными спинами). Распишем возможные варианты измерения этих кубитов в стандартном базисе:

qubit I	qubit II
$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$
$\|1\rangle$	$\|1\rangle$

Нам удобно и дальше считать состояние всей квантовой системы вектором в некотором гильбертовом пространстве. Поскольку возможных результатов измерения у нас теперь 4, то и количество базисных векторов равно четырем (и пространство четырехмерно). Обозначим базисные вектора этого пространства:

qubit I	qubit II	vector
$\|0\rangle$	$\|0\rangle$	$\|00\rangle$
$\|0\rangle$	$\|1\rangle$	$\|01\rangle$
$\|1\rangle$	$\|0\rangle$	$\|10\rangle$
$\|1\rangle$	$\|1\rangle$	$\|11\rangle$

Теперь представим, что до измерения один из кубитов находился в суперпозиции базовых состояний. Например, вот так:

qubit I	qubit II
$\|0\rangle$	$\alpha\|0\rangle + \beta\|1\rangle$

В нашем новом базисе мы можем записать это совокупное состояние следующим образом.

qubit I	qubit II	vector
$\|0\rangle$	$\alpha\|0\rangle + \beta\|1\rangle$	$\alpha\|00\rangle + \beta\|01\rangle$

Вероятность измерения:

$$\begin{aligned} P(|00\rangle) &= |\alpha|^2 \\ P(|01\rangle) &= |\beta|^2 \\ P(|10\rangle) = P(|11\rangle) &= 0 \end{aligned} \tag{11}$$

Вектор четырехмерный, длина его по-прежнему равна 1.

Полностью смешанное состояние:

qubit I	qubit II	vector
$\alpha\|0\rangle + \beta\|1\rangle$	$\gamma\|0\rangle + \delta\|1\rangle$	$\alpha\gamma\|00\rangle + \alpha\delta\|01\rangle + \beta\gamma\|10\rangle + \beta\delta\|11\rangle$

Легко показать, что сумма квадратов коэффициентов по-прежнему равна 1.

$$|\alpha\gamma|^2 + |\alpha\delta|^2 + |\beta\gamma|^2 + |\beta\delta|^2 = 1$$

Вообще говоря, любой вектор единичной длины в пространстве H^{2^n} представляет какое-то реально возможное состояние системы из n кубитов.

Нам нужно договориться, как мы будем представлять вектора в H^{2^n} в виде столбцов (т.е. как мы их перенумеруем).

Для одного кубита мы нарисовали векторы базиса на картинке (fig. 3):

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \quad |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$$

Для двух (и более) кубитов мы определим вектор столбец описывающей их системы через тензорное (кронекерово) произведение векторов отдельных кубитов:

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\cdot\begin{pmatrix}1\\0\end{pmatrix}\\0\cdot\begin{pmatrix}1\\0\end{pmatrix}\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}$$

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}1\cdot\begin{pmatrix}0\\1\end{pmatrix}\\0\cdot\begin{pmatrix}0\\1\end{pmatrix}\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\cdot\begin{pmatrix}1\\0\end{pmatrix}\\1\cdot\begin{pmatrix}1\\0\end{pmatrix}\end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}$$

$$|11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\cdot\begin{pmatrix}0\\1\end{pmatrix}\\1\cdot\begin{pmatrix}0\\1\end{pmatrix}\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

Такой способ определения столбцов в получившемся пространстве не является единственным. Мы могли перенумеровать вектора как угодно иначе, но кронекерово произведение дает нам естественную и удобную для дальнейшей работы нумерацию.

Таким образом, система из трех кубитов описывается вектором в восьмимерном пространстве, а размерность пространства системы из десяти кубитов – 1024. Для тысячи кубитов мы получаем пространство, размерность которого описывается числом с 300 нулями.

Построив компьютер на всего лишь 1000 атомов мы получаем в свое распоряжение "монстра", состояние которого описывается 10^{30} комплексными числами. А это гораздо больше, чем элементарных частиц в наблюдаемой вселенной! Понятно, откуда у Фейнмана был оптимизм относительно перспектив квантовых вычислений!

