ГОСУДАРСТВЕННЫЙ НАУЧНЫЙ ЦЕНТР РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНСТИТУТ ФИЗИКИ ВЫСОКИХ ЭНЕРГИЙ

ИФВЭ 2001-12
ОАФ

И.А. Качаев

КВАНТОВЫЕ ВЫЧИСЛЕНИЯ

Протвино 2001

УДК 530.145+621.142 М–24

Аннотация

Качаев И.А. Квантовые вычисления: Препринт ИФВЭ 2001-12. – Протвино, 2001. – 24 с., 1 рис., библиогр.: 30.

Данная статья представляет собой обзор работ по квантовым вычислениям и квантовой теории информации. Может служить введением в предмет.

Abstract

Kachaev I.A. Quantum Computations: IHEP Preprint 2001-12. – Protvino, 2001. – p. 24, figs. 1, refs.: 30.

This article presents a review of works in a field of quantum computing and quantum theory of information and can serve as an introduction to the subject.

Содержание

1. Введение. Зачем это нужно

"Because nature isn't classical, dammit..."
Richard P. Feynman

Квантовая теория информации — очень молодая область науки, возникшая в 80-х годах XX века на стыке классической теории информации, теории вычислений и нерелятивистской квантовой механики. Возможно, одна из причин ее возникновения — то обстоятельство, что с уменьшением размеров электронных приборов влияние квантовомеханических эффектов на их работу становится существенным и с этим влиянием надо как-то бороться либо попытаться обратить его на пользу. Однако гораздо более важным фактором является принципиальная ограниченность возможностей классических компьютеров при решении определенных классов задач. Использование компьютера, работающего на основе принципов квантовой механики, обещает в этих случаях *экспоненциальное* по объему задачи ускорение работы.

Вся история квантовой теории информации к настоящему моменту укладывается в 15–20 лет. Одной из первых работ данного направления (1982 г.) является [1], в которой Р. Фейнман предложил использовать для моделирования эволюции квантовомеханической системы контролируемую эволюцию другой, "стандартной", квантовомеханической системы. Отсюда было уже недалеко до идеи универсального вычислительного устройства на основе квантовой эволюции физической системы [4] и вообще компьютера как устройства, реализующего определенный набор математических аксиом на основе определенного набора физических законов [3]. В результате оказалось, что вычислительная сложность алгоритма может зависеть от того, на основе какой физической аксиоматики он строится. А когда в 1994 г. П. Шор построил первый практически полезный квантовый алгоритм [22], да еще затрагивающий сферу криптографии, прогресс в области квантовой теории информации стал неизбежен... Обнаружение же таких эффектов, как квантовая телепортация (1993 г.) и квантовая коррекция ошибок (1996 г.), может пролить новый свет и на основания самой квантовой механики.

Практически вся информация, изложенная в этом обзоре, почерпнута в сети Internet, которая является сейчас, по-видимому, наиболее полным источником информации по данному вопросу. Соответственно в ссылках зачастую указаны адреса в сети Internet, по которым эти материалы можно получить. Поиск материалов по данной теме можно начать по адресам [5] и [6]. Обсуждение близких вопросов, связанных с основаниями и историей квантовой механики, можно найти в [7]. Мы в основном следуем работам [8,9]. В последнее время (2000 г.) появились русскоязычные сетевые источники [10] и [11].

2. Основы квантовой теории информации

2.1. Принципы квантовой механики

Основой для построения схемы квантовых вычислений является нерелятивистская квантовая механика в классической вероятностной интерпретации, никаких дополнительных постулатов не вводится. Достаточно рассматривать системы с конечным числом степеней свободы. Соответствующие постулаты (принципы) нерелятивистской квантовой механики можно сформулировать следующим образом:

1. Состояние изолированной системы представляется зависящим от времени вектором $|\psi(t)\rangle$ в некотором гильбертовом пространстве. Если система имеет конечное число степеней свободы, это пространство будет конечномерным векторным пространством над полем комплексных чисел, а физические состояния системы будут представлены нормированными векторами в этом пространстве с условием нормировки $\langle\psi|\psi\rangle = 1$. Физический смысл такого описания состоит в том, что квантовая механика является линейной теорией: если система может находиться в двух различных состояниях $|a\rangle$ и $|b\rangle$, то она может находиться и в произвольной линейной комбинации этих состояний $c_1|a\rangle + c_2|b\rangle$ с комплексными коэффициентами c_1, c_2 и условием нормировки $|c_1|^2 + |c_2|^2 = 1$.
2. Физические величины (наблюдаемые) представляются операторами в соответствующем пространстве, а для системы с конечным числом степеней свободы соответственно матрицами конечного размера в выбранном базисе.
3. Вектор состояния эволюционирует со временем в соответствии с линейным дифференциальным уравнением Шредингера:

$$i\hbar\frac{d}{dt}|\psi(t)\rangle = \mathcal{H}|\psi(t)\rangle,$$

где $\mathcal{H}$ есть (эрмитов) оператор Гамильтона для данной системы. Вследствие этого эволюция вектора состояния за конечное время определяется уравнением

$$|\psi(t)\rangle = U(t)|\psi(0)\rangle\,, \quad \text{где } U(t) = \exp\left(-\frac{i}{\hbar}\int \mathcal{H}\,dt\right)$$

есть некоторый определяемый гамильтонианом оператор эволюции. Эрмитовость оператора Гамильтона приводит к тому, что оператор эволюции является унитарным, $U^+U = UU^+ = 1$. Это гарантирует сохранение нормы вектора состояния и существование обратного оператора $U^{-1} = U^+$, т.е. возможность по конечному состоянию восстановить начальное: $|\psi(0)\rangle = U^+|\psi(t)\rangle$. Таким образом, эволюция изолированной системы является унитарной и обратимой.
4. Постулат измерения. Существуют взаимодействия, называемые *наблюдениями* или *измерениями,* при которых квантовомеханическая система перестает быть изолированной и вступает во взаимодействие с макроскопической (классической) системой, называемой *измерительным прибором,* у которой существует несколько (скажем, k) различимых состояний. В результате такого взаимодействия прибор переходит *случайным образом* в одно из возможных состояний с номером $i = 1 \ldots k$, а система переходит в соответствующее *собственное состояние* $|\psi_i\rangle$. Вероятность перехода в данное состояние P_i зависит только от конструкции прибора (т.е. измеряемой величины) и состояния системы $|\psi\rangle$ в момент измерения. Исходное состояние системы необратимо разрушается, единственной информацией, которую удается измерить, является (случайный) номер состояния, в которое перешел прибор (и, соответственно, система).

   Математически формализовать этот постулат можно следующим образом. Пусть состояние системы описывается вектором состояния в некотором гильбертовом пространстве H. *Наблюдаемой* $\mathcal{O}$ называется любой набор подпространств $E_1, E_2 \ldots E_k \subseteq H$, которые полностью подразделяют H и не перекрываются:

$$E_1 \times E_2 \times \cdots \times E_k = H, \quad E_i \perp E_j \quad \textit{для} \quad i, j = 1 \ldots k, \quad i \neq j.$$

Любой вектор состояния $|\psi\rangle$ может быть представлен как линейная комбинация (суперпозиция) компонент, лежащих в каждом из пространств E_i:

$$|\psi\rangle = \sum_{i=1}^{k} \alpha_i |\psi_{E_i}\rangle,$$

где α_i есть произвольные комплексные коэффициенты с условием нормировки $\sum_{i=1}^{k} |\alpha_i|^2 = 1$. Тогда результат наблюдения вектора состояния $|\psi\rangle$ посредством наблюдаемой $\mathcal{O}$ будет следующим:

а) будет случайно выбрано одно из E_i с вероятностью $|\alpha_i|^2$;
б) исходный вектор состояния $|\psi\rangle$ превратится ("коллапсирует") в $|\psi_{E_i}\rangle$ (нормированный);
в) единственной полученной информацией является номер выбранного подпространства i.

Отсюда следует, что при повторном измерении мы всегда получим в точности тот же результат, поскольку вектор состояния уже лежит в E_i.
Таким образом, операция измерения также преобразует квантовомеханическую систему, однако оператор преобразования (обычно называемый *проектором*) не является ни унитарным, ни обратимым.

Разумеется, описанная схема имеет свои ограничения. Во-первых, она работает только с чистыми состояниями и полностью игнорирует формализм матрицы плотности. Там, где необходим выход за пределы формализма чистых состояний, подробности мы просто опускаем. Постулат измерения сформулирован для достаточно частного случая систем с дискретным спектром. Релятивистские аспекты квантовой механики игнорируются, в частности, вопрос о симметрии волновой функции системы тождественных частиц нигде не обсуждается. Подразумевается, что мы работаем с дискретными степенями свободы и задачу симметризации полной волновой функции всегда можно возложить на ее координатную часть. Однако эта схема вполне достаточна для выполнения нашей задачи — описания основных идей квантовой теории информации.

