

# ПРИРОДА

№ 12, 2002 г.

Валиев К.А., Кокин А.А.

## **От кванта к квантовым компьютерам**

© “Природа”

Использование и распространение этого материала  
в коммерческих целях  
возможно лишь с разрешения редакции



Сетевая образовательная библиотека “VIVOS VOCO!”  
(грант РФФИ 00-07-90172)

[vivovoco.nns.ru](http://vivovoco.nns.ru)  
[vivovoco.rsl.ru](http://vivovoco.rsl.ru)  
[vivovoco.usu.ru](http://vivovoco.usu.ru)  
[www.ibmh.msk.su/vivovoco](http://www.ibmh.msk.su/vivovoco)

# От кванта к квантовым компьютерам

К.А.Валиев, А.А.Кокин

**Т**ехника XXI в. рождается из синтеза новых идей в математике, физике, информатике и технологии. Яркий пример тому — работа над созданием квантовых компьютеров. Они позволят решать некоторые задачи, недоступные даже самым мощным современным суперкомпьютерам, обеспечат более высокую скорость многих сложных вычислений; сообщения, посланные по линиям квантовой связи, невозможно будет ни перехватить, ни скопировать. Построение квантовых компьютеров в очередной раз подтвердило бы, что Природа имеет средства для осуществления любой корректно сформулированной задачи.

## У истоков

14 декабря 1900 г. немецкий физик и будущий нобелевский лауреат М.Планк доложил на заседании Берлинского физического общества об открытии квантовых свойств теплового излучения. Этот день считается днем рождения квантовой физики: родилось понятие *кванта* энергии, и в число других фундаментальных постоянных вошла постоянная Планка  $h = 6.62 \cdot 10^{-34}$  Дж·с. В декабре 2000 г. весь научный мир отметил столетний юбилей постоянной Планка, а с ним и юбилей квантовой физики.

© К.А.Валиев, А.А.Кокин



**Камиль Ахметович Валиев**, академик, директор Физико-технологического института РАН, руководитель лаборатории физики квантовых компьютеров, заведующий кафедрой физических и технологических проблем микроэлектроники Московского физико-технического института и кафедрой квантовой информатики Московского государственного университета им.М.В.Ломоносова. Область научных интересов — квантовая теория магнитного резонанса, физика полупроводников и технология микроэлектроники, квантовая информатика.



**Александр Александрович Кокин**, кандидат физико-математических наук, старший научный сотрудник той же лаборатории. Занимается квантовой теорией полупроводников, методами моделирования элементов микро- и нанозлектроники, физикой квантовых компьютеров.

Открытие Планка, появившаяся затем в 1905 г. теория фотоэлектрического эффекта А.Эйнштейна, создание в 1913 г. Н.Бором первой квантовой теории атомных спектров и обнаружение в 1925 г. Дж.Уленбеком и С.Гаудсмитом спина у электрона стимулировали дальнейшее бурное развитие теории и экспериментальных исследований квантовых процессов.

Уже в 1925 г. В.Гейзенберг предложил матричный вариант квантовой механики, а в 1926 г. Э.Шрёдингер составил свое знаменитое волновое

уравнение для описания движения электрона во внешнем поле. В это же время Э.Ферми и П.Дирак получили квантово-статистическое распределение для электронного газа, учитывающее при заполнении отдельных квантовых состояний принцип, который сформулировал тогда же В.Паули. Анализ квантово-механической задачи о движении электрона в периодическом электрическом поле кристаллической решетки, выполненный Ф.Блохом в 1928 г., показал, что электронный энергетический спектр в кристаллическом твердом теле имеет зонную структуру. Это привело к существенным изменениям наших представлений о Природе вообще и о твердом теле в частности.

