Июнь 1999 г. *Том 169, № 6*

УСПЕХИ ФИЗИЧЕСКИХ НАУК

КОНФЕРЕНЦИИ И СИМПОЗИУМЫ

Научная сессия Отделения общей физики и астрономии Российской академии наук

(27 января 1999 г.)

27 января 1999 г. в Институте физических проблем им. П.Л. Капицы РАН состоялась научная сессия Отделения общей физики и астрономии РАН. На сессии были заслушаны доклады:

1. **Валиев К.А.** (Физико-технологический институт РАН, Москва). *Квантовые компьютеры: можно ли их сделать "большими"?*
2. **Молотков С.Н.** (Физический институт им. П.Н. Лебедева РАН, Москва). *Квантовая криптография.*

Краткое содержание первого доклада публикуется ниже.

PACS number: 03.67.Lx

Квантовые компьютеры: можно ли их сделать "большими"?

К.А. Валиев

Идеи о возможности построения квантового компьютера восходят к работам Р. Фейнмана 1982 – 1986 гг. [1 – 3]. Рассматривая вопрос о вычислении эволюции квантовых систем на цифровом компьютере, Фейнман обнаружил "нерешаемость" (noncomputability) этой задачи: оказывается, что ресурсы памяти и быстродействия классических машин недостаточны для решения квантовых задач. Например, система из n квантовых частиц с двумя состояниями (спины 1/2) имеет 2^n базисных состояний; для ее описания необходимо задать (и записать в память ЭВМ) 2^n амплитуд этих состояний. Отталкиваясь от этого негативного результата, Фейнман высказал предположение, что, вероятно, "квантовый компьютер" будет обладать свойствами, которые позволят решать на нем квантовые задачи [1 – 3].

"Классические" компьютеры построены на транзисторных схемах, обладающих нелинейными зависимостями между входными и выходными напряжениями. По существу, это бистабильные элементы; например, при низком входном напряжении (логический "0") входное напряжение высокое (логическая "1"), и наоборот.

Такой бистабильной транзисторной схеме в квантовом мире можно сопоставить двухуровневую квантовую частицу: состоянию E_0, $|\Psi_0\rangle$ припишем значения логического "0"$\equiv|0\rangle$, состоянию $|\Psi_1\rangle$, $E_1 > E_0$ — значение логической "1"$=|1\rangle$. Переходам "0"$\rightarrow$"1" в бистабильной транзисторной схеме здесь будут соответствовать переходы с уровня на уровень: $|0\rangle \leftrightarrow |1\rangle \equiv E_0 \leftrightarrow E_1$. Однако квантовый бистабильный элемент, получивший название кубит, обладает новым, по сравнению с классическим, свойством суперпозиции состояний: он может быть в любом суперпозиционном состоянии $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, где α, β — комплексные числа, $|\alpha|^2 + |\beta|^2 = 1$. Состояния квантовой системы из n двухуровневых частиц имеют в общем случае вид суперпозиций $|\Psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i|\Psi_i\rangle$ 2^n базовых состояний $|\Psi_i\rangle = |i_1 i_2 \ldots i_n\rangle$, $i_k = 0; 1$. В конечном счете квантовый принцип суперпозиции состояний позволяет придать квантовому компьютеру принципиально новые "способности".

Доказано, что квантовая ЭВМ может быть построена всего из двух элементов (вентилей): однокубитового элемента $Q(\theta, \varphi)$ и двухкубитового элемента контролируемое НЕ(CNOT). Матрица 2×2 элемента $Q(\theta, \varphi)$ имеет вид

$$Q(\theta, \varphi) = \begin{pmatrix} \cos\dfrac{\theta}{2} & -\mathrm{i}\exp(-\mathrm{i}\varphi)\sin\dfrac{\theta}{2} \\ -\mathrm{i}\exp(\mathrm{i}\varphi)\sin\dfrac{\theta}{2} & \cos\dfrac{\theta}{2} \end{pmatrix}. \quad (1)$$