2.2. Квантовые биты

Как известно, в классических компьютерах единицей хранения информации является бит — система, имеющая два состояния, называемые обычно 0 и 1. По аналогии мы можем определить *квантовый бит,* или сокращенно q-бит, как квантовомеханическую систему, имеющую два состояния, обозначаемых соответственно как $|0\rangle$ и $|1\rangle$. Однако в отличие от классического случая в квантовой механике эти два состояния могут интерферировать между собой, так что наиболее общее состояние квантового бита может быть записано как

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

где α, β есть комплексные числа и выполнено условие нормировки $|\alpha|^2 + |\beta|^2 = 1$. Это равенство, записанное в традиционной для квантовой механики нотации "состояний", введенной Дираком, можно переписать в обозначениях матричной алгебры, поскольку наши векторы состояний образуют по построению двумерное пространство:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad |\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

Физические реализации подобной системы с двумя состояниями могут быть разнообразными: электрон или ядро со спином $1/2$, ориентированным по или против направления магнитного поля; атом с двумя различными энергетическими состояниями; фотон с горизонтальной или вертикальной поляризацией и т.п. Поскольку квантовый бит может находиться в состоянии любой из (несчетного) множества возможных суперпозиций, на первый взгляд кажется, что мы можем упаковать неограниченное количество классической информации в состояние одного квантового бита. Однако это не так.

Во-первых, при "изготовлении" суперпозиции мы фактически имеем дело не с дискретными, а с непрерывными величинами, и именно точность процедуры приготовления заданного состояния определяет количество записываемой информации. Аналогично в классической электронике мы можем хранить информацию не в виде логических уровней, а в виде произвольного напряжения на электрическом элементе. Точность задания, поддержания и измерения этого напряжения определяет количество хранимой информации.

Во-вторых, в квантовом случае то, что записано, попросту не удастся прочесть. Действительно, размерность пространства состояний нашей системы равна двум, и в соответствии с постулатом измерения мы можем сконструировать наблюдаемую величину не более чем с двумя состояниями (в пространство размерности N невозможно вложить более чем N ортогональных подпространств) и получить в результате измерения два варианта ответа, в общем случае даже не наверняка, а с определенной вероятностью. Таким образом, в случае одного квантового бита никакого выигрыша по сравнению с классическим случаем не получается.

Естественной наблюдаемой для одного квантового бита может служить $\mathcal{B} = \{E_0, E_1\}$, где E_0 и E_1 есть подпространства, натянутые на базисные векторы $|0\rangle$, $|1\rangle$. Примером другой наблюдаемой может служить $\mathcal{O} = \{E_{0'}, E_{1'}\}$, где $E_{0'}, E_{1'}$ задаются векторами

$$|0'\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \text{ и } |1'\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Если физически состояние нашего q-бита закодировано в виде вертикальной или горизонтальной поляризации фотона, наблюдаемая $\mathcal{O}$ будет соответствовать измерению поляризации фотона в проекции на оси, повернутые на 45° градусов к вертикали. Если состояния $|0\rangle$,$|1\rangle$ реализованы в виде состояний электрона с определенной проекцией спина на ось Z, наблюдаемая $\mathcal{O}$ будет измерять проекцию спина на ортогональную оси Z ось X или Y.

В классическом случае вычислительная система из одного бита может выполнять преобразования $\{0,1\} \to \{0,1\}$. Легко проверить, что таких преобразований всего четыре: тождественное, инверсия (операция *не*), установка бита в 0, установка в 1. В квантовом случае репертуар преобразований одного бита гораздо богаче и представляет собой пространство унитарных матриц 2×2. Несложно выписать квантовые аналоги классических преобразований:

$$\mathrm{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathrm{Not} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \mathrm{Set0} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \quad \mathrm{Set1} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}.$$

Однако операции установки бита в определенное состояние необратимы (предыдущее состояние теряется), а потому соответствующие операторы неунитарны и не могут быть операторами эволюции. Эти действия можно выполнить только классическими средствами. Оператор *Not* совпадает с матрицей Паули σ_x. Его, а также и все остальные

операторы группы $SU(2)$ можно физически реализовать методами ядерного магнитного резонанса, т.е. контролируемой эволюции системы со спином $1/2$ в комбинации постоянного и переменного магнитных полей [12]. В частности, оператор *Not* есть просто оператор переворота спина на 180°. Правда, при этом на самом деле реализуется преобразование $|1\rangle \to |0\rangle$, $|0\rangle \to -|1\rangle$, но нежелательный фазовый фактор тоже можно исправить. Упомянем еще оператор поворота спина на 90° A и оператор Адамара H, который часто возникает в вычислениях:

$$A = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

В качестве курьеза можно упомянуть "квадратный корень из *не*", оператор, двукратное применение которого и в самом деле дает оператор инверсии:

$$\sqrt{Not} = \frac{1}{4} \begin{pmatrix} 1-i & 1+i \\ 1+i & 1-i \end{pmatrix}.$$

Физически это все тот же оператор поворота спина на 90° с дополнительным фазовым сдвигом компонент.

2.3. Квантовые регистры. Entanglement

Очевидно, что для практических вычислений необходимо более одного бита. Назовем *квантовым регистром* упорядоченный набор из конечного числа, скажем n, квантовых битов. Биты в регистре могут быть как изолированы, так и взаимодействовать друг с другом в соответствии с требуемым законом эволюции. Естественно обозначать базисные состояния квантового регистра соответствующими упорядоченными строками из нулей и единиц, так что у регистра из двух битов базисные состояния будут $|00\rangle$,$|01\rangle$,$|10\rangle$, $|11\rangle$. Число базисных состояний у регистра из n битов составляет 2^n, в точности как и общее число состояний классического битового регистра той же длины. Наиболее общим вектором состояния n-битового квантового регистра является

$$|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle,$$

где в обозначении базисных векторов $|i\rangle$ под i подразумевается двоичная запись этого числа.

Если два q-бита, составляющие квантовый регистр, находятся в определенных состояниях $|\varphi_1\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ и $|\varphi_2\rangle = \beta_0|0\rangle + \beta_1|1\rangle$, то состояние квантового регистра является тензорным произведением $|\varphi_1\rangle$ и $|\varphi_2\rangle$:

$$|\psi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle = \left(\sum_{i=0}^{1} \alpha_i |i\rangle\right) \bigotimes \left(\sum_{j=0}^{1} \beta_j |j\rangle\right) = \sum_{i,j=0}^{1} \alpha_i \beta_j |ij\rangle. \tag{1}$$

Аналогично если A и B есть унитарные преобразования, действующие независимо на $|\varphi_1\rangle$ и $|\varphi_2\rangle$, их совместное действие на $|\psi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle$ будет определяться 4×4-матрицей прямого произведения

$$C = A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B \\ a_{21}B & a_2 B \end{pmatrix} \quad \text{как} \quad (A \otimes B)\left(|\varphi_1\rangle \otimes |\varphi_2\rangle\right) = \left(A|\varphi_1\rangle\right) \otimes \left(B|\varphi_2\rangle\right).$$

Однако основной смысл объединения квантовых битов в квантовый регистр состоит в том, чтобы позволить им быть взаимозависимыми. Фундаментальное свойство квантовомеханических систем состоит в том, что их состояние не обязано сводиться к определенным состояниям подсистем. Далеко не любые состояния двухбитового квантового регистра могут быть выражены как прямые произведения состояний отдельных битов. Примером такого состояния может служить

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle\right).$$

При измерении такого состояния в стандартном базисе результаты $|00\rangle$ и $|11\rangle$ будут наблюдаться с вероятностью 50%, а результаты $|01\rangle$ и $|10\rangle$ не будут наблюдаться никогда. Прямой проверкой можно убедиться, что не существует таких α_i, β_i, при которых выполняется уравнение (1) (уравнения на $\alpha_i\beta_j$ противоречивы). Таким образом, регистр как целое находится в определенном квантовомеханическом состоянии, в то время как его подсистемы в определенных состояниях не находятся, иначе бы уравнение 1 выполнялось. Такое "скрученное", взаимозависимое состояние системы в англоязычных статьях описывается термином *entanglement,* к сожалению, адекватный русский перевод автору неизвестен. Состояния подсистем в подобном случае следует описывать на более общем языке матрицы плотности, однако нам для дальнейшего изложения это не понадобится.

2.4. Квантовые схемы

Как мы знаем, эволюция квантовой системы описывается унитарными операторами. Однако для системы из n квантовых бит операторы общего вида представляют собой $2^n \times 2^n$-матрицы, и мыслить подобными объектами для человека непривычно. Гораздо естественнее представлять себе эволюцию системы в виде набора последовательных преобразований сравнительно простого вида, каждое из которых затрагивает сравнительно немного, 2–3 отдельных бита. В результате эволюция квантовой системы представляется аналогичной работе обыкновенной логической схемы. Соответствующие частные преобразования называют обычно квантовыми логическими элементами (quantum gates), а всю схему эволюции в целом — квантовой схемой. Основной особенностью квантовых логических элементов по сравнению с классическими является то, что они обязаны быть унитарными, а следовательно — обратимыми.

