КВАНТОВЫЕ КОМПЬЮТЕРЫ
от идеи к реализации

К. Валиев

Квантовая механика, описывающая, казалось бы, далекий от нас микромир, все активнее вторгается в практические сферы человеческой деятельности. Появляется все больше приборов, основанных на квантовомеханических принципах - от квантовых генераторов до микроэлектронных устройств. Видимо, пришел черед и вычислительной техники - компьютеры, построенные на квантовых вычислительных элементах, обещают совершить переворот в ряде направлений вычислительной математики. Конечно, это еще проекты, но вполне возможно, что через какое-то время квантовый компьютер станет инструментом столь же привычным, как сегодня - обычный компьютер.

ПРИНЦИП СУПЕРПОЗИЦИИ В КВАНТОВОМ МИРЕ

На рубеже 19–20 веков возникла великая физическая теория – квантовая механика. За четверть века Планк, Бор, Шредингер, Гейзенберг и др. создали новый математический аппарат и решили основные задачи квантового описания объектов микромира.

Один из важнейших принципов квантовой механики – принцип суперпозиции состояний: если квантовая система может существовать в состояниях $|\Psi_1\rangle$ и $|\Psi_2\rangle$, то она может столь же «законно» пребывать в состояниях, являющихся их суперпозицией: $a|\Psi_1\rangle+b|\Psi_2\rangle$, a, b – комплексные «амплитуды», $|a|^2+|b|^2=1$, $|\Psi\rangle$ - вектор состояния системы. Математически принцип суперпозиции – это следствие линейности уравнения Шредингера, основного уравнения квантовой механики. Принцип суперпозиции противоречит представлениям человека, сложившимся при наблюдении "классических" явлений в макромире, т.е. он контринтуитивен. Это хорошо иллюстрирует пример парадоксального кота Шредингера: если кот может пребывать в состояниях |жив⟩ и |мертв⟩, то согласно принципу суперпозиции, он способен существовать и в состоянии $|\Psi\rangle = a|$жив$\rangle + b|$мертв$\rangle$, т.е. быть одновременно и живым, и мертвым. Отметим, что контринтуитивны и такие свойства квантовых частиц, как корпускулярно-волновой дуализм, коллапс волновой функции при измерении и др.

Важнейший вопрос в квантовой механике – измерение параметров квантовой частицы. Суперпозиционное состояние $|\Psi\rangle = a|$жив$\rangle + b|$мертв$\rangle$ математически можно рассматривать как вектор в Гильбертовом пространстве, где базисные векторы |жив⟩ и |мертв⟩ суть орты осей координат, a и b – проекции вектора $|\Psi\rangle$ на эти координатные оси. При измерении аппаратура так воздействует на частицу, что вектор состояния проецируется на ось |жив⟩ или на ось |мертв⟩. При этом проекции вектора a и b – амплитуды вероятности обнаружить частицу в том или ином состоянии: $P_{жив}=|a|^2$, $P_{мертв}=|b|^2$. Числовые значения вероятностей P находят статистически, путем многократных измерений идентичных систем.

КУБИТ – КВАНТОВЫЙ БИТ

На основании принципа суперпозиции все приборы можно разделить на «квантовые» и «классические». Состояния квантового прибора подчиняются принципу суперпозиции, а классического – нет. Эволюция состояний квантового прибора происходит согласно квантовому уравнению Шредингера. С этой точки зрения все квантовые системы являются квантовыми приборами. Если с различными состояниями квантового прибора связать информационные понятия и символы, его можно использовать для представления информационного процесса. В результате из квантовых приборов формируется квантовая элементная база квантовых информационных систем. Наибольший интерес представляют квантовые системы с двумя состояниями, позволяющие строить информационные системы с двоичным исчислением.

Квантовую систему с двумя состояниями, способную нести один бит информации, называют ***кубит (qubit)*** [1]. Если эти состояния $|\Psi_0\rangle$ и $|\Psi_1\rangle$ связаны с двумя уровнями энергии $E_0<E_1$, то говорят о двухуровневой системе. В других случаях состояния системы могут различаться поляризацией (фотона) или фазой (сверхпроводника). Квантовая система может быть макроскопической (сверхпроводники, сверхтекучие жидкости, бозе-газ), отдельной атомной частицей или колебательной модой. Все они применимы для образования кубита.