К 1930 г. было установлено, что в отличие от металлов, для полупроводников, как и для диэлектриков, характерно наличие в зонном энергетическом спектре запрещенной зоны между потолком наиболее высоко лежащей заполненной зоны и дном самой нижней пустой. Однако у полупроводников ширина запрещенной зоны достаточно мала, и при комнатных температурах через нее за счет теплового возбуждения с заметной вероятностью могут перебрасываться электроны. В 1931 г. А.Вильсон показал, что проводимость в полупроводниках имеет место лишь при наличии незаполненных зон. Ток, создаваемый электронами не полностью заполненных зон, оказывается эквивалентным току, создаваемому некоторыми квазичастицами с положительным зарядом — дырками (последние соответствуют свободным от электронов состояниям в зоне). Полупроводники, в зависимости от преобладания электронов или дырок, стали относить к электронному ( $n$ ) или дырочному ( $p$ ) типам проводимости.

Таким образом, выяснилось, что характерные для полупроводников свойства обусловлены зонным характером электронного энергетического спектра, т.е. отражают *квантовые свойства* твердого тела. В результате уже в начале 30-х годов были заложены надежные теоретические основы для дальнейшего развития физики полупроводников, и в частности контактных явлений в  $p$ - $n$ -переходах. Интерес к этим переходам стал возрастать с тех пор, как Б.И.Давыдов в 1938 г. опубликовал первую работу по теории явления выпрямления и возникновения фотоэдс в таких структурах.

## От теории — к технологии

Прикладное значение  $p$ - $n$ -переходов было должным образом оценено не сразу. Электроника того времени развивалась исключительно на основе вакуумных электронных ламп, и специалисты-электронщики мало интересовались полупроводниками. Перелом наступил после изобретения в 1948 г. сотрудниками Bell Laboratories (США) Дж.Бардином и У.Браттейном точечно-контактного кристаллического триода на основе германия  $n$ -типа (названного ими *транзистором*) и появления в 1949 г. работы У.Шокли по квантовой теории плоскостных диодов и транзисторов. Именно тогда начался беспрецедентный качественный прорыв в полу-

проводниковой электронике (за что данные авторы и были отмечены Нобелевской премией).

Важную роль в развитии полупроводниковой электроники сыграли разработка кремниевой планарной технологии, основанной на контролируемой диффузии примесей в локальных областях приповерхностного слоя кремниевой пластины, и создание в 1959 г. на фирме «Fairchild Electronics» (США) первого планарного биполярного транзистора на кремнии. Рождение микроэлектроники принято относить именно к этой дате. Несколько позже был сделан первый полевой транзистор со структурой металл—окисел—полупроводник (МОП-транзистор) на кремнии, выполненный также по планарной технологии. Он стал впоследствии одним из основных структурных единиц больших интегральных схем — элементной базы современных цифровых электронных компьютеров. Первые советские планарные биполярные транзисторы были изготовлены в НИИ «Пульсар» в Москве и в НИИ молекулярной электроники в Зеленограде в 1965 г. В том же году начал готовить специалистов в области микроэлектроники новый вуз в Зеленограде — Московский институт электронной техники.

Успехи в развитии кремниевой микроэлектроники наглядно выражаются так называемым законом Г.Мура, согласно которому число транзисторов в кристалле одной интегральной схемы в течение первых 15 лет (начиная с 1959 г.) удваивалось каждый год, а затем такое удвоение происходило приблизительно за полтора года. По экспоненциальному закону уменьшаются со временем и характерные размеры элементов схем, достигшие к началу XXI в. порядка 10 нм. Если тенденция уменьшения размеров сохранится и дальше, то к атомным масштабам (менее 1 нм) твердотельная технология перейдет уже через 10—15 лет. Тактовая частота, с которой работают современные процессоры, поднялась до 2 ГГц и продолжает увеличиваться, растет и производительность многопроцессорных вычислительных систем. Фактом стала производительность в  $10^{12}$  операций в секунду (1 терафлоп) недавно созданной в России ЭВМ; в США сейчас ведутся работы по обеспечению производительности уже в 10 терафлопов.