Представим себе кубиты в виде подброшенных в воздух монеток. Пока монетки вращаются в воздухе, они как бы находятся в суперпозиции состояний Орел – Решка. Падая на пол, монетка проходит через процесс измерения в базисе орла и решки. Для одной подброшенной монетки мы имеем два возможных исхода, для двух – 4, для трех – 8, а для десяти одновременно подброшенных монеток – уже 1024 возможных исхода их измерения!

Пришло время узнать, почему на подброшенных монетах нельзя построить квантовый компьютер.

4 Измерение системы кубитов

Удивительнее и интереснее всего то, что не любое состояние вида

$$\begin{aligned} \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle \\ |\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1 \end{aligned} \tag{12}$$

раскладывается на тензорное произведение отдельных кубитов. Например, каждое из состояний Белла:

$$\begin{aligned} \alpha\,|00\rangle + \beta\,|11\rangle \\ \alpha\,|01\rangle + \beta\,|10\rangle \\ |\alpha|^2 + |\beta|^2 = 1 \end{aligned} \tag{13}$$

описывает реальную систему, которую можно построить, например, на двух фотонах. Разложить эти состояния на тензорное произведение двух кубитов нельзя. Получается, что частицы, на которых хранятся кубиты, как бы "запутанны". Состояния такого вида (которые нельзя разложить на тензорное произведение отдельных кубитов) так и называются – запутанными (англ. entangled). Именно такие состояния нам не удастся реализовать в виде подброшенных в воздух монеток.

Запутанные состояния очень не нравились Альберту Энштейну, и вот по какой причине. Дело в том, что систему, состоящую из нескольких кубитов можно измерять не только целиком, но и по частям (измерять отдельные кубиты). При измерении состояния (12) целиком мы получаем один из четырех базисных векторов с вероятностью, равной квадрату модуля коэффициента при нем. Но физически система располагается на двух разных

частицах, и, поэтому, никто нам не мешает подвергнуть измерению одну из них, а вторую не трогать.

При этом, если, например, при измерении первого кубита мы получим вектор $|0\rangle$, то из указанной суммы уходят все слагаемые с единицей на первом месте, а оставшиеся члены нужно домножить на нормализующий коэффициент, чтобы длина вектора была равна 1:

$$|0\rangle \left(\frac{\alpha |0\rangle}{\sqrt{|\alpha|^2 + |\beta|^2}} + \frac{\beta |1\rangle}{\sqrt{|\alpha|^2 + |\beta|^2}} \right)$$

В результате измерения первого кубита состояние второго кубита не изменилось. При измерении запутанного состояния, например, любого из состояний Белла, измерение первого кубита автоматически приводит к измерению второго. Мгновенно!

Даже если запутанные частицы разнесены друг от друга на много световых лет, измерение одной из них мгновенно определяет состояние второй. Энштейн называл этот феномен «жутким дальнодействием».

Однако, с точки зрения многомировой интерпретации, такая ситуация совсем не выглядит магической. Для незапутанного состояния из двух кубитов в мультивселенной присутствуют почти полностью идентичные варианты вселенной, отличающиеся только состоянием интересующих нас частиц.

$\|00\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$

При этом относительная доля вселенных для каждого конкретного состояния (относительная площадь каждого квадрата на диаграмме) соответствует квадрату коэффициента при этом состоянии в суперпозиции (12). До момента измерения экземпляры наблюдателя во всех четырех типах вселенных идентичны друг другу. Но после измерения первого кубита часть экземпляров наблюдателя "запутывается" с верхней строчкой таблицы (те, что получили $|0\rangle$), а вторая часть – с нижней строкой (получившие в результате измерения $|1\rangle$). Измерив один кубит мы сужаем доступный нам набор вселенных.