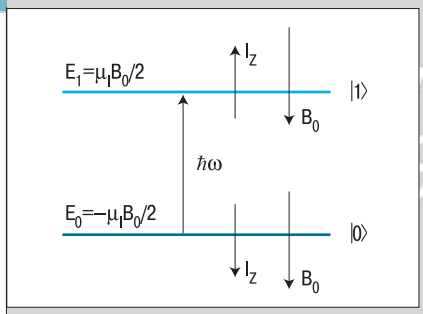

Рис. 1. Кубит на основе состояний спинов

Простейшим является спиновый кубит, построенный на двух состояниях (уровнях энергии) спина I= ±1/2: $E_0=-\mu_1 B_0/2$, $E_1=\mu_1 B_0/2$, $|\Psi_{E_0}\rangle=|0\rangle$, $|\Psi_{E_1}\rangle=|1\rangle$ (рис. 1) [2].

ЭЛЕМЕНТАРНЫЕ ОПЕРАЦИИ НАД КУБИТАМИ В КВАНТОВОМ КОМПЬЮТЕРЕ

Доказано, что любой квантовый алгоритм можно разложить на последовательность элементарных преобразований состояний отдельных кубитов и пар кубитов (одно- и двухкубитовые преобразования, или «вентили»). Пусть начальное состояние кубита – суперпозиция $|\Psi(0)\rangle=a(0)|0\rangle+b(0)|1\rangle$. После преобразования, совершенного за время t, состояние кубита будет $|\Psi(t)\rangle=a(t)|0\rangle+b(t)|1\rangle$. Такое преобразование называют «поворотом» вектора $|\Psi(0)\rangle$ к $|\Psi(t)\rangle$. Чтобы построить квантовый компьютер, нужно научиться совершать преобразования двух типов: любые повороты вектора $|\Psi(0)\rangle$ любого заданного кубита и поворот одного кубита под контролем другого [3].

Повороты кубита выполняются под воздействием внешнего резонансного поля. Квантовая эволюция состояния кубита $|\Psi(t)\rangle$ описывается уравнением Шредингера

$$i\hbar\frac{\partial|\Psi(t)\rangle}{\partial t}=\hat{H}_1(t)|\Psi(t)\rangle,$$

где $\hat{H}_1(t)=\mu\varepsilon_0\cos(\omega t+\varphi)$ – энергия взаимодействия дипольного момента μ кубита и внешнего резонансного электрического поля (например, лазера). Приведенное уравнение легко решается, его результат:

$$\begin{cases}a(t)=\cos\left(\frac{\theta}{2}\right)a(0)-e^{i\varphi}\sin\left(\frac{\theta}{2}\right)b(0)\\ b(t)=-ie^{i\varphi}\sin\left(\frac{\theta}{2}\right)a(0)+\cos\left(\frac{\theta}{2}\right)b(0),\end{cases}$$

$\theta=\Omega t$, $\Omega=\mu\varepsilon_0/2\hbar$.

Пусть в начальный момент кубит находился в состоянии $|0\rangle$ (т.е. $a(0)=1$, $b(0)=0$). Тогда $a(t)=\cos(\theta/2)$, $b(t)=-ie^{i\varphi}\sin(\theta/2)$, а вероятности найти кубит в момент t в состояниях $|0\rangle$ и $|1\rangle$ равны

$P_0=|a(t)|^2=\cos^2(\theta/2)=1/2(1+\cos\Omega t)$,

$P_1=|b(t)|^2=\sin^2(\theta/2)=1/2(1-\cos\Omega t)$.