Простейшими классическими логическими элементами являются *И, ИЛИ, ИСКЛЮЧАЮЩЕЕ ИЛИ (AND, OR, XOR).* Все они отображают два входных бита в один бит результата и потому никак не могут быть обратимыми, а следовательно — не могут быть реализованы квантовомеханически. Проще всего поправить положение для функции XOR — как известно, она обратима в том смысле, что по ее результату и одному из входных параметров можно восстановить второй: если $c = a \oplus b$, то $b = a \oplus c$ и $a = b \oplus c$. Поэтому для превращения функции XOR в обратимый унитарный оператор достаточно сохранить на выходе один из ее аргументов и определить ее, скажем, следующим образом:

$$\mathrm{Cnot}|a, b\rangle = |a, a \oplus b\rangle.$$

В квантовом варианте эта функция обычно называется *управляемое-НЕ (controlled-NOT)*, поскольку ее эффект сводится к следующему: если первый (управляющий) бит находится в состоянии $|0\rangle$, второй (целевой или управляемый) бит сохраняет свое состояние; иначе

целевой бит инвертируется. В матричной нотации и в нотации состояний это преобразование выглядит следующим образом, индексы у C_{12} указывают управляющий и целевой биты:

$$C_{12} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \text{ или } \begin{array}{l} |00\rangle \to |00\rangle \\ |01\rangle \to |01\rangle \\ |10\rangle \to |11\rangle \\ |11\rangle \to |10\rangle \end{array}.$$

Поскольку классические логические функции *AND, OR* не являются обратимыми (в том же смысле, что и *XOR*), в квантовом варианте их можно выполнить не менее чем на трех битах, фактически сохраняя на выходе состояния обоих входов. Например, *AND* превращается в дважды управляемое НЕ (controlled-controlled-NOT), которое определяется естественным образом: целевой бит инвертируется тогда и только тогда, когда оба управляющих бита находятся в состоянии $|1\rangle$.

Преобразование "управляемое НЕ" играет очень важную роль в системе квантовой логики. Идеи, заложенные при его конструировании, и свойства этого квантового аналога логической операции *XOR* имеют очень широкую область применимости:

- "Управляемые" операторы — универсальный способ конструирования несложных и часто легко реализуемых унитарных операторов: если управляющий бит находится в состоянии $|0\rangle$, применим к целевому биту оператор A, иначе применим к нему B;
- Сохранение входных аргументов на выходе — универсальный способ обратимого вычисления функций. Если у нас есть аргумент $|x\rangle$ длиной n бит и мы хотим построить оператор (квантовую схему) F, вычисляющую функцию $f(x)$, используя в качестве рабочих переменных еще m бит, схема эта может выглядеть следующим образом:
$$F|x, 0, 0^m\rangle \to |x, f(x), 0^m\rangle.$$
Для сохранения обратимости входные данные и рабочее пространство необходимо вернуть в исходном состоянии.
- Неразрушающая запись. Грубо говоря, унитарность эволюции приводит к тому, что квантовая информация не может быть потеряна. Для сохранения обратимости необходимо позаботиться и о том исходно нулевом бите, который в итоге превратится в значение функции $f(x)$. Этот бит не может быть просто уничтожен, необходима конструкция, сохраняющая и его исходное значение $|0\rangle$, и конечное $|f(x)\rangle$. Это можно сделать, если на самом деле схема F работает следующим образом:
$$F|x, b\rangle \to |x, b \oplus f(x)\rangle.$$
При $b = 0$ получается то, что нужно, и такая схема является обратимой. Таким образом, операция *исключающее или* перезаписывает ячейку памяти неразрушающим образом.
- Универсальность. Один или несколько операторов (gates) называются универсальными, если из них можно составить схему, реализующую любое унитарное преобразование. Сам по себе оператор controlled-not не универсален, но становится таковым, если к нему добавить вращение общего вида, действующее на один q-бит следующим образом [13]:
$$V(\theta, \phi) = \begin{pmatrix} \cos(\theta/2) & -ie^{-i\phi}\sin(\theta/2) \\ -ie^{i\phi}\sin(\theta/2) & \cos(\theta/2) \end{pmatrix}.$$

Конкретная форма этого оператора берет свое начало из техники ядерного магнитного резонанса. Достаточно выбрать одно из вращений этого класса с иррациональными (в долях π) θ, ϕ. Там же [13] показано, что почти все двухбитовые операторы универсальны, так что controlled-NOT в этом смысле скорее исключение.

- Обмен квантовых состояний. Для любых $|\phi\rangle$,$|\psi\rangle$

$$C_{12}C_{21}C_{12}|\phi\rangle|\psi\rangle = |\psi\rangle|\phi\rangle,$$

причем эти состояния могут быть реализованы даже на физически разных системах (скажем, электронах и фотонах). По сути, эта формула представляет собой квантовый вариант известной среди программистов задачи-шутки: как обменять местами значения переменных a и b, не используя дополнительной памяти? Очень просто:

$$\begin{array}{lcl} a & := & a \oplus b \\ b & := & a \oplus b \quad ; \text{ теперь } b \text{ содержит исходное значение } a \\ a & := & a \oplus b \quad ; \text{ теперь и } a \text{ содержит исходное значение } b. \end{array}$$

- Возможность реализации. Операция XOR была неявно реализована в экспериментах по переносу поляризации в области электронно-ядерной резонансной спектроскопии [12] еще в 1956 году. Перенос поляризации фактически описывался схемой $|a, b\rangle \to |a \oplus b, a\rangle$, и авторов в первую очередь интересовал перенос состояния поляризации $|a\rangle$ на систему $|b\rangle$, а попутная реализация логической функции осталась в то время незамеченной.

2.5. Теорема о некопируемости квантового состояния

Квантовомеханическое состояние общего вида (неизвестное заранее и не описанное классической процедурой приготовления) невозможно скопировать. Доказательство этого фундаментального факта довольно просто. Чтобы изготовить копию состояния $|\alpha\rangle$, необходимо найти такой линейный и унитарный оператор U, действующий на пару состояний $|\alpha\rangle$ и $|0\rangle$, который выполнит эволюцию $U(|\alpha\rangle|0\rangle) = |\alpha\rangle|\alpha\rangle$. Поскольку это "копирующее устройство" должно работать на любом векторе состояний, выберем другой вектор состояния $|\beta\rangle \neq |\alpha\rangle$ и скопируем его тоже: $U(|\beta\rangle|0\rangle) = |\beta\rangle|\beta\rangle$. Наконец, возьмем третий вектор, являющийся линейной комбинацией двух предыдущих: $|\gamma\rangle = (|\alpha\rangle + |\beta\rangle)/\sqrt{2}$. Пытаясь скопировать и его тоже, по линейности оператора U получаем

$$U(|\gamma\rangle|0\rangle) = \frac{1}{\sqrt{2}}(|\alpha\rangle|\alpha\rangle + |\beta\rangle|\beta\rangle) \neq |\gamma\rangle|\gamma\rangle,$$

то есть совсем не то, что нужно. Эта аргументация предложена в работе [14]. Разумеется, любой оператор может копировать *некоторые* состояния, ортогональные друг другу, например controlled-NOT успешно копирует состояния $|0\rangle$ и $|1\rangle$, но не $(|0\rangle \pm |1\rangle)/\sqrt{2}$.

2.6. Квантовый параллелизм

В отличие от классического квантовый регистр может находиться в состоянии суперпозиции, включающей в себя все его 2^n состояний. Если мы теперь применим к такому "всеобщему" состоянию какой-нибудь "полезный" унитарный оператор эволюции, переводящий любое базисное состояние в некую нужную нам функцию от этого состояния, мы

получим в регистре суперпозицию значений этой функции на всех возможных входных данных. Таким образом, за один цикл работы квантового компьютера мы выполняем *одновременно* 2^n вычислений — экспоненциально большой по n объем вычислительной работы. Это явление обычно называют *квантовым параллелизмом*.

Однако не все так просто. Для того чтобы извлечь какую-то информацию из полученного результата, конечное состояние квантового регистра необходимо измерить. Разумеется, мы можем построить наблюдаемую, имеющую 2^n состояний, применить ее к нашему состоянию, в котором замешаны все 2^n результатов вычислений, и получить в результате с некоторой вероятностью один из 2^n результатов. Однако это будет всего лишь *одно* состояние классического регистра из n битов. Квантовая суперпозиция будет разрушена, остальная содержавшаяся в ней информация в общем случае будет потеряна. Ситуацию можно несколько улучшить, повторив цикл работы компьютера несколько раз и получив распределение вероятности конечного результата измерений. Однако в общем и целом можно прийти к выводу, что использовать экспоненциальное ускорение вычислений можно только тогда, когда один результат измерения содержит некую общую, интегральную характеристику *всех* значений вычисляемой функции, т.е. обнаруживает у этой функции некую периодичность, симметрию или групповую структуру. Именно в этих случаях удается построить практически полезные квантовые алгоритмы.

Отметим ещё, что вполне возможно построение квантового компьютера, работающего только с базовыми состояниями $|0\rangle$ и $|1\rangle$. Именно такое устройство и было предложено в первых работах Фейнмана [2]. Функционально оно представляет собой копию классического компьютера. В нем вполне возможно копирование информации, но нет и не может быть никакого параллелизма. Никакого особенного выигрыша по сравнению с классическим компьютером такое устройство не дает, что и было отмечено Фейнманом.