Для состояния Белла диаграмма выглядит несколько иначе:

$\|00\rangle$	$\|11\rangle$

Вариантов вселенных, в которых мы можем находиться, всего два, и измерение любого из кубитов достоверно указывает нам, где мы на этой картинке.

Таким образом, измерение изменяет не частицы, несущие кубиты, а разделяет ранее идентичные экземпляры наблюдателей.

5 Эволюция квантовой системы

Эволюция квантовой системы унитарна. Это значит, что любое изменение ее состояния выражается действием унитарного оператора. Поскольку изменение состояния и есть вычисление, то и "программа" для квантового компьютера представляет собой последовательное применение к вектору состояния различных унитарных операторов.

Оператор U унитарен, если его сопряженный оператор совпадает с обратным:

$$UU^* = U^*U = I$$

Матрица сопряженного оператора представляет собой транспонированную матрицу исходного оператора, все числа в которой заменены на сопряженные.

Необходимым и достаточным условием унитарности оператора является сохранение им при отображении длин векторов и углов между ними:

$$\begin{aligned} \forall \phi \in H \qquad & \| U\,|\phi\rangle \,\| = \| \,|\phi\rangle \,\| \\ \forall \phi, \psi \in H \qquad & |\,\langle\, U\,|\phi\rangle \;|\; U\,|\psi\rangle \,\rangle\,| = |\,\langle \phi|\psi\rangle\,| \end{aligned} \tag{14}$$

Приведем несколько примеров.

Оператор Адамара.

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Проверим его унитарность:

$$H^* = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = H$$

$$H^*H = HH = \left(\frac{1}{\sqrt{2}}\right)^2 \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = I$$

Применим оператор Адамара к состояниям $|0\rangle$ и $|1\rangle$:

$$H\,|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = |+\rangle$$

$$H\,|1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = |-\rangle$$

Мы видим, что из стандартного базиса $|0\rangle - |1\rangle$ оператор Адамара делает базис Адамара. Поскольку H является самосопряженным, и, следовательно обратным к себе самому, то его повторное применение у базису Адамара вернет нам обычный базис.

Гейт X.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Проверим его унитарность:

$$X^* = X$$

$$XX = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = I$$

Применим оператор X к состояниям $|0\rangle$ и $|1\rangle$:

$$X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

$$X|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

Мы видим, что гейт X – это квантовый аналог классического гейта NOT.

Гейт CNOT.

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Этот гейт уже для системы из двух кубитов, поскольку предназначен для четырехмерного пространства. Унитарность мы проверим, воспользовавшись упомянутым ранее признаком. Посмотрим на образ базиса после применения этого гейта:

$$CNOT|00\rangle = |00\rangle$$
$$CNOT|01\rangle = |01\rangle$$
$$CNOT|10\rangle = |11\rangle$$
$$CNOT|11\rangle = |10\rangle$$

Мы видим, что это перестановка изначального базиса. Гейт действует как условный NOT. Если первый (старший) кубит равен единице, то ко второму применяется гейт NOT. Если же первый кубит – ноль, то ко второму не применяется ничего (применяется тождественный оператор).

Поскольку образом ортонормированного базиса оказался ортонормированный базис, это значит, что длины векторов и углы между ними оператор сохраняет, а значит он унитарен.

Далее мы будем пользоваться диаграммами следующего вида.

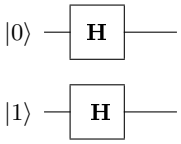

Fig. 6. Схема квантового алгоритма.

Горизонтальные линии будут обозначать кубиты (старший вверху), и на этих линиях мы будем слева направо размещать операторы в порядке их применения. Например, на (fig. 6) изображено применение оператора Адамара сразу к двум кубитам, старший из которых был в состоянии $|0\rangle$, а младший – в состоянии $|1\rangle$.