Основой оперативной памяти современного цифрового компьютера служит совокупность макроскопических полупроводниковых элементов — *классических битов* с двумя базисными логическими булевыми состояниями «0» и «1». Процессор строится из логических элементов-вентилей, которые производят локальные операции над своими исходными состояниями для того, чтобы получить в результате определенное конечное состояние на выходе. Примером простейшего классического вентиля является известный в микроэлектронике КМОП-инвертор (состоящий из пары МОП-транзисторов с противоположным типом проводимости канала), который осуществляет операцию НЕ, т.е. изменяет состояние «0» на «1» или наоборот.

Логические состояния в каждом бите — это, например, два значения тока в определенном проводнике или потенциала на нем (реальной основой элемент-

ной базы компьютера стали транзисторы). В ходе вычисления потоки информации взаимодействуют нелинейным образом, строго определенным для каждой логической операции, и благодаря этому преобразуются. Соответствующие процессы происходят на физическом уровне и с носителями информации — токами и напряжениями. Существенно, что информация представляется с помощью макроскопических некогерентных классических величин. В этом смысле современные цифровые компьютеры, несмотря на исходную квантовую природу процессов, происходящих в полупроводниковых элементах, рассматриваются как *классические*.

Последние два десятилетия ознаменовались также освоением иных, не кремниевых материалов и интенсивными поисками новых физических принципов для приборов с характерными размерами, сравнимыми с длиной волны де Бройля (~20 нм). Для последних существенны более тонкие по сравнению с массивными полупроводниками квантовые свойства: это квантовые ямы, нити и точки. Такие структуры потребовали новых технологических подходов — родилась нанотехнология.

Среди прочих примером наноэлектронных полупроводниковых приборов могут служить транзисторы с резонансным туннелированием, в том числе на горячих электронах, и одноэлектронные транзисторы, характеристики которых существенным образом определяются свойствами электронных квантовых состояний и квантовым характером эволюции этих состояний. Однако по-прежнему при работе вентилях, построенных на наноэлектронных, как и на традиционных микроэлектронных приборах, используются классические булевы логические состояния, а передаваемая информация обрабатывается с помощью некогерентных классических сигналов, носителями которых являются электрические токи и напряжения.

При переходе в область наноэлектронных устройств пришлось столкнуться с проблемой уменьшения энергии, рассеиваемой в процессе вычислительных операций. Мысль о возможности *логически обратимых* операций, не сопровождающихся потерей энергии, впервые высказал Р.Ландауер еще в 1961 г. Теоретический фундамент решения проблемы заложил Ч.Беннетт: он показал, что универсальный цифровой компьютер типа вычислительной машины Тьюринга может быть построен на логически и термодинамически обратимых вентилях таким образом, что энергия будет рассеиваться только за счет необратимых периферийных процессов ввода информации в машину (приготовление исходного состояния) и соответственно вывода из нее (считывание результата). Сейчас уже существуют и конкретные схемотехнические реализации подобных вентилях.

## Экскурсия в гильбертово пространство

Совсем недавно прогресс микроэлектроники и вы-

числительной техники виделся на пути дальнейшего увеличения степени интеграции, быстроедействия интегральных схем и использования логически обратимых вентилях. Кардинально новые идеи и принципы построения вычислительных устройств должны были прийти из других областей физики, подобно тому как в электронику из физики полупроводников пришел принцип действия полупроводникового транзистора. Отправной точкой стал пересмотр самого подхода к представлению информации — эту роль возложили на волновую функцию квантовой системы. Носителями информации должны стать квантовые ячейки, именуемые *кубитами* (quantum bit или qubit), такого рода, что связанная с ними некоторая физическая величина может принимать два значения (у системы есть два *базисных состояния*). Но если возможных значений характеристики по-прежнему два, чем же кубит отличается от классического бита? Различие между ними принципиально. Дело в том, что классический бит всегда пребывает в каком-то одном из двух булевых состояний: «0» или «1», т.е. последние заняты с вероятностями либо  $P(0) = 1$ , либо  $P(1) = 1$ . Кубит же может находиться в некотором состоянии, представляющем собой суперпозицию базисных квантовых состояний. Чтобы вложить в рассуждения конкретный физический смысл, заметим, что в качестве кубитов рассматриваются различные квантовые двухуровневые системы, и в частности искомым характеристикой могут быть электронные и ядерные спины со спиновым квантовым числом  $I = 1/2$ . Далее мы ограничимся в основном сис-

темами ядерных спинов, преимуществ которых при использовании в качестве кубитов впоследствии коснемся.