3. Квантовые алгоритмы

Конструирование квантовых алгоритмов существенно отличается от подобной деятельности для обычных компьютеров. Реально полезные алгоритмы можно пересчитать по пальцам, и практически все известные до настоящего времени обсуждаются ниже. Не все эти алгоритмы вычислительные, но все представляют собой весьма необычные способы использования принципов квантовой механики.

3.1. Моделирование физических систем

Наиболее простым и естественным применением квантового компьютера, то есть квантовой системы с управляемой эволюцией, может оказаться моделирование других квантовых систем. Для моделирования вектора состояния квантовой системы с размерностью пространства состояний 2^n требуется классический компьютер с памятью примерно такого же размера, однако достаточно квантового регистра размера n. Для моделирования эволюции такой системы в общем случае надо перемножать унитарные матрицы размера $2^n \times 2^n$, так что и классический и квантовый компьютеры могут оказаться неэффективны — квантовая схема в принципе может оказаться экспоненциально большого размера. Однако показано, что очень широкий класс систем (например, многочастичные системы с локальными взаимодействиями) может моделироваться эффективно.

3.2. Квантовая телепортация

Предположим, нам необходимо передать из пункта А в пункт Б, от Алисы к Бобу (обычные персонажи из статей по теории информации), один квантовый бит в состоянии $|\phi\rangle$. Точнее, мы хотим передать полную информацию об этом состоянии, материальная система, на которой реализован этот бит, нам не нужна. Если существует классический алгоритм построения состояния $|\phi\rangle$, можно передать в пункт Б этот алгоритм и восстановить на месте требуемое состояние. В противном случае, казалось бы, единственным выходом является поместить наше состояние в большой мешок, изолирующий от внешней среды, и в таком виде физически переправить его в пункт Б. Можно также обменять наше состояние с произвольным состоянием какой-нибудь системы-переносчика, например фотона, и физически отправить эту более транспортабельную систему. Такой обмен состояний возможен с помощью функции управляемое-НЕ. Другого выхода вроде бы не существует, поскольку полностью изучить произвольное состояние $|\phi\rangle$ невозможно — первое же измерение его разрушит, а наделать с него копий невозможно. Однако в 1993 году был обнаружен способ [18] передачи из А в Б полной информации о состоянии $|\phi\rangle$, при котором из А в Б передается только классическая информация! Основана эта конструкция на использовании парадокса Эйнштейна-Подольского-Розена.

Как известно, предложенный Эйнштейном, Подольским и Розеном (ЭПР) мысленный эксперимент [15] по обнаружению дальнодействия в квантовой механике можно свести к рассмотрению пары квантовых систем с двумя дискретными состояниями каждая (сами авторы рассматривали более сложный непрерывный случай системы двух частиц с нулевым полным импульсом, и акцент делался на доказательстве неполноты квантовомеханического описания действительности). Рассмотрим пару частиц А и В со спином 1/2 и обозначим состояние с положительной проекцией спина на ось z как $|\uparrow\rangle$, а состояние с отрицательной проекцией как $|\downarrow\rangle$. Система из двух частиц первоначально приготавливается в синглетном по спину состоянии $1/\sqrt{2}\,(|\uparrow\rangle|\downarrow\rangle - |\downarrow\rangle|\uparrow\rangle)$, а затем частицы разносятся на значительное расстояние в пространстве. Поскольку суммарный угловой момент системы равен нулю, измерение спина частицы А в проекции на любую ось мгновенно переводит частицу В в состояние, в котором ее проекция спина на ту же ось в точности противоположна той, которую мы измерили у А. Точнее было бы сказать, что изменяется не состояние частицы В, а наше знание (информация) об этом состоянии. Подобная "передача" информации не противоречит теории относительности лишь потому, что на самом деле деле информация остается в пункте А, поскольку из-за теоремы о некопируемости в пункте В мы не можем "изучить" состояние частицы В, а потому и не можем переслать мгновенный сигнал (невозможно установить, когда же следует начинать измерять состояние частицы В, а повторить измерение не получится).

Все, что мы можем сделать, это получить корреляцию между результатами измерений проекций спинов А и В на различные оси η_A, η_B, повернутые на углы ϕ_A, ϕ_B к оси z. Теория [16,17] предсказывает вероятность получить при таком измерении одинаковый для обеих частиц результат (оба "+" или оба "−") $P = \sin^2((\phi_A - \phi_B)/2)$, то есть ноль при $\phi_A = \phi_B$, 100% при $\phi_A = \phi_B + 180^\circ$ и 75% при $\phi_A - \phi_B = 120^\circ$. Замечательно то, что невозможно приписать частицам А и В *локальные*, т.е. независимые свойства, которые бы порождали столь высокие корреляции. Так, для $\phi_A - \phi_B = 120^\circ$ локальные скрытые переменные могут породить корреляции не более 2/3. Проведенные эксперименты [24,25] подтвердили справедливость квантовой механики.

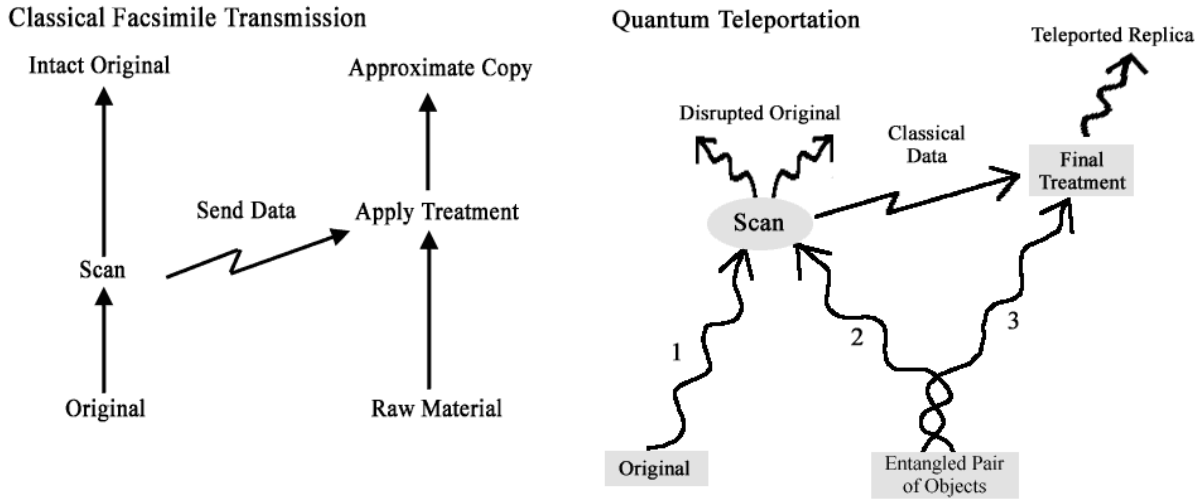

Рис. 1. Сравнение классической факсимильной передачи данных (слева) и квантовой телепортации (справа).

По указанным причинам сами по себе ЭПР-корреляции непригодны для передачи информации. Однако если их скомбинировать с классическим сигналом, возникает конструкция, которую обычно называют квантовой телепортацией [18]. Она изображена справа на рисунке 1.

Для передачи состояния $|\phi\rangle$ (будем называть его частицей 1) из А в Б Алисе и Бобу следует заранее запастись парой частиц 2 и 3 в синглетном ЭПР-состоянии

$$|\Psi_{23}^-\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow_2\rangle|\downarrow_3\rangle - |\downarrow_2\rangle|\uparrow_3\rangle\right),$$

которые следует разделить и частицу 2 отдать Алисе, а частицу 3 — Бобу. Можно представить себе некий "центр телепортации" С, который изготавливает такие пары и заранее рассылает всем желающим. Состояние частицы 1 можно записать как $|\phi_1\rangle = a|\uparrow_1\rangle + b|\downarrow_1\rangle$, где a и b неизвестные комплексные коэффициенты с $|a|^2+|b|^2 = 1$, а совместное состояние частиц 1,2,3 представляет собой прямое произведение независимых состояний $|\phi_1\rangle|\Psi_{23}^-\rangle$.