Кубит с частотой Ω (частота Раби) переходит из состояния $|0\rangle$ в состояние $|1\rangle$, а в промежуточные моменты времени находится в состоянии $|\Psi(t)\rangle=a(t)|0\rangle+b(t)|1\rangle$. Контролируя длительность и фазу внешнего воздействия, можно перевести кубит в состояние, описываемое любой суперпозицией. При $\Omega t=\pi/2$ получаем преобразование Адамара H:

$$|0\rangle\xrightarrow{H}\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle),$$

$$|1\rangle\xrightarrow{H}\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle),$$

а при $\Omega t=\pi$ – операцию отрицания HE:

$|0\rangle\xrightarrow{HE}|1\rangle$, $|1\rangle\xrightarrow{HE}|0\rangle$.

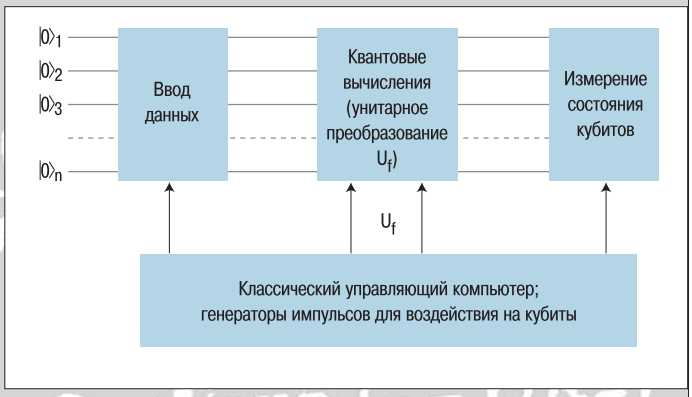

Рис. 2. Структурная схема квантового компьютера

В двухкубитовом преобразовании поворот $V(\theta,\varphi)$ контролируемого кубита совершается только когда состояние контролирующего кубита – $|1\rangle$. Для такого преобразования необходимо физическое взаимодействие между контролирующим и контролируемым кубитами хотя бы во время выполнения операции. Специалисты предлагают как использовать природное взаимодействие кубитов (например, контактное спин-спиновое взаимодействие ядер в молекулах), так и включать его внешним воздействием (напряжениями на электродах). Если $V(\theta,\varphi)$=HE, реализуется операция *Контролируемое HE* (CNOT), $|\Psi_1\rangle\rightarrow|\Psi_1\rangle\oplus|\Psi_2\rangle$, где $\oplus$ – знак сложения по модулю 2. Подробно преобразования состояний кубитов описаны в [4–7].

КВАНТОВЫЙ КОМПЬЮТЕР

Структура квантового компьютера представлена на рис. 2. Его квантовую часть составляют n кубитов. К каждому из них может быть приложено селективное воздействие резонансными импульсами внешнего переменного поля. Генераторами полей и адресацией их излучения управляет классический компьютер. Перед началом вычислительного процесса все n кубитов необходимо инициализировать – привести в состояние $|0\rangle$. Это не тривиальная операция. Если в качестве кубитов используются спины ядер, для их инициализации потребуется охлаждение до температур порядка 1 мкК или поляризация спинов накачкой. Посредством одно- и двухкубитовых вентилей вводятся данные и исполняется алгоритм. Результат вычисления записывается в конечном квантовом состоянии кубитов. Чтобы его считать, эти состояния необходимо измерить.

Важнейшее свойство квантового компьютера – квантовый параллелизм. Составим квантовый алгоритм U_f вычисления функции f(x). Инициализируем все кубиты компьютера в состояние $|0\rangle$. Над каждым из n используемых в вычислениях кубитов произведем преобразование Адамара

$$|0\rangle\xrightarrow{H}\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle).$$

Результатом будет суперпозиция 2^n базисных состояний системы из n кубитов с одинаковыми вероятностями $2^{-n/2}$. Базисные состояния $|x\rangle$ представляют собой двоичные числа от 0 до 2^n-1. Произведем над $|x\rangle$ преобразование U_f, соответствующее вычислению функции f(x). В результате за один прогон алгоритма U_f получим суперпозицию, содержащую значения функции f от огромного числа значений аргумента x (от 0 до 2^n-1). В этом и заключается феномен квантового параллелизма. Число значений аргумента x определяется только количеством n задействованных в вычислительном процессе кубитов.