Вентиль $Q(\theta, \varphi)$ описывает поворот вектора состояния кубита от оси z к полярной оси, заданной углами θ, φ. Если θ, φ — иррациональные числа, то многократным применением $Q(\theta, \varphi)$ вектору состояния можно придать любую наперед заданную ориентацию. Именно в этом заключается "универсальность" однокубитового вентиля в форме (1). В частном случае $\theta = \pi/2$, $\varphi = 0$ получаем однокубитовый логический элемент НЕ(NOT): НЕ$|0\rangle = |1\rangle$, НЕ$|1\rangle = |0\rangle$. При физической реализации элемента НЕ необходимо воздействовать на квантовую частицу (кубит) импульсом извне, переводящим кубит из одного состояния в другое. Вентиль контролируемое НЕ исполняют, воздействуя на два взаимодействующих между собой кубита: при этом посредством взаимодействия один кубит контролирует эволюцию другого. Переходы под влиянием внешних импульсов хорошо известны в импульсной магнитно-резонансной спектроскопии. Вентиль НЕ соответствует перевороту спина $I_z \leftrightarrow -I_z$ под действием импульса $Y(\pi)$

(вращение намагниченности вокруг оси Y на угол π). Вентиль CNOT выполняется на двух спинах 1/2 с гамильтонианом $H = \omega_i I_{zi} + A_{ij} I_{zi} I_{zj} + H'_{\text{imp}}(t)$ (спин I_j контролирует I_i). CNOT выполняется в три шага: импульс $Y_i(\pi/2)$+свободная прецессия в течение времени $\tau = \pi/A_{ij}$+импульс $X_i(\pi/2)$. Если $I_{zj} = 1/2$ (контролирующий кубит в состоянии $|0\rangle$), то при указанных воздействиях контролируемый кубит совершает переходы $I_{zi} \to I_{xi} \to I_{yi} \to I_{zi}$ (или $-I_{zi} \to -I_{xi} \to -I_{yi} \to -I_{zi}$). Если же $I_{zj} = -1/2$ (контролирующий кубит в состоянии $|1\rangle$), то результат эволюции контролируемого кубита будет другим: $I_{zi} \to I_{xi} \to -I_{yi} \to -I_{zi}$ $(-I_{zi} \to -I_{xi} \to \to I_{yi} \to I_{zi})$. Таким образом, спин I_i эволюционирует поразному при $I_{zj} = 1/2$ и $I_{zj} = -1/2$: $|00\rangle \to |00\rangle$, $|01\rangle \to |01\rangle$, $|10\rangle \to |11\rangle$, $|11\rangle \to |10\rangle$; здесь в $|i_1 i_2\rangle$ i_1 — состояние контролирующего кубита.

При рассмотрении вопроса о реализации квантового компьютера на тех или иных квантовых системах в первую очередь исследуют реализуемость и свойства элементарных вентилей НЕ и контролируемое НЕ.

Для дальнейшего полезно также ввести однокубитовое преобразование Адамара (Hadamard):

$$\mathrm{H}|0\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)\,, \quad \mathrm{H}|1\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big)\,.$$

В технике магнитного резонанса эти вентили осуществляются импульсами $\pi/2$:

$$Y\left(\frac{\pi}{2}\right) I_z \to I_x\,, \quad Y\left(\frac{\pi}{2}\right)(-I_z) \to -I_x\,.$$

Схема квантового компьютера представлена на рисунке. До начала работы компьютера все кубиты (квантовые частицы) должны быть приведены в состояние $|0\rangle$, т.е. в основное состояние. Это условие само по себе не тривиально. Оно требует или глубокого охлаждения (до температур порядка миликельвина), или применения методов поляризации. Систему n кубитов в состоянии $|00\ldots0\rangle$ можно считать регистром памяти, приготовленным для записи входных данных и проведения вычислений. Кроме этого регистра обычно предполагают существование дополнительных (вспомогательных) регистров, необходимых для записи промежуточных результатов вычислений. Запись данных осуществляется путем того или иного воздействия на каждый кубит компьютера. Примем, например, что над каждым кубитом регистра совершается преобразование

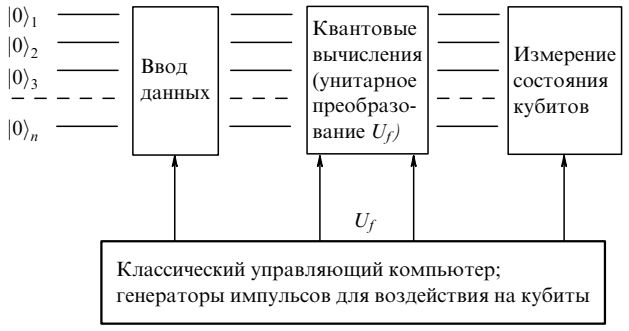


Схема квантового компьютера.