Начиная передачу, Алиса измеряет состояние *пары* частиц 1 и 2 в так называемом базисе Белла, который состоит из синглета $|\Psi_{12}^-\rangle$ и триплета

$$|\Psi_{12}^+\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow_1\rangle|\downarrow_2\rangle + |\downarrow_1\rangle|\uparrow_2\rangle\right), \quad |\Phi_{12}^\pm\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow_1\rangle|\uparrow_2\rangle \pm |\downarrow_1\rangle|\downarrow_2\rangle\right),$$

которые представляют собой полный базис для системы частиц 1 и 2. Полное состояние системы трех частиц до измерения можно переписать как

$$|\Psi_{123}\rangle = \frac{a}{\sqrt{2}}\left(|\uparrow_1\rangle|\uparrow_2\rangle|\downarrow_3\rangle - |\uparrow_1\rangle|\downarrow_2\rangle|\uparrow_3\rangle\right) + \frac{b}{\sqrt{2}}\left(|\downarrow_1\rangle|\uparrow_2\rangle|\downarrow_3\rangle - |\downarrow_1\rangle|\downarrow_2\rangle|\uparrow_3\rangle\right).$$

В этом выражении состояния частиц 1,2 можно выразить через базис Белла $|\Psi_{12}^\pm\rangle$, $|\Phi_{12}^\pm\rangle$ и получить

$$|\Psi_{123}\rangle = \frac{1}{2}\Big[|\Psi_{12}^-\rangle(-a|\uparrow_3\rangle - b|\downarrow_3\rangle) + |\Psi_{12}^+\rangle(-a|\uparrow_3\rangle + b|\downarrow_3\rangle) + |\Phi_{12}^-\rangle(a|\downarrow_3\rangle + b|\uparrow_3\rangle) + |\Phi_{12}^+\rangle(a|\downarrow_3\rangle - b|\uparrow_3\rangle)\Big].$$

В момент измерения состояние системы 1,2,3 коллапсирует в состояние, соответствующее одному из членов этого выражения. В результате измерения Алиса получит одно из четырех состояний пары 1,2 с равной вероятностью 1/4, а частица 3, принадлежащая Бобу, соответственно спроецируется в одно из четырех чистых состояний

$$|\phi_3\rangle = -\begin{pmatrix} a \\ b \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix}.$$

Эти состояния лишь фиксированными матричными множителями отличаются от исходного состояния частицы 1. Теперь Алисе достаточно передать Бобу по классическому каналу (телефону) номер результата своего измерения (1,2,3,4), что составляет два бита классической информации, после чего Боб восстанавливает из своей частицы 3 копию состояния частицы 1, применив к частице 3 один из четырех фиксированных унитарных операторов (фактически это фазовый сдвиг и вращения на 180° вокруг осей z, x, y соответственно). Телепортация завершена, Боб имеет копию частицы 1, но никакие квантовые объекты из А в Б не передавались! Состояние частицы 1 необратимо разрушено измерением, в руках у Алисы осталось одно из состояний базиса Белла пары 1 и 2, теорема о некопировании не нарушена.

Телепортация является линейной операцией, а потому она будет работать не только для чистых, но и для смешанных и entangled состояний. Например, если частица 1 образовывала до телепортации ЭПР пару с частицей 0, после телепортации частицы 3 и 0 по-прежнему будут образовывать синглетную пару. Существует и обобщение на системы с $N > 2$ ортогональных состояний.

Классическое сообщение играет существенную роль в этой конструкции. Если попытаться "угадать" это сообщение и выбрать оператор реконструкции случайным образом, получится равномерная смесь всех возможных состояний, никак не коррелированная с исходным состоянием. Послать таким способом сверхсветовой сигнал невозможно. Таким образом, телепортация завершается только в момент прихода классического сигнала, то есть происходит она внутри светового конуса и не нарушает никаких физических законов. Любопытно то, что для выполнения телепортации Алисе даже не нужно знать местонахождение Боба — классическую информацию можно передать широковещанием (по телевизору), копия воссоздастся там, где находится частица 3.

Выполнены первые эксперименты по практической реализации квантовой телепортации отдельных фотонов [20]. Передавались состояния поляризации фотона в направлении ±45° к осям квантования и их линейная комбинация — состояние круговой поляризации. В качестве источника ЭПР-пар использовалась параметрическая конверсия в нелинейном кристалле, при которой ультрафиолетовый фотон распадается на пару фотонов красного цвета с ортогональными состояниями поляризации. В настоящее время неизвестен какой-либо способ выполнить полное измерение в базисе Белла. Экспериментаторы обошли эту трудность, выполняя измерения в проекции на один из векторов базиса Белла (синглетный), что все же позволяет выполнить телепортацию в 25% случаев.

В сети Internet доступен on-line обзор по квантовой телепортации [19] и оригинальные статьи [18] и [20]. Есть и популярное описание [21] этого эксперимента.

В одном из советских фантастических рассказов 60-х годов был осужден на пожизненное заключение конструктор системы телепортации, которая копировала предметы на выходе, уничтожая на входе. Дело вскрылось, когда система скопировала человека,

но забыла уничтожить оригинал. Создателям системы квантовой телепортации подобная участь не грозит...

3.3. Факторизация больших чисел

Факторизация (разложение на множители) больших (100 и больше десятичных цифр) чисел является одной из актуальнейших задач современной теории чисел и криптоанализа. Задача эта является вычислительно сложной, поскольку трудоемкость всех известных классических алгоритмов ее решения *экспоненциально* растет с размером задачи. Допустим, нам необходимо разложить на множители число N, в двоичной записи которого n разрядов. Очевидный способ — попробовать поделить N на все целые числа (или на все простые числа, разница невелика) от 2 до $\sqrt{N}$. Если у числа N нет маленьких делителей, придется перебрать порядка $\sqrt{N} \sim 2^{n/2}$ вариантов. Существуют хитроумные алгоритмы типа "квадратичного решета" и "решета числового поля", которые решают эту задачу за время порядка $\exp(cn^{1/3})$, где c есть константа порядка единицы. Эти алгоритмы факторизуют число из 100 десятичных цифр за недели, но для 200 цифр нужны уже миллионы лет. До сих пор неизвестно, существует ли классический алгоритм факторизации с *полиномиальной* по n сложностью.

С задачей факторизации тесно связана так называемая задача о *дискретном логарифме*. Задано число N и целые числа $a, b < N$. Целое число $x < N$ называется *дискретным логарифмом* b по основанию a и модулю N, если оно является решением уравнения $a^x = b \bmod N$. Считается, что вычислительная сложность дискретного логарифмирования примерно такая же, как у факторизации.

Задачи эти крайне важны в криптографии, поскольку на них основаны практически широко используемые алгоритмы *шифрования с открытым ключом* RSA и El Gamal, которые позволяют осуществить на первый взгляд невозможное — конфиденциальную связь по открытому каналу. Алгоритм "рукопожатия" Эль Гамаль настолько прост, что его можно описать в нескольких строках. Абоненты А и Б хотят установить секретную связь по каналу, *все* сообщения по которому просматриваются сторонним наблюдателем. Можно использовать шифрование, но как передать пароль? Абоненты А и Б

- *открыто* выбирают большое простое число N и число $e < N$;
- тайно и никуда ничего не передавая, А выбирает случайным образом число $A < N$, Б выбирает число $B < N$;
- А вычисляет $e^A \bmod N$ и передает его Б;
- Б вычисляет $e^B \bmod N$ и передает его А.

Теперь и А, и Б могут независимо вычислить число

$$X = (e^B)^A \bmod N = (e^A)^B \bmod N,$$

которое и будет служить паролем. Наблюдателю, который видел все, не достается ничего, поскольку из прошедших по каналу e^A и e^B невозможно за разумное время найти A и B.

Алгоритм RSA (названный по именам авторов: Ривера, Шамира, Адлемана) породил целый класс методов шифрования, для которых и привилось название *шифрование с открытым ключом*. Все эти методы устроены так, что они имеют два ключа, один используется только для шифрования данных, другой — только для расшифровки. Пользователь в соответствии с алгоритмом генерирует такую пару ключей, после чего ключ

шифрования (*публичный ключ*) раздает всем желающим, а ключ дешифрования (*приватный ключ*) хранит у себя. В результате он получает конфиденциальный почтовый ящик — любой желающий может зашифровать письмо открытым ключом и бросить его в ящик, но только хозяин может письмо достать (дешифровать). Этот алгоритм годится и для передачи пароля по открытому каналу: каждая сторона попросту создает собственную пару ключей и собственный "почтовый ящик". К сожалению, все известные алгоритмы шифрования с открытым ключом очень трудоемки, поэтому выгоднее передать пароль для более простого метода шифрования, чем шифровать весь поток данных. А вот для писем время шифрования особой роли не играет, там описанные методы используются непосредственно.

Столь же естественно в этих методах возникает и конструкция *цифровой подписи*. Если сохранить в тайне ключ шифрования, а публично распространить ключ дешифровки, только автор сможет зашифровать сообщение, а расшифровать и проверить его сможет любой желающий. Во всех известных на сегодняшний день алгоритмах шифрования с открытым ключом каждый ключ представляет собой пару больших целых чисел, а взлом шифра (нахождение по открытому ключу приватного и наоборот) требует решения задачи факторизации (в некоторых случаях задачи нахождения дискретного логарифма).