Однако при измерении конечного состояния компьютера суперпозиция состояний его кубитов разрушается. Возникает вопрос: в чем польза от квантового параллелизма, если в результате можно получить (в данном случае – с вероятностью 2^{-n}) только одно из значений f(x′)? Для вычисления функции при другом аргументе x″ инициализацию, вычисление, измерение придется повторять сначала. Тем не менее, квантовый параллелизм находит практическое применение. Дело в том, что нас может интересовать какое-то одно из значений функции f(x′). Если как-либо увеличить вероятность интересующего состояния $|f(x')\rangle$ до значений, близких к 1, то нужное нам значение f(x′) было бы найдено при первом же измерении с вероятностью ~1.

$$|\Psi_1\rangle=\sum_{x=0}^{2^n-1}C_x|x\rangle,$$

Состояние системы кубитов Ψ_1 в более общем виде выглядит как где C_x – комплексные числа, $C_x=|C_x|\exp(i\varphi)$. В алгоритм вычисления можно включить операции над векторами $|x\rangle$, изменяющие фазу:

$$\sum_{x=0}^{2^n-1}C_x|x\rangle\rightarrow\sum_{x=0}^{2^n-1}e^{i\varphi_x}C_x|x\rangle.$$

$|x\rangle\rightarrow\exp(i\varphi_x)|x\rangle$. Тогда

Вычислительный процесс носит характер интерференции – комплексные амплитуды базисных состояний образуются при сложении комплексных чисел. Изменяя фазы амплитуд, можно добиться, чтобы амплитуды интересующих состояний складывались конструктивно, а других – деструктивно. Так построен знаменитый алгоритм Гровера поиска в неструктурированной базе данных [8]. Некоторые авторы вообще рассматривают квантовый компьютер как сложное интерференционное устройство, усматривая его вычислительную мощь именно в интерференции векторов состояний [6].

ПУТИ СОЗДАНИЯ КВАНТОВЫХ КОМПЬЮТЕРОВ

Наиболее впечатляющие результаты получены в экспериментах по квантовым вычислениям методом импульсного ядерного магнитного резонанса (ЯМР) в молекулярных жидкостях (ансамблевый квантовый компьютер) [9, 10]. Предлагается также использовать ионы в ловушках в вакууме [11], ядерные спины атомов ^{31}P в монокристаллическом кремнии [12], спины одиночных электронов в квантовых точках в двумерном газе в полупроводниковых гетероструктурах [13], атомы в резонаторах электромагнитного поля [14]. Возможно создание кубитов на состояниях сверхпроводников, разделенных

переходами Джозефсона и различающихся числом зарядов [15–17] или фазой сверхпроводников [18]. Одно из достоинств применения сверхпроводников – использование структур с наноразмерами, технология которых в значительной мере разработана. Интересно, что модели квантовых компьютеров могут быть построены на линейных оптических элементах (делители пучка, поляризаторы, фазовращатели, интерферометры). В последнем случае одиночный фотон проходит через оптическую систему. Его волновая функция охватывает всю оптическую систему, интерферируя на выходных интерферометрах. Обнаружение фотона в том или ином интерферометре есть измерение результата вычисления. Таким образом, оптическая модель квантового компьютера весьма наглядно демонстрирует интерференционную природу квантового вычислительного процесса [19].