Уровни энергии отдельного ядерного спина в магнитном поле  $\mathbf{B}$  изображены на рис.1. Им соответствуют собственные состояния  $|0\rangle$  и  $|1\rangle$ , которые суть ба-

зисные состояния кубита. Суперпозиция этих базисных состояний описывается так называемым *вектором состояния* в специальном двумерном комплексном *гильбертовом пространстве* состояний:

$$|\psi\rangle = c_0 |0\rangle + c_1 |1\rangle, \quad |c_0|^2 + |c_1|^2 = 1.$$

Базисные векторы состояния  $|0\rangle$  и  $|1\rangle$  в этом пространстве являются единичными ортами, а комплексные амплитуды  $c_0$ ,  $c_1$  можно рассматривать как проекции вектора состояния на направление базисных состояний — ортов (рис.2).

Вектор состояния может изменяться весьма тонко, принимая произвольные направления в гильбертовом пространстве, а вероятности найти спин в том или ином базисном состоянии выражаются через модули коэффициентов  $c_0$ ,  $c_1$ :  $P(0) = |c_0|^2$ ,  $P(1) = |c_1|^2$ . Это и означает, что спин может находиться в базисных состояниях  $|0\rangle$  и  $|1\rangle$  одновременно. Помимо вероятнос-

тей  $P(0)$  и  $P(1)$  заполнения базисных состояний  $|0\rangle$

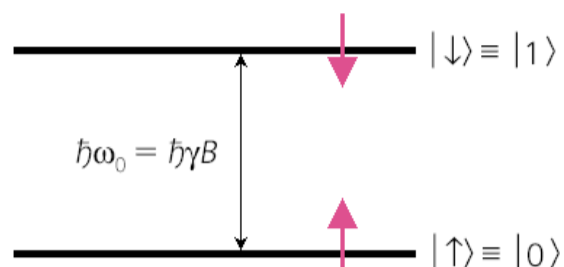


Рис.1. Уровни энергии ядерного спина с  $I = \frac{1}{2}$  с гиромангнитным отношением  $\gamma > 0$  в магнитном поле  $\mathbf{B}$  (положительное значение проекции спина соответствует направлению его

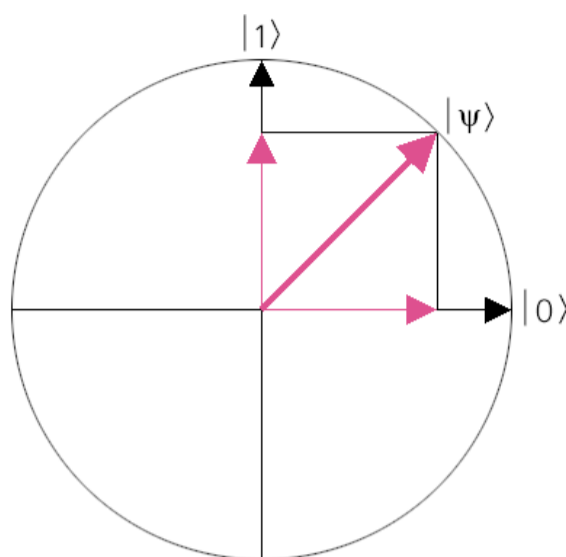


Рис.2. Вектор состояния суперпозиции  $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$  и его проекции на направление базисных состояний (ортов) в двумерном гильбертовом пространстве.