Адамара:

$$\begin{aligned}\mathrm{H}_n \otimes \mathrm{H}_{n-1} \otimes \ldots \otimes \mathrm{H}_1 |0_1 0_2 \ldots 0_n\rangle = \\ = 2^{-n/2} \prod \big(|0\rangle_1 + |1\rangle_1\big) \ldots \big(|0\rangle_n + |1\rangle_n\big) = \\ = 2^{-n/2} \sum_{x=0}^{2^n-1} |x\rangle = |\Psi_1\rangle\,. \end{aligned} \tag{2}$$

В результате система перешла в состояние суперпозиции из 2^n базисных состояний с амплитудой $2^{-n/2}$. Каждое базисное состояние представляет собой двоичное число x, от $x = 0(|00\ldots0\rangle)$ до $x = 2^n - 1(|11\ldots1\rangle)$. Отметим, что горизонтальные линии на рисунке обозначают оси времени.

Выполнение алгоритма $f(x)$ совершается путем унитарного преобразования U_f суперпозиции $|\Psi_1\rangle$. U_f представляет собой унитарную матрицу размерности 2^n. При физическом осуществлении посредством импульсных воздействий на кубиты извне матрица $U_f(2^n)$ должна быть представлена как векторное произведение матриц размерности 2 $(U(2))$ и 2^2 $(U(2^2))$. Последние могут быть выполнены последовательным воздействием на единичные кубиты $(U(2))$ или пары кубитов $(U(2^2))$:

$$U_f = U_k \otimes U_{k-1} \otimes \ldots \otimes U_0\,. \tag{3}$$

Количество сомножителей в этом разложении определяет длительность (и сложность) вычислений $f(x)$. Все U_l в (3) выполняются с применением операций NOT, CNOT, H (или их разновидностей).

Замечательно, что линейный унитарный оператор U_f действует одновременно на все члены $|x\rangle$ суперпозиции $|\Psi_1\rangle = 2^{-n/2} \sum_{x=0}^{2^n-1} |x\rangle$:

$$U_f|\Psi_1\rangle|0\rangle = 2^{-n/2} \sum_{x=0}^{2^n-1} U_f|x\rangle|0\rangle = 2^{-n/2} \sum_{x=0}^{2^n-1} |x\rangle|f(x)\rangle\,. \tag{4}$$

Результаты вычисления $|f(x)\rangle$ записываются в запасном регистре, который перед применением U_f находился в состоянии $|0\rangle$. За один прогон вычислительного процесса мы получаем значения искомой функции f при всех значениях аргумента $x = 0, \ldots, 2^n - 1$. Этот феномен получил название квантового параллелизма.

Измерение результата вычислений сводится к проецированию вектора суперпозиции в (4) на вектор одного из базисных состояний $|x\rangle$:

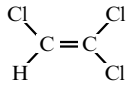
$$\mathrm{R}2^{-n/2} \sum_{x=0}^{2^n-1} |x\rangle|f(x)\rangle = 2^{-n/2}|x\rangle|f(x)\rangle\,. \tag{5}$$

Здесь проступает одно из слабых мест квантового компьютера: число $|x\rangle$ в процессе измерения "выпадает" по закону случая. Чтобы найти $f(x^*)$ при заданном x^*, надо много раз провести вычисления и измерения, пока случайно не выпадет $|x^*\rangle|f(x^*)\rangle$. Если входные данные структурированы, так что в $|\Psi_1\rangle = \sum_{x=0}^{2^n-1} c_x|x\rangle$ амплитуда c_{x^*} вектора $|x^*\rangle$ может иметь значение, близкое к 1, тогда при измерении мы найдем сразу состояние $|x^*\rangle|f(x^*)\rangle$ с вероятностью $|c_{x^*}|^2 \sim 1$. Если x^* заранее не известно и нет возможности структурировать входные данные, то можно предусмотреть в алгоритме операции, определяющие нужный член суперпозиции и путем итераций вычислительного процесса увеличивающие до значений ~ 1 амплитуды этого члена суперпозиции. Так построен,

например, алгоритм Гровера поиска некоторого объекта в неструктурированной базе данных [4].