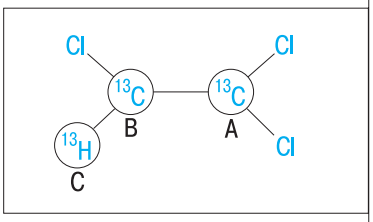

Рис. 3. Система из трех кубитов на основе молекулы трихлорэтилена

В ансамблевом ядерном магнитнорезонансном квантовом компьютере кубитами выступают спины I=1/2 ядер водорода (протоны) и углерода ^{13}C в молекулах жидкости. Так, в молекуле трихлорэтилена (рис. 3) спины ядер двух атомов ^{13}C и одного протона образуют три кубита. Два атома ^{13}C химически неэквивалентны, поэтому частоты их ЯМР ω_A и ω_B будут различны во внешнем постоянном магнитном поле B_0. Протон имеет третью резонансную частоту ω_C. Подавая импульсы переменного магнитного поля на частотах ω_A, ω_B, ω_C, можно селективно управлять квантовой эволюцией любого из этих спинов (выполнять однокубитовые вентили). Между спинами ядер, разделенных одной химической связью ^{1}H – ^{13}C и ^{13}C – ^{13}C, имеется магнитное контактное взаимодействие, энергия которого $H_I=2J_{AB}I_{ZA}I_{ZB}+2J_{BC}I_{ZB}I_{ZC}$.

Взаимодействия $I_A \leftrightarrow I_B$ и $I_B \leftrightarrow I_C$ позволяют строить двухкубитовые вентили $CNOT_{AB}$, $CNOT_{BA}$, $CNOT_{BC}$, $CNOT_{CB}$ (первый индекс обозначает контролирующий, второй – контролируемый кубит). Операции $CNOT_{AC}$ и $CNOT_{CA}$ основываются на процессах обмена состояниями соседних спинов.

Поскольку молекул в пробирке импульсного ЯМР-спектрометра достаточно много (~10^{20}), можно говорить об ансамбле параллельно работающих квантовых компьютеров. Это позволяет решить сложные проблемы инициализации и измерения состояния кубитов по завершении процесса вычислений. Состояния $|0\rangle$ и $|1\rangle$ кубита в конечном состоянии определяются по знаку (фазе) линии резонансного поглощения: при $|0\rangle$ наблюдается, например, линия поглощения, а при $|1\rangle$ – излучения.

На спиновых двух- и трехкубитовых квантовых компьютерах уже реализованы модельный квантовый алгоритм Дойча-Иозса по определению типа дискретной функции от дискретного аргумента [20], алгоритм Гровера поиска в базе данных [21], алгоритм с квантовой коррекцией ошибок [22]. Эти результаты произвели большое впечатление на научное сообщество. Однако построить квантовый компьютер данного типа с числом кубитов порядка 10^3 вряд ли возможно, так как трудно представить столько ядер с различимыми частотами магнитного резонанса.

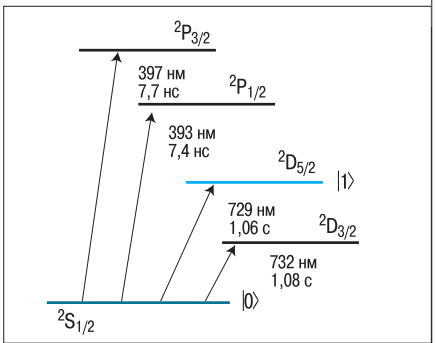

Рис. 4. Энергетическая диаграмма кубита на основе ионов Ca^+.
Числа у стрелок показывают длину волны лазера, вызывающего переход, и время жизни иона на соответствующем уровне

Интересна идея построения квантового компьютера на ловушках в вакууме. Ионы или атомы размещают в области минимума потенциала, создаваемого системой электродов и электромагнитных полей. Тепловое движение атомов замораживают методом лазерного охлаждения. Изначально данную технологию развивали для создания квантовых стандартов частоты. Но сегодня большой интерес к ней связан с квантовыми компьютерами. Эксперименты в этом направлении ведут в Лос-Аламосе и Национальном институте стандартов США [1, 23]. "Подвешенные" в вакууме ионы и атомы являются максимально изолированными от окружающего мира квантовыми частицами. Внешняя связь сохраняется только для их удержания в ловушке (посредством электродов с напряжениями) и управления квантовой эволюцией (сфокусированные лазерные пучки).