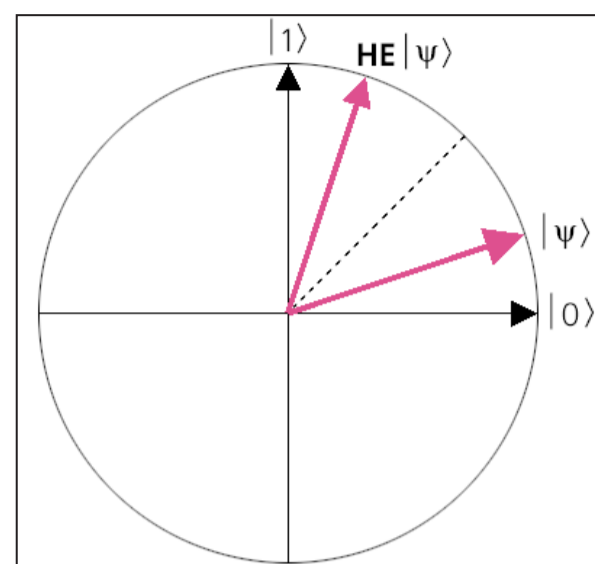


Рис.3. Поворот вектора состояния  $|\psi\rangle$  в двумерном гильбертовом пространстве при унитарной операции HE над кубитом.

и  $|1\rangle$ , состояние кубита характеризуется *когерентными* или *интерференционными* слагаемыми в вероятности состояния  $|\psi\rangle$ , которые определяются произведениями комплексных амплитуд  $c_0c_1^*$  и  $c_0^*c_1$ . Именно здесь кроется принципиальное различие классического и квантового битов.

Пока мы говорили об одном отдельно взятом кубите; для двух кубитов гильбертово пространство становится четырехмерным, и произвольный вектор состояния характеризуется уже четырьмя комплексными коэффициентами. Размерность пространства и число коэффициентов для описания произвольной суперпозиции базисных состояний растет с числом кубитов  $L$  по показательному закону, т.е. как  $2^L$ . Уже при  $L = 100$  это число достигает громадного значения примерно  $10^{30}$ , что делает практически невозможной полное моделирование такой физической системы на классическом цифровом компьютере.

Идею о *квантовых вычислениях* впервые высказал российский математик Ю.И.Манин в 1980 г. [1], но активно обсуждаться она стала лишь после опубликования в 1982 г. статьи американского физика-теоретика, нобелевского лауреата Р.Фейнмана [2]. Последний обратил внимание на то, что эффективное моделирование  $L$ -кубитовых квантовых систем можно осуществить, если выполнять логические операции на квантовых системах, которые действуют с использованием суперпозиции состояний многих кубитов. Он предложил и первую схему квантового обратимого компьютера [3].

Поскольку законы квантовой физики на микроскопическом уровне суть линейные и обратимые, то и соответствующие квантовые логические устройства, производящие операции с когерентными (чистыми) квантовыми состояниями отдельных кубитов, оказываются также обратимыми. Квантовые вычислитель-

ные операции сводятся просто к определенным поворотам вектора состояния в  $2^L$ -мерном гильбертовом пространстве без изменения его длины. Такие преобразования называются *унитарными*.

Например, однокубитовая унитарная операция, поворачивающая вектор состояния из положения  $|0\rangle$  на  $45^\circ$  в плоскости  $|0\rangle, |1\rangle$ , приводит к суперпозиции  $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$  (рис.2). В качестве другого примера можно

привести простейшую унитарную операцию HE над одним кубитом: в отличие от аналогичной классической она производится над состоянием суперпозиции базисных состояний  $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$ , в которой происходит «обмен» базисными состояниями  $|0\rangle \rightarrow |1\rangle$  и  $|1\rangle \rightarrow |0\rangle$ . В результате этой операции получим  $|\psi\rangle = c_0|1\rangle$

+  $c_1|0\rangle$ , т.е. вектор состояния переходит в положение, симметричное относительно биссектрисы угла между направлениями ортов (рис.3).

Выполнять подобные логические операции над кубитами можно с помощью соответствующим образом подобранных внешних воздействий, которыми управляют обычные, классические, компьютеры.