В 1994 году Петеру Шору (Peter Shor) удалось построить квантовый алгоритм, решающий задачи факторизации и дискретного логарифма за полиномиальное время [22]. Этот изящный результат основан на использовании квантового параллелизма и сведения задачи к поиску периода некоторой функции. Пусть нам необходимо разложить на множители некоторое число N. Выберем произвольное $a < N$ и рассмотрим функцию

$$f_N(x) = a^x \bmod N.$$

Эта функция является периодичной с некоторым периодом r хотя бы потому, что число ее значений конечно. Если N простое, то $r = N - 1$, но этот случай легко исключается классическими методами, существуют быстрые алгоритмы проверки простоты числа. В общем случае имеем

$$f_N(x + r) = f_N(x) \quad \text{и соответственно} \quad a^r = 1 \bmod N.$$

Если известно r (дискретный логарифм единицы по основанию a), разложение N на множители легко находится классическими методами. Действительно, если r четное, из $a^r - 1 = 0 \bmod N$ имеем

$$\left(a^{r/2} - 1\right)\left(a^{r/2} + 1\right) = 0 \bmod N.$$

Поскольку произведение в левой части делится на N, его сомножители должны иметь общие с N делители, которые и находятся классическим алгоритмом Евклида (поиска наибольшего общего делителя). Если r нечетное или множитель в левой части вырождается в ноль, алгоритм проваливается, и нам следует выбрать другое a. При больших N это случается очень редко.

Задача нахождения r есть задача о дискретном логарифме и классическое ее решение за полиномиальное время неизвестно. Квантовомеханическая часть алгоритма Шора и предназначена для быстрого поиска r. Для решения этой задачи мы используем квантовый компьютер с двумя квантовыми регистрами длины n такой, что $M = 2^n > N$, $M \sim N^2$. Алгоритм выглядит следующим образом:

- Приготовим классическим путем оба регистра в состоянии $|0\rangle$. Переведем входной регистр в "универсальное" состояние, в котором с равными амплитудами присутствуют все 2^n возможных состояний. Реализуется это действие просто, достаточно подействовать на каждый бит в отдельности преобразованием Адамара H, которое отображает $|0\rangle \to 1/\sqrt{2}(|0\rangle + |1\rangle)$:

$$H|0\rangle \cdots H|0\rangle = \frac{1}{2^{n/2}} \left(|0\rangle + |1\rangle\right)^n = \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle.$$

- Применим к нашим регистрам квантовую схему, которая вычисляет $f_N(x)$. Существует быстрый классический алгоритм вычисления этой функции, можно показать, что при этом условии всегда существует и быстрый квантовый аналог. Наши регистры перейдут в состояние

$$\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle|f_N(x)\rangle.$$

  В выходном регистре возникла суперпозиция всех возможных значений $f_N(x)$.
- Измерим состояние выходного регистра. Это измерение даст нам значение функции $f_N(k)$ при каком-то случайном k, а состояние выходного регистра соответственно редуцируется до $|f_N(k)\rangle$. Измеренное значение нас не интересует, но вот состояние *входного* регистра при этом редуцируется до линейной комбинации тех и только тех состояний, которые совместимы с измеренным на выходе значением, то есть сохранятся те x, для которых $f_N(x) = f_N(k)$, т.е. $x = k, k + r, k + 2r, \ldots$
- Для извлечения возникшей во входном регистре периодичности применим к нему квантовое преобразование Фурье

$$U|x\rangle = \frac{1}{M} \sum_{k=0}^{M-1} e^{i2\pi kx/M} |k\rangle$$

  и измерим результат. При преобразовании Фурье период r преобразуется в M/r, и с высокой вероятностью мы измерим число близкое к jM/r с неким $j = 1, 2, \ldots$. Опять-таки классическими средствами (разложением в непрерывную дробь, все тот же алгоритм Евклида) мы извлекаем из этого числа r, на чем алгоритм завершается.

Алгоритм Шора является вероятностным со средней сложностью порядка $\log^3(N)$. По-видимому, эффективность алгоритмов подобного типа основана не только на экспоненциально большом количестве участвующих состояний, но и на своеобразной перекачке информации при редуцировании "скрученного" (entangled) состояния $|x\rangle|f_N(x)\rangle$.

3.4. Поиск в базе данных

Еще одним примером эффективного квантового алгоритма является алгоритм поиска информации в неупорядоченной базе данных, иногда называемый универсальным алгоритмом перебора. В 1997 году в работе [27] был предложен быстрый алгоритм решения следующей простой задачи: задан неупорядоченный набор из N предметов, найти номер предмета, совпадающего с данным образцом. Нетрудно доказать, что классический метод последовательного сравнения образца со всеми предметами потребует в среднем $N/2$

сравнений. Предложенный Гровером квантовомеханический алгоритм требует порядка $\sqrt{N}$ шагов. Работает он следующим образом.

Мы должны как-то отличать нужный элемент за номером j от всех остальных, ненужных. Предположим, что нами для этой цели сконструирован унитарный оператор сравнения S, который выделяет нужный элемент следующим образом: он действует как тождественый на ненужные элементы и меняет фазу у нужного:

$$S|i\rangle = |i\rangle \text{ при } i \neq j \text{ и } S|j\rangle = -|j\rangle.$$

Возьмем квантовый регистр, достаточно длинный, чтобы число его состояний превышало N. Переведем его в "универсальное" состояние, в котором все возможные состояния регистра присутствуют с равными амплитудами. Обозначим амплитуду выделенного состояния a, обычного b. Если состояние регистра для краткости обозначать парой этих амплитуд, можно описать исходное состояние как

$$|a, b\rangle = a|j\rangle + b\sum_{i\neq j}|i\rangle,$$

где по условию нормировки $a^2 + (N-1)b^2 = 1$. В исходном состоянии $a = b = 1/\sqrt{N}$. Применим к этому состоянию сложное преобразование U_G, которое определено следующим образом: сначала преобразование S, затем преобразование Фурье, смена знака у всех компонент за исключением $|0\rangle$, обратное Фурье-преобразование. Можно показать, что это преобразование приводит к следующему результату:

$$U_G|a, b\rangle = \left|\frac{2N-2}{N}b + \frac{N-2}{N}a,\ \frac{N-2}{N}b - \frac{2}{N}a\right\rangle.$$

Коэффициент при выделенном элементе стал несколько больше, чем при остальных. Фактически выполнен некий поворот в пространстве состояний в направлении чистого состояния $|j\rangle$. Далее мы просто применяем преобразование U_G m раз, где $m \simeq (\pi/4)\sqrt{N}$. При этом исходное состояние приближается к чистому $|j\rangle$. Остается только его измерить.

Иногда этот метод сравнивают с выпечкой пирога в печи: квантовое состояние помещают в "квантовую печь", и ответ медленно вызревает до готовности. Если его вынуть слишком рано, он будет сырой, неточный; если передержать, он сгорит и рассыплется. Доказано, что метод этот оптимален — никакой квантовый алгоритм не может работать быстрее чем за время порядка $O(\sqrt{N})$. Следует заметить, что ускорение в данном случае не экспоненциальное, так что для теории вычислений этот метод ничего нового не дает.

Однако практическая полезность данного метода велика. Это и в самом деле универсальный алгоритм перебора. Существует множество задач, в которых найти решение нелегко, а проверить, что решение правильное, просто. Ярким примером является подбор пароля к шифрованным данным. Любую такую задачу можно в крайнем случае решать полным перебором методом Гровера — проверку правильности решения можно вставить в алгоритм сравнения S.

3.5. Квантовая коррекция ошибок

Алгоритмы факторизации и поиска, описанные выше, требуют для практически полезной реализации тысяч квантовых битов и миллионов квантовых логических переходов (моделирование физических систем может быть полезным уже при размере компьютера в

несколько бит). Однако абсолютно точная реализация операторов эволюции (квантовых переходов) и абсолютная изолюция системы от окружающей среды (гарантирующая унитарность эволюции и сохранение когерентности состояний) невозможна. Соответственно ошибки в принципе могут быть двух видов — обратимые, вызываемые неточностью реализации операторов эволюции, и необратимые, т.е. потери когерентности, вызываемые паразитным взаимодействием с макроскопическим окружением или спонтанным излучением. Как мы уже видели, в отличие от классического квантовый компьютер является системой не с дискретным, а с непрерывным пространством состояний, в результате чего малые ошибки могут накапливаться и в конце концов нарушать работу компьютера. В соответствии с этим до последнего времени считалось, что крупномасштабные квантовые вычисления могут оказаться в принципе невозможными.

Положение в корне изменилось в 1996 году с появлением работы Петера Шора [23], в которой были предложены квантовые коды, корректирующие ошибки. Конструкция эта реализует, на первый взгляд, невозможное — она позволяет перевести квантовый компьютер в "правильное" вычислительное состояние, не измеряя его состояния и даже в случае необратимых ошибок. Поскольку отсутствует измерение, отсутствует и связанная с ним потеря когерентности. Достигается это в принципе тем же путем, что и в классических кодах, корректирующих ошибки: к каждому информационному биту добавляется несколько служебных, называемых обычно оболочкой, ансиллой. Группа этих физических битов образует логический бит, состояние которого и используется в вычислениях, а полное пространство состояний всех физических битов перестает быть непрерывным и разбивается на ячейки, различие состояний внутри которых на состояние логического бита не влияет и время от времени корректируется. Вероятность перескока из ячейки в ячейку и соответственно некорректируемой ошибки может быть сделана произвольно малой.