Энергетическая диаграмма кубита на основе ионов Ca^+ приведена на рис. 4. Уровни $^2S_{1/2}$ (основной) и $^2D_{5/2}$ (метастабильный) выбраны как логические $|0\rangle$ и $|1\rangle$. Сфокусированные на ионе импульсы лазерного излучения с длиной волны 729 нм выполняют однокубитовые эволюции. Другие переходы используются для доплеровского лазерного охлаждения ($^2S_{1/2} \rightarrow {}^2P_{1/2}$, 397 нм; $^2D_{3/2} \rightarrow {}^2P_{1/2}$, 866 нм), лазерного охлаждения колебаний ионов в ловушке (рамановское рассеяние на переходе $^2S_{1/2} \rightarrow {}^2D_{3/2}$), а также при считывании информации.

Однако в квантовом компьютере на основе ионных ловушек сложно реализовать двухкубитовые вентили CNOT. Расстояние между ионами в ловушке (10–20 мкм) достаточно велико по сравнению с атомными размерами, поэтому прямое взаимодействие между внутренними кубитами ионов практически отсутствует. Но поскольку эти ионы участвуют в колебательном движении, можно ввести дополнительный кубит. Его логический $|0\rangle$ соответствует колебательному движению (одной из мод) в основном состоянии, логическая $|1\rangle$ – колебательному состоянию с одним фононом. В результате внутренние кубиты отдаленных ионов взаимодействуют через колебательное движение системы ионов. Однако достаточно сложно организовать преобразования, включающие переходы между уровнями энергии электронов внутри атомов и переходы между колебательными состояниями цепочки ионов,. Неудивительно, что в опытах по созданию квантового компьютера на ионах в ловушке пока не наблюдается быстрого прогресса.

Большой интерес вызывают проекты твердотельной реализации элементов квантовых компьютеров, поскольку можно использовать накопленный опыт микроэлектронной технологии. При этом сами компьютеры имели бы сходство с чипами микросхем. В [12] в качестве кубитов предлагается использовать спины I=1/2 ядер фосфора ^{31}P в монокристаллическом кремнии (рис. 5). Частотой магнитного резонанса можно управлять, подавая на наноэлектрод над атомом электрическое напряжение V – оно поляризует электронную оболочку атома и изменяет константу A так называемого сверхтонкого взаимодействия электронного S и ядерного I спинов атома (энергия взаимодействия $H_1=A(V)\cdot I\cdot S$). Так достигается селективный доступ внешнего резонансного магнитного поля к спину атомного ядра. Структура с единичным атомом, встроенным в заданную точку под электродом, отдаленно напоминает полевой транзистор. Если в последнем затвор управляет движением электронов проводимости в канале, в случае кубита напряжения на затворе воздействуют на движение электрона внутри атома, поляризуя атом и изменяя резонансную частоту кубита.

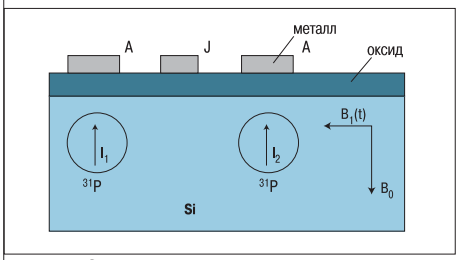

Рис. 5. Структура кремниевого квантового чипа.
Напряжения на электродах A управляют частотой магнитного резонанса ядерных спинов; с помощью напряжения на электроде J «включается» взаимодействие спинов $A|_1|_2$, необходимое для операции Контролируемое НЕ

Однако на этом пути немало проблем. Так, необходимо организовать производство бесспиновых монокристаллических слоев кремния (без спинового изотопа ^{29}Si), разместить единичные атомы ^{31}P в заданных точках

кремния, вырастить бездефектный барьерный слой, создать систему управляющих электродов с наноразмерами. Нужна низкотемпературная электроника, управляющая напряжениями на электродах. Кристалл следует охладить до температур ~1 мК, чтобы все спины ядер ^{31}P оказались в основном состоянии ($|0\rangle$). Достаточно сложная проблема – измерение конечных состояний ядерных спинов (одним из вариантов ее решения могла бы стать реализация идеи ансамблевого квантового компьютера).