## В чем сила квантовых вычислений?

Элементарный шаг при квантовых вычислениях — унитарная операция над  $L$ -кубитовой суперпозицией состояний регистра из  $L$  кубитов — выполняется так,

что сразу все  $2^L$  комплексные амплитуды обрабатываются параллельно. В классическом компьютере подобное действие потребовало бы  $2^L$  отдельных элементарных шагов для обработки каждой амплитуды. Именно это свойство — *квантовый параллелизм* в работе квантовых устройств — приводит к экспоненциальному ускорению вычислительного процесса. В нем заключается одно из главных преимуществ квантовых компьютеров по сравнению с классическими цифровыми. Вычисление приобретает характер интерференции: комплексные амплитуды состояний многих кубитов могут складываться конструктивно и деструктивно, образуя необходимые суперпозиции квантовых состояний. Так построен, например, знаменитый алгоритм поиска в неструктурированной базе данных, придуманный Л.Гровером.

Особое свойство квантовых состояний, принципиально отличающее их от классических, — *запутывание* (entanglement), когда взаимодействие между кубитами порождает такую когерентную суперпозицию квантовых состояний нескольких элементов, которая не сводится к произведению состояний отдельных кубитов. Примером может служить запутанное состояние двух кубитов типа  $\frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle)$  (так называ-

емое состояние Эйнштейна—Подольского—Розена).

Запутанные состояния играют очень важную роль в различных процессах передачи и обработки квантовой информации. Хотя само понятие было введено еще Шрёдингером под названием «Verschränkung» (скрещивание) в 1935 г., внимание оно привлекло к себе лишь с 1993 г. Тогда обнаружили теоретическую возможность передавать с его помощью неизвестное для отправителя А квантовое состояние двухуровневой системы к получателю В без реального перемещения самого элемента. Это явление, получившее название *телепортации*, стало далее основой для развития принципиально нового метода секретной передачи информации (криптографии). В последнее время оно было экспериментально продемонстрировано на простейших квантовых системах. Благодаря свойству запутывания открылись новые пути кодирования, обеспечения помехозащищенности и более эффективного управления информацией.

Импульс дальнейшему интенсивному развитию квантовых методов вычислений придал квантовый алгоритм факторизации американского математика П.Шора (1994), который производит разложение  $L$ -значного числа на простые множители за время, пропорциональное  $L^3$  [4] (классические алгоритмы требуют для этого времени, экспоненциально зависящего от  $L$ ). Например, разложение 1000-значного числа на простые множители с помощью наилучшего классического алгоритма требует около  $10^{23}$  элементарных вычислительных операций, что займет на одноплатном цифровом компьютере более  $10^7$  лет. Использование квантового алгоритма Шора позволяет выполнить эти вычисления на компьютере с тактовой частотой даже в 1 Гц всего за 10 дней. Эта задача имеет существенное практическое значение, поскольку лежит

в основе самого популярного метода криптографии. Проблема состоит в том, что для решения таких задач требуются квантовые компьютеры с числом кубитов не меньшим, чем разрядность факторизируемого числа  $L$ . Считается, что алгоритм Шора уже сейчас позволит найти применение квантовым компьютерам весьма скромных размеров (до десятков кубитов) для целей квантовой коммуникации.

Одним из важных приложений квантовых вычислений, возможно, окажется моделирование поведения широкого класса многочастичных квантовых систем, как предлагал еще Фейнман [2]. Такие задачи могут стать особенно актуальными: быстрое продвижение современной нанотехнологии все глубже в область нанометровых масштабов требует прямого моделирования электронных процессов в приборах нанoeлектроники, в том числе и в многокубитовых квантовых устройствах. В повестке дня стоит и моделирование физических свойств различных сложных органических молекулярных и биологических систем, искусственных полупроводниковых и магнитных материалов и структур и т.д.

## Структура квантового компьютера

Квантовые методы выполнения вычислительных операций, передачи и обработки информации уже начинают воплощаться в реально функционирующих экспериментальных устройствах, что стимулирует активные усилия по реализации *квантовых компьютеров*.