Вектор системы в этом примере четырехмерен (поскольку у нас два кубита), а значит и матрица такого преобразования должна быть 4×4. Как она будет выглядеть? Очень просто – двухкубитный оператор Адамара представляет собой тензорное произведение однокубитных:

$$H_2 = H \otimes H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} H & H \\ H & -H \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Легко доказать (сделайте это в качестве упражнения), что в общем случае верно тождество:

$$A|x\rangle \otimes B|y\rangle = (A \otimes B)|xy\rangle . \tag{15}$$

Представим теперь, что у нас есть система из двух кубитов, и мы хотим применить оператор Адамара только ко второму из них:

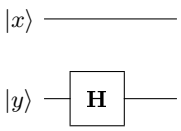

Fig. 7. H на одном кубите.

Как будет выглядеть матрица такого оператора?

Так как с первым кубитом ничего не происходит, это равносильно применению к нему тождественного оператора. Поэтому матрица такого оператора представляет собой тензорное произведение I на H.

$$I \otimes H = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} H & 0 \\ 0 & H \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

Для обратной ситуации:

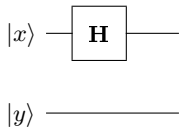

Fig. 8. H на одном кубите.

Матрица будет выглядеть так:

$$H \otimes I = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} I & I \\ I & -I \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$$

Оператор CNOT мы будем обозначать на схеме вот так:

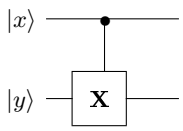

Fig. 9. Оператор CNOT.

Кубит $|x\rangle$ – контрольный, $|y\rangle$ – контролируемый.

Рассмотрим оператор CNOT в трехкубитной системе (fig. 10).

Матрица оператора должна иметь размер 8×8. Такой оператор будет выглядеть как тензорное произведение I на CNOT:

$$I \otimes CNOT = \begin{pmatrix} CNOT & 0 \\ 0 & CNOT \end{pmatrix}$$

А как быть, если контрольный бит у нас первый, а контролируемый – 3-й (fig. 11)?

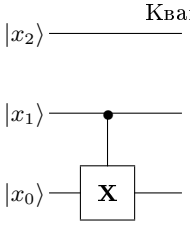

Fig. 10. Оператор CNOT. 3 кубита.

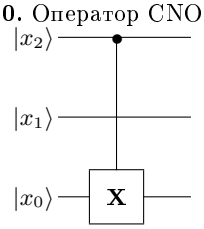

Fig. 11. Оператор CNOT. 3 кубита.

Если бы мы могли разложить оператор CNOT на тензорное произведение двух матриц, скажем A и B, то формула для такого CNOT выглядела бы так:

$$A \otimes I \otimes B \tag{16}$$

Дело в том, что оператор CNOT нельзя разложить на тензорное произведение двух матриц 2 на 2. Он является в некотором смысле аналогом запутанного состояния, которое мы не можем разложить на тензорное произведение двух состояний. Это запутывающий оператор, и с помощью подобных операторов мы будем получать запутанные состояния. Но как же нам получить его матрицу для нашего примера? Она ведь тоже не будет являться произведением вида (16). Таких операторов A и B просто не существует.

Легко показать, что воздействие оператора на базисный вектор с номером k (такой, у которого в векторе-столбце единственная единица стоит на месте k) дает нам в результате столбец оператора с номером k.

$$Ae_k = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1k} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2k} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nk} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ \cdots \\ 1 \\ \cdots \\ 0 \end{pmatrix} = \begin{pmatrix} a_{1k} \\ a_{2k} \\ \cdots \\ a_{nk} \end{pmatrix}$$

Поэтому, зная, какой образ для какого из базисных векторов мы хотим получить, мы можем найти полный вид оператора (fig. 11):

$$
\begin{aligned}
|000\rangle &\to |000\rangle \\
|001\rangle &\to |001\rangle \\
|010\rangle &\to |010\rangle \\
|011\rangle &\to |011\rangle \\
|100\rangle &\to |101\rangle \\
|101\rangle &\to |100\rangle \\
|110\rangle &\to |111\rangle \\
|111\rangle &\to |110\rangle
\end{aligned}
\tag{17}
$$

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

6 Оператор Адамара

Напоследок мы докажем полезное выражение для оператора Адамара для системы из n кубитов. Оно нам многократно пригодится далее:

$$
\begin{gathered}
H_n |x\rangle = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} (-1)^{x \bullet y} |y\rangle \\
x \bullet y = x_0 y_0 \oplus x_1 y_1 \oplus \cdots \oplus x_{n-1} y_{n-1}
\end{gathered}
\tag{18}
$$

Доказательство по индукции.