До создания полномасштабного (10^3–10^4 кубитов) квантового компьютера предстоит пройти большой путь. Пока неясно, какой вариант окажется предпочтительнее. Широкомасштабные поиски идут по всему фронту физики, постоянно возникают новые идеи и предложения. Оптимисты полагают, что среди них могут найтись «прорывные», которые приблизят долгожданный момент. По-видимому, одной из таких идей можно считать метод квантовой коррекции ошибок.

КВАНТОВАЯ КОРРЕКЦИЯ ОШИБОК

У квантового компьютера есть грозный противник. Имя ему – декогерентизация. Кубиты нельзя полностью изолировать от внешнего мира, они подвержены шумовому воздействию среды. Флуктуации напряжений на электродах, шумовые токи, неточности выполнения самих импульсных воздействий на кубиты – все это вносит неконтролируемые ошибки в фазы и амплитуды состояний кубитов при вычислительном процессе. По истечении времени декогерентизации квантовых состояний системы кубитов контролируемый вычислительный процесс прекратится. А время декогерентизации, как правило, меньше, чем нужно для выполнения сложного алгоритма, состоящего из многих (~10^9) вентилей.

Ситуация казалась тупиковой. Однако выход был найден в квантовой коррекции ошибок [24]. В теории обычных компьютеров хорошо известны методы кодирования $|0\rangle$ и $|1\rangle$ большим числом битов. При возникновении ошибки анализ кодовых комбинаций позволяет ее найти и исправить. Такой подход удалось разработать в квантовом варианте, где ошибки могут быть фазовыми и амплитудными. Выяснилось, что если вероятность ошибки при выполнении одной элементарной операции ниже некоторого порога, вычислительный процесс может длиться сколь угодно долго – операции квантовой коррекции исправляют больше ошибок, чем вносят. Этот вывод очень важен – по существу он имеет силу теоремы существования полномасштабного квантового компьютера.

ТЕХНОЛОГИЯ АТОМНЫХ РАЗМЕРОВ

Технологии с атомным разрешением уже довольно зрелы, работа с отдельными атомами является экспериментальной реальностью. Можно утверждать, что на рубеже 2020–2030 годов начнется изготовление микросхем, работающих на квантовых принципах. Три сегодняшних технологии могут оказаться базовыми: молекулярная эпитаксия, нанолитография и зондовая микроскопия. Молекулярная эпитаксия позволяет создавать совершенные моноатомные слои кристаллов, т.е. атомный размер достигается по толщине. Велико значение и электронно-лучевой нанолитографии с разрешением 1–10 нм. Методы зондовой микроскопии позволяют наблюдать поверхность тел с атомным разрешением. В то же время зонды используют как атомные манипуляторы – они позволяют перемещать, доставлять, снимать атомы с поверхности. Зонды могут служить и катализаторами локальных поверхностных химических реакций (окисление, травление, осаждение материала), доставляя энергию локального возбуждения (химической активации) в форме электрического тока, напряжения, фотонов, механической энергии (деформации). Наконец, зондовые методы применимы для измерения состояния атомных частиц.

РОЛЬ КВАНТОВЫХ КОМПЬЮТЕРОВ

Для квантовых компьютеров пока разработано небольшое число алгоритмов, но уже получены ошеломляющие результаты. В 1994 году Шор создал алгоритм факторизации – определения простых множителей больших чисел [25]. На классическом компьютере для этого требуется экспоненциально большое число операций. На невозможности решить данную задачу за приемлемое время на современных компьютерах основан алгоритм кодирования секретной информации RSA. Шор показал, что квантовый компьютер способен решить задачу факторизации за n^3 операций, где n – разрядность числа. Коэффициент ускорения решения при больших n может быть весьма велик. Такое же ускорение имеет место для ряда задач квантовой физики [26]. В то же время установлено, что многие алгоритмы, неплохо выполняемые на классических компьютерах, не ускоряются на квантовом [27].

Таким образом, квантовые компьютеры не могут полностью заменить существующий компьютерный мир, а лишь дополняют его. В алгоритме Шора, по-видимому, впервые обнаружен феномен, когда класс сложности задачи коренным образом изменяется в зависимости от того, на каких физических принципах основан вычислительный процесс. Свое слово должны сказать математики – им предстоит разработать квантовые алгоритмы и определить, для каких задач достигается ускорение и каким оно будет.