При анализе унитарной эволюции квантовой системы, совершающей вычислительный процесс, выявляется важность физических процессов типа интерференции. Унитарные преобразования совершаются в пространстве комплексных чисел, и сложение фаз этих чисел носит характер интерференции. Известна продуктивность преобразований Фурье в явлениях интерференции и спектроскопии. Оказалось, что и в квантовых алгоритмах неизменно присутствуют преобразования Фурье. Преобразование Адамара является простейшим дискретным фурье-преобразованием. Вентили типа NOT и CNOT могут быть осуществлены непосредственно на интерферометре Маха–Зендера с использованием явления интерференции фотона и вращения его вектора поляризации [5].

Исследуются различные пути физической реализации квантовых компьютеров. Модельные эксперименты по квантовому компьютингу выполнены на импульсном ядерном магнитно-резонансном спектрометре [6–10]. В этих моделях работало два или три спина (кубита), например два спина ядер ^{13}C и один спин протона в молекуле трихлорэтилена [10]



Однако в этих опытах квантовый компьютер был "ансамблевым": выходные сигналы компьютера сложены большим числом молекул в жидком растворе ($\sim 10^{20}$).

К настоящему времени высказаны предложения о реализации квантовых компьютеров на ионах и молекулах в ловушках в вакууме [11], на ядерных спинах в жидкостях (см. выше), на ядерных спинах атомов ^{31}P в кристаллическом кремнии [12], на спинах электронов в квантовых точках, созданных в двумерном электронном газе в гетероструктурах GaAs [13], на переходах Джозефсона [14]. Как видим, в принципе, квантовый компьютер можно построить на атомных частицах в вакууме, жидкости, кристаллах. При этом в каждом случае предстоит преодолеть те или иные препятствия, однако среди них можно выделить несколько общих, обусловленных принципами действия кубитов в квантовом компьютере. Поставим задачу создать полномасштабный квантовый компьютер, содержащий, скажем, 10^3 кубитов (хотя и при $n = 100$ квантовый компьютер может стать полезным инструментом).

1. Нужно найти способы "инициализации" кубитов компьютера в состояние $|0 \ldots 0\rangle$. Для спиновых систем в кристаллах очевидно применение сверхнизких температур и сверхсильных магнитных полей. Применение поляризации спинов накачкой может оказаться полезным при одновременном применении охлаждения и больших магнитных полей.

Для ионов в вакуумных ловушках сверхнизкое охлаждение ионов (атомов) достигается лазерными методами. Очевидна также необходимость холодного и сверхвысокого вакуума.

2. Необходимо иметь технологию избирательного воздействия импульсами на любой выбранный кубит. В области радиочастот и спинового резонанса это означает, что каждый спин должен обладать своей резонансной частотой (в терминах спектроскопического разрешения). Различия резонансных частот для спинов в молекулах обусловлены химическими сдвигами для спинов одного изотопа и одного элемента; необходимые различия частот имеются для спинов ядер различных элементов. Однако здравый смысл подсказывает, что эти дарованные природой различия резонансных частот вряд ли достаточны, чтобы работать с 10^3 спинов.

Более перспективными представляются подходы, когда можно управлять извне резонансной частотой каждого кубита. В предложении о кремниевом квантовом компьютере кубитом служит ядерный спин примесного атома ^{31}P. Частота резонанса определяется константой A сверхтонкого взаимодействия ядерного и электронного спинов $H_{IS} = A\mathbf{I} \times \mathbf{S}$ атома ^{31}P. Электрическое поле на наноэлектроде, находящемся над атомом ^{31}P, поляризует атом и изменяет константу A (соответственно резонансную частоту ядерного спина). Таким образом, наличие электрода встраивает кубит в электронную схему и настраивает его резонансную частоту.