На примере классических кодов покажем принцип, каким образом такая схема может обходиться без измерений. Классический код, устойчивый к ошибкам, может быть построен следующим образом: из всего множества n-битных двоичных чисел выберем подмножество чисел "настолько различных", что они остаются различными даже после добавления к ним (побитного сложения без переноса) любого числа из предопределенного "множества ошибок", например всех чисел с единственным ненулевым битом. Если выбранное подмножество чисел замкнуто относительно сложения, код называется линейным. Линейный код полностью определяется его *матрицей контроля четности* H, которая ортогональна всем корректным кодовым словам: $H \cdot u = 0$. Отсюда следует, что если нам встретилось неправильное кодовое слово $u' = u + e$ с неким ошибочным вкладом e, то

$$H \cdot u' = (H \cdot u) + (H \cdot e) = H \cdot e.$$

Если из последнего выражения можно восстановить e, что возможно для всего класса корректируемых ошибок, то мы можем вычесть это e из u' и восстановить u. Такая операция восстановления не зависит от u. Отсюда следует, что для коррекции ошибки вовсе не нужно знать (измерять) то сообщение, которое мы корректируем.

Конструкции квантовых кодов, корректирующих ошибки, достаточно сложны, и мы не будем вдаваться в детали. Сухой же остаток состоит в следующем. Существует некое пороговое значение точности на один шаг δ_0, такое что при меньшей погрешности возможно сколь угодно длинное квантовое вычисление (причем погрешности могут возникать во всех битах, и значащих, и корректирующих). Оценки δ_0 колеблются в диапазоне от $1/300$

до 10^{-6}. В принципе возможны и системы, в которых устойчивость к ошибкам заложена на "физическом" уровне, например системы, основанные на анионных возбуждениях [26].

3.6. Квантовая криптография

Одним из важнейших и быстро развивающихся практических приложений квантовой теории информации является квантовая криптография. Основная идея квантовой криптографии проста и понятна: поскольку скопировать (размножить) квантовую информацию невозможно, квантовое сообщение либо придет по назначению, либо попадет к стороннему наблюдателю, но тогда этот факт можно обнаружить. Возможно учесть и потерю некоторых бит из-за шума и ограниченной эффективности детекторов. Существует несколько схем криптографических протоколов, использующих передачу квантовой информации. Обычно они основаны на использовании двух некоммутирующих наблюдаемых или на основе парадокса ЭПР (квантовой телепортации).

Телепортация и другие схемы на основе парадокса ЭПР представляют собой великолепные методы передачи шифрованной информации: довольно трудно представить себе, где же передаваемую телепортацией информацию можно было бы перехватить. Квантовый канал передачи здесь отсутствует как таковой: до начала телепортации используемая ЭПР-пара стандартна и вообще никакой информации не несет, а после момента измерения по каналу связи передается только классическая информация, которой недостаточно для воспроизведения переданного сообщения. Единственный недостаток этих методов — то, что они пока экспериментально не реализованы.

Гораздо более простыми в реализации являются квантовые криптографические протоколы на основе двух некоммутирующих переменных. Приведем один из возможных методов. Этот алгоритм может работать и в присутствии шума [8].

Как и в классическом случае, будем решать задачу *распространения ключей*, то есть передачи по открытому каналу пароля для последующего шифрования данных. Паролем будет являться большое целое число, кодируемое как строка классических битов. Для достижения этой цели мы будем передавать из пункта А в пункт Б по квантовому каналу передачи квантовые биты в базисных состояниях $|0\rangle$, $|1\rangle$ и их линейные комбинации $|+\rangle = |0\rangle + |1\rangle$, $|-\rangle = |0\rangle - |1\rangle$ (нормировочный множитель опускаем). Физической реализацией этой схемы может служить передача по оптоволоконному кабелю состояний фотона, поляризованных в проекции на прямые и повернутые на 45° пары осей квантования. Основная идея состоит в следующем. Передадим из А в Б $2n$ квантовых битов, при передаче случайно выбирая одно из четырех состояний, а при приеме случайно выбирая ось квантования для измерений. После этого пункты А и Б публично по открытому классическому каналу (телефону) сообщают друг другу, какие оси квантования были выбраны для посылки и приема каждого из $2n$ квантовых битов. Сохраним те и только те результаты передачи, у которых оси квантования приемника и передатчика, как оказалось, совпадали. В отсутствии шумов эти биты были переданы и измерены точно. Припишем измеренным значениям $|0\rangle$, $|+\rangle$ классический бит 0, значениям $|1\rangle$, $|-\rangle$ бит 1, и в результате в пунктах А и Б мы теперь имеем одну и ту же классическую битовую последовательность длиной приблизительно n. Эту битовую строку обычно называют результатом *первичной квантовой передачи (raw quantum transmission, RQT).*

Постороннему наблюдателю очень трудно перехватить эту строку, не оставив при этом следов своего присутствия. Квантовый бит невозможно скопировать, самым гру-

бым способом перехвата является активный — внешний наблюдатель разрывает канал сообщения, измеряет приходящие из пункта А биты и дублирует их в пункт Б. Однако выбор осей квантования наблюдателя лишь в половине случаев совпадет с выбором осей передатчика, поэтому половина перехваченных сообщений будет дублирована в пункт Б неправильно. Однако в пункте Б эти неправильно скопированные сообщения будут в половине случаев еще и неправильно измерены, поскольку измеряться они будут в проекции на оси, совпадающие с осями передатчика и соответственно не совпадающие с осями наблюдателя. В итоге приблизительно $n/4$ измеренных битов случайно совпадет с тем, что было передано, и только $n/4$ битов RQT будет разрушено наблюдателем. Однако и этого вполне достаточно для обнаружения факта наблюдения. Для контроля целостности сообщения передатчик и приемник публично выбирают случайным образом $n/2$ битов из RQT и сравнивают их. Если все эти биты совпадают, вероятность того, что канал просматривается, можно оценить как $(3/4)^{n/2} \approx 10^{-125}$ для $n \approx 1000$. Остальные $n/2$ битов RQT представляют собой переданный секретный ключ.

Системы передачи сообщений с использованием квантовых протоколов доступны уже сегодня. В 1997 году реализована квантовая передача сообщений по стандартному оптоволоконному кабелю на расстояние 23 км под озером Женева со скоростью порядка единиц МГц [29]. Квантовые биты кодировались состояниями поляризации лазерных импульсов со средней интенсивностью 0.1 фотона на импульс. Столь низкая интенсивность нужна для того, чтобы импульсы, содержащие более одного фотона, были маловероятны — такие импульсы содержат более одного бита в одинаковом состоянии, а потому их теоретически возможно "расщепить" и подсмотреть.

Огромные архивы по квантовой криптографии существуют в Internet [28].

4. Возможности физической реализации

Задача практической реализации квантового процессора представляется очень и очень технически сложной. Как правило, речь идет о прецизионном управлении отдельными атомами. Необходимо удовлетворить нескольким почти несовместимым требованиям:

- Квантовые биты должны быть надежно изолированы друг от друга и от окружающей среды. При этом стабильными должны быть не только базисные состояния $|0\rangle$ и $|1\rangle$, но и их линейные комбинации типа $|0\rangle + |1\rangle$, и именно здесь характерное время потери когерентности меньше всего.
- Для создания логических переходов необходимо иметь возможность избирательно воздействовать на отдельные биты и пары битов, а также приводить их во взаимодействие между собой. Взаимодействия эти должны контролироваться с высокой точностью (по крайней мере, не хуже критической, обеспечивающей работу кода, корректирующего ошибки).
- Необходимо иметь возможность приготавливать необходимые исходные состояния и измерять конечные.

Существует несколько более или менее реальных подходов к проблеме реализации квантового компьютера.

• Ионные ловушки. Квантовые биты представляются состояниями отдельных ионов или атомов, захваченных в электромагнитные ловушки в глубоком вакууме. Время жизни

некоторых уровней сверхтонкой структуры основного состояния по спонтанному распаду в такой ловушке может достигать тысяч лет. Переходы между состояниями одного иона могут реализовываться взаимодействием с лазерным лучом, но двухбитовые переходы таким путем реализовать нельзя. Их предлагается реализовать путем возбуждения колебательных мод механического движения системы ионов как целого (фононов). Приготовление исходного состояния возможно методами лазерного охлаждения, методы измерения состояния системы в этой технике также известны. Основной экспериментальной трудностью является охлаждение системы ионов в основное состояние, до температуры менее микроКельвина. Основным источником потери когерентности является, по-видимому, нагревание системы из-за взаимодействия с шумовым напряжением на электродах. Оценки показывают, что при современном уровне технологии можно применить порядка 100 переходов к нескольким квантовым битам. В дальней перспективе можно надеяться увеличить эти величины раз в десять, но вряд ли больше.