В заключение отметим, что в ходе разработки идей квантовой информатики углубляются знания и о самой квантовой физике, уясняются ее основные понятия и принципы. Кроме того, квантовые методы позволяют создать квантовый канал связи и передавать по нему информацию. Но об этом сюжете квантовой информатики мы расскажем в будущем.

ЛИТЕРАТУРА

1. **Schumacher B.W.** – Phys. Rev. A51 (1995), p. 2738–2747.
2. **Hughes R.J.** et al. – Fortschr. Phys. 46 (1998) 45, p. 329–361.
3. **Barenco A.** et al. – Phys. Rev. A52 (1995), p. 3457.
4. **Steane A.** Quantum Computing. – Quant-ph/9708033, v.2, 1997, Sept. 24.
5. **Rieffel. E., Polak W.** An Introduction to Quantum Computing for non-physicists. – Quant-ph/9809016, 1998, Sept. 24.
6. **Aharonov D.** Quantum Computation. – Quant-ph/9812037, 1998, Dec.15.
7. **Preskill J.** Lecture Notes for Physics 229/ – Quantum Information and Computation, 1998, Sept.
8. **Grover L.K.** Proceedings of the Twenty Eight Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, 1996. p. 212–219.
9. Cory D.G., Fahmy A.F., Havel T.F. Proc. of the 4th Workshop on Physics and Computation (Complex Systems Institute, Boston, New England), 1996.
10. **Gershenfeld N.A., Chuang I.L.** – Science, 1997, p. 275, 350–356.
11. **Cirak J.I., Zoller P.** – Phys. Rev. Lett. 74, 1995, p.4091–4094.
12. **Kane B.E.** – Nature 393, 1998, May 14.
13. **Loss D., Vincenzo D.P.** – Phys. Rev., A57, №1, p. 120–126.
14. **Cirac J.I.** et al. – Phys. Rev. Lett. 78, 1997, p. 3221.
15. **Shnirman A., Schön G., Hermon Z.** – Phys. Rev. Lett. 79, 1997, p. 2371–2374.
16. **Schön G., Shnirman A., Makhlin Y.** – Cond-mat/9811029, 1998, Nov., 3.
17. **Averin. D.V.** – Solid State Comm. 105, 1998, p. 659–664.
18. **Ioffe L.B.** et al. – Cond-mat/9809116, 1999, v.2.
19. **Adami C., Cert N.J.** – Quant-ph/9806048, 1998, June 14.
20. **Chuang I.L.** et al. – Nature 393, 1998, p. 143–146.
21 **Jones J.A., Mosca M., Hansen R.S.** – Nature, 393, 1998, p. 344–346.
22. **Cory D.G.** et al. – Quant-ph/9802018, 1998, Feb 6.
23. **Wineland D.J.** et al. – J. Res. Natl. Inst. Stand. Tech. 103, 1998, p. 259.
24. **Steane A.** – Proc. Roy. Soc. of London A, 452, 1996, p. 2551–2577.
25. **Shor P.W.** – SIAMJ. Comp., 26, 1997, № 5, p. 1484–1509.
26. **Zalka C.** – Proc. Roy. Soc. Lond. A 454, 1998, p. 313–322.
27. **Ozhigov Y.** – Quant-

Квантовый компьютер сделал реальный скачок

Трое ученых — Исаак Чуанг (Лос-Аламосская национальная лаборатория), Нийл Гершенфельд (Массачусетский технологический институт) и Марк Кубинек (Берклийский калифорнийский университет) — впервые при комнатной температуре загрузили данные и считали результат выполнения алгоритма Гровера сконструированным ими квантовым компьютером. Компьютер выполнен на молекулах хлороформа. И хотя его демонстрационное устройство содержит всего два квантовых разряда, это событие знаменательно уже тем, что впервые продемонстрирована возможность работы квантового компьютера без необходимости установления температуры, близкой к абсолютному нулю.

pubs.cmpnet.com/eet/news/98/1006news/quantum.html