3. Для выполнения операции CNOT_{ij} (контролируемое НЕ) необходимо взаимодействие между кубитами i и j вида $A_{ij}I_{zi}I_{zj}$. Такое взаимодействие возникает между спинами ядер в молекуле, если ядра i и j разделены одной химической связью. В принципе, необходимо иметь возможность выполнять операцию CNOT_{ij} для любых пар кубитов $i \neq j$. Иметь физическое взаимодействие кубитов одного масштаба величины и по принципу "все со всеми" в природной среде вряд ли возможно. Очевидна потребность в способе настройки среды между кубитами извне путем введения электродов с управляемым потенциалом. Таким путем можно создать, например, перекрытие волновых функций электронов в соседних квантовых точках и возникновение взаимодействия вида $J(V)S_i \times S_j$ между спинами электронов [13]. Перекрытие волновых функций электронов соседних атомов ^{31}P обусловливает возникновение взаимодействия вида $A_{ij}\mathbf{I}_i \times \mathbf{I}_j$ между ядерными спинами [12].

Чтобы обеспечить операцию CNOT_{ij}, где i и j — отдаленные кубиты, между которыми взаимодействие вида $A_{ij}\mathbf{I}_i \times \mathbf{I}_j$ отсутствует, необходимо применить в компьютере операцию обмена состояниями по цепочке $j \to l \to k \to \ldots \to p$, так что $A_{ip}I_iI_p$ обеспечивает операцию CNOT_{ij}, поскольку состояние I_p совпадает с состоянием I_j.

4. В ходе выполнения унитарного преобразования, соответствующего избранному алгоритму, кубиты компьютера подвергаются воздействию со стороны среды; в результате амплитуды и фазы вектора состояния кубита испытывают случайные изменения — декогерензацию. По существу, декогерензация — это релаксация тех степеней свободы частицы, которые используются в кубите. Время декогерензации τ_d равно времени релаксации. В ядерном магнитном резонансе в жидкостях времена T_1 и T_2 релаксации составляют 1–10 с. Для ионов в ловушках с оптическими переходами между уровнями E_0 и E_1 временем декогерензации выступают время спонтанного излучения и время столкновений с остаточными атомами. Очевидно, что декогерензация — это серьезное препятствие квантовому компьютингу: начатый вычислительный процесс приобретает черты случайности по истечении времени декогерензации.

Однако можно достичь устойчивого квантового вычислительного процесса в течение сколь угодно долгого времени $\tau \gg \tau_d$, если систематически использовать методы квантового кодирования и коррекции ошибок (фазовых и амплитудных) [15]. Доказано, что при относительно невысоких требованиях к безошибочному выполнению элементарных операций типа NOT и CNOT (вероятность ошибки не более 10^{-5}) методы квантовой коррекции ошибок (QEC) обеспечивают устойчивую работу квантового компьютера.

Возможно и активное подавление процесса декогеренизации, если над системой кубитов проводить периодические измерения. Измерение с большой вероятностью обнаружит частицу в "правильном" состоянии, а малые случайные изменения вектора состояния при измерении коллапсируют (квантовый эффект Зенона [16, 17]). Однако трудно пока сказать, насколько полезным может быть такой прием, поскольку такие измерения сами по себе могут воздействовать на вычислительный процесс и нарушить его.

5. Состояния кубитов после завершения вычислительного процесса должны быть измерены, чтобы определить результат вычисления. Сегодня нет освоенной технологии таких измерений. Очевиден, однако, путь поисков такой технологии: надо использовать методы усиления в квантовом измерении. Например, состояние ядерного спина I передается электронному спину S; от последнего зависит орбитальная волновая функция; зная орбитальную волновую функцию, можно организовать передачу зарядов (ионизацию); присутствие или отсутствие заряда одиночного электрона можно обнаружить классическими электрометрическими методами [12, 13]. Большую роль в этих измерениях будут играть, вероятно, методы зондовой силовой микроскопии.