• Ядерный магнитный резонанс. Эта техника широко используется на практике для изучения строения молекул. Квантовый процессор в данном случае состоит из отдельной молекулы вещества, спинами ядер некоторых атомов в ней (как правило, водорода) можно управлять, поместив систему в комбинацию сильного постоянного и резонансного переменного магнитных полей. Квантовые биты представлены состояниями ядерных спинов, унитарные операторы реализуются импульсами переменных магнитных полей, расщепление уровней из-за спин-спинового взаимодействия дает возможность реализовать двухбитовые операции. Измерение состояния достигается обычным для ЯМР методом — детектированием индуцированного радиоизлучения. Конечно, в ЯМР-спектрометр помещают не отдельную молекулу, а вполне макроскопическое количество вещества. Таким образом, на самом деле используется эволюция не чистого состояния, а матрицы плотности, но и этого оказывается достаточно. Эксперименты масштаба нескольких битов уже проводятся. Так, на двух спинах молекулы хлороформа $CHCl_3$ удалось реализовать алгоритм поиска на четыре состояния [30]. Использовались спины ядер водорода и углерода-13. Однако на большее количество квантовых бит эта техника масштабируется не слишком хорошо, поскольку измеряемый сигнал для n бит падает как 2^{-n}.

Приведенные методы считаются в какой-то степени традиционными. Опишем кратко более экзотические возможности, приведенные в [9].

• Системы сверхпроводящих гранул. При низких температурах микроскопические сверхпроводящие гранулы могут нести заряд всего в несколько пар электронов (электроны в сверхпроводнике связаны в пары). Гранулы взаимодействуют между собой посредством джозефсоновских контактов, этим взаимодействием можно управлять. Однако точность управления каждой гранулой должна быть очень высокой.

• Анионы. Анионы — это особые возбуждения в двумерных квантовых системах, например в двумерной электронной жидкости в магнитном поле. При движении одного такого возбуждения вокруг другого состояние системы меняется строго определенным образом. При наличии в жидкости нескольких *неабелевых анионов* состояние жидкости является вырожденным, причем кратность вырождения экспоненциально зависит от числа анионов. Все эти вырожденные состояния могут образовывать квантовые суперпозиции. На такую суперпозицию никак нельзя воздействовать, не перемещая анионы, а потому она идеально защищена от возмущений. Если обвести один анион вокруг другого,

суперпозиция подвергнется определенному унитарному преобразованию. Это преобразование *абсолютно точное.* Таким образом, мы имеем систему, защищенную от ошибок на физическом уровне. Может быть, эта идея *топологического квантового вычисления* воплотится и как-нибудь иначе.

5. Заключение

Квантовая теория информации еще только зарождается, перспективы и пределы ее развития пока что совершенно неясны. Экспериментальное исследование и практическое использование некоторых ее результатов возможно уже сейчас (квантовая криптография), некоторые (моделирование квантовых систем и телепортация состояния отдельных частиц) станут доступны в ближайшее время, возможности практической реализации вычислительных методов пока что трудно себе представить, настолько сложной представляется эта задача. Перспективы теоретического развития тоже кажутся весьма значительными. Можно надеяться, что дело не ограничится открытием ряда более или менее оригинальных алгоритмов. Может быть, удастся глубже понять принципы измерения в квантовой механике, построить что-то вроде информационной динамики, обнаружить некие общие принципы возникновения, распространения и рассеяния информации, выделить классические вычисления как стабильное подмножество квантовых, понять причины потери когерентности на макроуровне, причины возникновения принципа возрастания энтропии. В любом случае влияние квантовой теории информации на науку и общество в целом может оказаться огромным.

В заключение я хочу поблагодарить О.А. Хрусталева за внимание к работе и полезные обсуждения.

Список литературы

[1] Richard P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics 21*, 1982, 467–488.

[2] Р.Ф. Фейнман. Квантовомеханические ЭВМ. УФН, 1986, т. 149, вып. 4, с. 671–688.

[3] Paul Benioff. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. *Journal of Statistical Physics 22*, 1980, 563–591.

[4] David Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London* A400, 1985, 97–117.

[5] Архив статей в электронном виде (e-prints) http://xxx.lanl.gov, раздел “квантовая физика”, quant-ph. Российское зеркало http://xxx.itep.ru.

[6] Quantum information and quantum computation at IBM. On-line обзор доступен по адресу http://www.research.ibm.com/quantuminfo/

[7] В.В.Белокуров, О.Д.Тимофеевская, О.А.Хрусталев. Квантовая телепортация — обыкновенное чудо. Ижевск, НИЦ “Регулярная и хаотическая динамика”, 2000.

[8] Andrew Steane. 1997. Quantum computing. LANL archive http://xxx.lanl.gov preprint quant-ph/9708022.

[9] А. Китаев, А. Шень, М. Вялый. Классические и квантовые вычисления. М.: МЦНМО, ЧеРо, 1999. В Internet доступна по адресу http://www.mccme.ru/free-books/

[10] Международный научный журнал "Квантовый компьютер", издается НИЦ "Регулярная и Хаотическая Динамика". Сетевая версия http://rcd.ru:8101/qc/

[11] Лаборатория физики квантовых компьютеров Физико-Технического института РАН (ФТИАН). Сетевой адрес лаборатории http://qc.ipt.ac.ru

[12] David P. DiVincenzo. Quantum Computation. Science, vol. 270, 13 October 1995, p. 255.

[13] David Deutsch, Adriano Barenco, and Artur Ekert. March 28, 1995. Universality in Quantum Computation, Proc. R. Soc. Lond. A **449**, 669-677.

[14] Wooters W.K. and Zurek W.H. A single quantum cannot be cloned. Nature **299**, 1982, 802.

[15] A.Einstein, B.Podolsky, and N.Rosen. Phys. Rev. **47**, 777 (1935).

[16] Bell J.S. On the Einstein-Podolsky-Rosen paradox. Physics **1**, 1964, 195–200.

[17] Bell J.S. On the problem of hidden variables in quantum theory. Rev. Mod. Phys. **38**, 1966, 447-452.

[18] Bennett C.H., Brassard G., Crepeau C., Jozsa R., Peres A. and Wootters W.K. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys. Rev. Lett. **70**, 1895–1898 (March 29, 1993). В сети Internet статья доступна по адресу
http://www.research.ibm.com/quantuminfo/teleportation/teleportation.ps

[19] Quantum teleportation. On-line обзор исследовательской группы фирмы IBM доступен по адресу http://www.research.ibm.com/quantuminfo/teleportation

[20] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, A. Zeilinger. Experimental Quantum Teleportation. Nature, December 10, 1997. Статья доступна по адресу http://info.uibk.ac.at/c/c7/c704/qo/ftppage.html

[21] Internet-версия журнальной статьи, Scientific American, "Beam me up", December 22, 1997, доступна по адресу http://www.sciam.com/explorations/122297teleport/

[22] Shor P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, in *Proc. 35th Annual Symp. on Foundations of Computer Science*, Santa Fe, IEEE Computer Society Press 1994; revised version 1995a e-print quant-ph/9508027 at LANL archive http://xxx.lanl.gov

[23] Shor P.W. Fault-tolerant quantum computation. In *Proceedings of the Symposium on the Foundations of Computer Science.* Los Alamitos, CA: IEEE Press (1996); e-print quant-ph/9605011.

[24] Aspect A. Testing Bell's inequalities. Europhys. News. **22**, 1991, 73–75.

[25] Kwiat P.G., Mattle K., Weinfurter H., Zeilinger A., Sergienko A. and Shih Y. New high-intencity source of polarization-entangled photon pairs. Phys. Rev. Lett. **75**, 1995, 4337–4341.

[26] A.Yu. Kitaev. Fault-tolerant quantum computations by anyons. (July 10, 1997) e-print quant-ph/9707021.

[27] Grover L.K. Quantum mechanics helps in searching for a needle in a haystack. Phys. Rev. Lett. **79**, 1997, 325–328.

[28] Internet-архивы по квантовой криптографии можно посмотреть по адресам:
http://eve.physics.ox.ac.uk/NewWeb/Research/crypto.html
http://www.cs.mcgill.ca/~crepeau/CRYPTO/Biblio-QC.html

[29] Zbinden H. et al. Interferometry with Faraday mirrors for quantum cryptography. Elect. Lett. 7, 1997.

[30] Isaac L. Chuang, Neil Gershenfeld, Mark Kubinec. Experimental Implementation of Fast Quantum Searching. PRL April 13, 1998. On-line версия
http://squint.stanford.edu/qc/local.html

Neil Gershenfeld, Isaac L. Chuang. Quantum computing with Molecules. Scientific American, June 1998. On-line версия
http://www.sciam.com/1998/0698issue/0698gershenfeld.html

Рукопись поступила 6 марта 2001 г.

И.А. Качаев
Квантовые вычисления.

Оригинал-макет подготовлен с помощью системы LaTeX.
Редактор Л.Ф.Васильева. Технический редактор Н.В.Орлова.

Подписано к печати 15.03.2001. Формат 60 × 84/8. Офсетная печать.
Печ.л. 3. Уч.-изд.л. 2,3. Тираж 130. Заказ 53. Индекс 3649.
ЛР №020498 17.04.97.

ГНЦ РФ Институт физики высоких энергий
142284, Протвино Московской обл.

Индекс 3649

П Р Е П Р И Н Т 2001-12, И Ф В Э, 2001