База:

$$
H_1 |x\rangle = \frac{1}{2^{1/2}} (|0\rangle + (-1)^x |1\rangle) = \frac{1}{2^{1/2}} \sum_{y=0}^{1} (-1)^{x \bullet y} |y\rangle
$$

Индукционный переход:

$$
H_n |x\rangle = \frac{1}{2^{n/2}} (|0\rangle + (-1)^{x_{n-1}} |1\rangle) \otimes \cdots \otimes (|0\rangle + (-1)^{x_0} |1\rangle) =
$$

Раскроем первую скобку:

$$
= \frac{1}{\sqrt{2}} |0\rangle \otimes \frac{1}{2^{\frac{n-1}{2}}} (|0\rangle + (-1)^{x_{n-2}} |1\rangle) \otimes \cdots \otimes (|0\rangle + (-1)^{x_0} |1\rangle) +
$$

$$+\frac{1}{\sqrt{2}}(-1)^{x_{n-1}}|1\rangle \otimes \frac{1}{2^{\frac{n-1}{2}}}(|0\rangle + (-1)^{x_{n-2}}|1\rangle) \otimes \cdots \otimes (|0\rangle + (-1)^{x_0}|1\rangle) =$$

Воспользуемся индукционным предположением:

$$= \frac{1}{\sqrt{2}}|0\rangle \otimes H_{n-1}|x_{n-2}\cdots x_0\rangle + \frac{1}{\sqrt{2}}(-1)^{x_{n-1}}|1\rangle \otimes H_{n-1}|x_{n-2}\cdots x_0\rangle =$$

$$= \frac{1}{2^{n/2}}\Bigg(|0\rangle \otimes \sum_{y=0}^{2^{n-1}-1}(-1)^{x_0y_0\oplus x_1y_1\oplus\cdots\oplus x_{n-2}y_{n-2}}|y\rangle +$$

$$+(-1)^{x_{n-1}}|1\rangle \otimes \sum_{y=0}^{2^{n-1}-1}(-1)^{x_0y_0\oplus x_1y_1\oplus\cdots\oplus x_{n-2}y_{n-2}}|y\rangle\Bigg) =$$

$$= \frac{1}{2^{n/2}}\Bigg(\sum_{y=0}^{2^{n-1}-1}(-1)^{x_0y_0\oplus x_1y_1\oplus\cdots\oplus x_{n-2}y_{n-2}\oplus x_{n-1}\cdot 0}|0\rangle|y\rangle +$$

$$+\sum_{y=0}^{2^{n-1}-1}(-1)^{x_0y_0\oplus x_1y_1\oplus\cdots\oplus x_{n-2}y_{n-2}\oplus x_{n-1}\cdot 1}|1\rangle|y\rangle\Bigg) =$$

$$= \frac{1}{2^{n/2}}\sum_{y=0}^{2^n-1}(-1)^{x\bullet y}|y\rangle$$

7 Дополнительные материалы

1. **Deutsch, David. "Quantum theory, the Church-Turing principle and the universal quantum computer".** Proceedings of the Royal Society A. 400 (1818) (July 1985): 97–117.
2. **John Preskill. Lecture notes for "Physics 219/Computer Science 219. Quantum Computation" (Formerly Physics 229)** http://www.theory.caltech.edu/people/preskill/ph229/index.html
3. **Симулятор квантового компьютера.** http://qc-sim.appspot.com