К настоящему времени открыты квантовые алгоритмы, приводящие к экспоненциальному ускорению вычислений по сравнению с вычислениями на классическом компьютере. К ним относится алгоритм Шора определения простых множителей больших (многоразрядных) чисел [18]. Эта чисто математическая проблема тесно связана с жизнью общества, так как на "невычислимости" таких множителей построены современные шифровальные коды. Именно это обстоятельство вызвало сенсацию, когда был открыт алгоритм Шора. Для физиков важно, что и решение квантовых задач (решение уравнения Шрёдингера для многочастичных систем) экспоненциально ускоряется, если использовать квантовый компьютер [19].

Наконец, очень важно, что в ходе исследований задач квантового компьютинга подвергаются новому анализу и экспериментальной проверке основные проблемы квантовой физики: проблемы локальности, реальности, дополнительности, скрытых параметров, коллапса волновой функции.

Идеи квантового компьютинга и квантовой связи возникли спустя сто лет после рождения первоначальных идей квантовой физики. Возможность построения квантовых компьютеров и систем связи показана выполненными к настоящему времени теоретическими и экспериментальными исследованиями. Квантовая физика "достаточна" для проектирования квантовых компьютеров на различной "элементной базе". Квантовые компьютеры, если их удастся построить, будут техникой XXI века. Для их изготовления потребуется создание и развитие новых технологий на нанометровом и атомном уровне размеров. Эта работа может занять, по-видимому, несколько десятилетий. Построение квантовых компьютеров было бы еще одним подтверждением принципа неисчерпаемости природы: природа имеет средства для осуществления любой корректно сформулированной человеком задачи. В заключение укажем на некоторые обзоры по квантовому компьютингу [20–22].

Список литературы

1. Feynman R P *Int. J. Theor. Phys.* **21** 467 (1982)
2. Feynman R P *Opt. News* (Feb.) 11 (1985)
3. Feynman R P *Found. Phys.* **16** (6) 507 (1986)
4. Grover L K *Phys. Rev. Lett.* **79** 325 (1997)
5. Adami C, Cerf N J, quant-ph/9806048, 14 June (1998)
6. Chuang I L et al. *Nature* (London) **393** 143 (1998)
7. Chuang I L et al. *Proc. R. Soc. London Ser. A* **454** 447 (1998)
8. Cory D G et al. *Proc. Natl. Acad. Sci. USA* **94** 1634 (1997)
9. Jones J A et al. *Nature* (London) **393** 344 (1998)
10. Cory D G et al., quant-ph/9802018, 6 Feb. (1998); *Phys. Rev. Lett.* **81** 2152 (1998)
11. Cirac J I, Zoller P *Phys. Rev. Lett.* **74** 4091 (1995)
12. Kane B E *Nature* (London) **393** 133 (1998)
13. Loss D, Di Vincenzo D P *Phys. Rev. A* **57** 120 (1998)
14. Shnirman A et al. *Phys. Rev. Lett.* **79** 2371 (1997); Schön G, Shnirman A, Makhlin Yu, cond-mat/9811029, 3 Nov. (1998)
15. Preskill J, quant-ph/9705031, v3, 26 Aug. (1997)
16. Халфин Л А *УФН* **160** (10) 185 (1990)
17. Braunstein S L, Smolin J A, quant-ph/9604036, v2, 22 Okt. (1996)
18. Shor P, in *Proc. 35th Annual Symposium on Foundations of Computer Science* (Los Alamitos, Calif.: IEEE Computer Soc. Press, 1994) p. 124
19. Zalka C *Proc. R. Soc. London Ser. A* **454** 313 (1998)
20. Steane A, quant-ph/9708022, v2, 24 Sept. (1997); *Rep. Prog. Phys.* **61** 117 (1998)
21. Rieffel E G, Polak W, quant-ph/9809016, 8 Sept. (1998)
22. Aharonov D, quant-ph/9812037, 15 Dec. (1998), in *Annual Reviews of Computational Physics* (Ed. D Stauffer) Vol. 6 (Singapore: World Scientific, 1998)