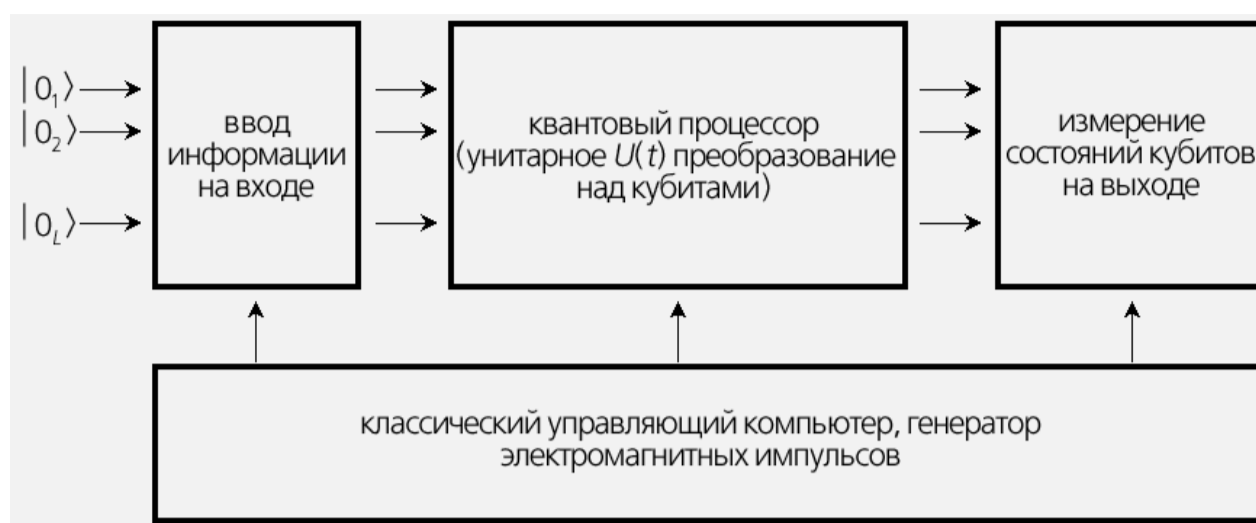
Принципиальная схема работы любого квантового компьютера может быть представлена следующим образом [5, 6] (см. рис.4). Основной его частью является квантовый регистр — совокупность некоторого числа  $L$  кубитов. Прежде чем вводить информацию в компьютер, надо организовать в регистре систему координат, в которой мы будем записывать числа. Сначала отдельные кубиты регистра должны быть приведены в основные базисные состояния, т.е. в состояния  $|0_1\rangle, |0_2\rangle,$

$$|0_3\rangle, \dots, |0_L\rangle = |0_1, 0_2, 0_3, \dots, 0_L\rangle.$$

Эта операция называется инициализацией (подготовкой начального) состояния регистра — так готовится исходное базисное состояние.

Далее подготавливаются остальные базисные состояния, чтобы получить полную систему ортогональных базисных состояний  $2^L$ -мерного гильбертова пространства. Для этого каждый кубит подвергается селективному воздействию (например, с помощью импульсов внешнего электромагнитного поля, управляемых классическим компьютером), которое переведет основные базисные состояния определенных кубитов в состояния  $|1\rangle$ . Тогда состояние всего регистра перейдет в суперпозиции базисных состояний вида

Рис.4. Схема квантового компьютера.



$|n\rangle = |n_1, n_2, n_3, \dots, n_L\rangle$  (где  $n_i = 0, 1$ ), задающие бинарное представление чисел  $n = \sum_{i=1}^L n_i 2^i$ . Таким образом система ортов будет построена.

При вводе информации конкретной задачи состояние входного регистра преобразуется (с помощью соответствующих импульсных воздействий) в необходимую когерентную суперпозицию базисных ортогональных состояний:

$$|\psi(0)\rangle = \sum_{n=0}^{2^L-1} c_n |n\rangle.$$

В таком виде информация далее обрабатывается квантовым процессором, который выполняет последовательность логических операций — унитарное преобразование  $U(t)$ , действующее на состояние всего регистра. К моменту времени  $t$  после вычисления исходное квантовое состояние становится новой суперпозицией вида

$$|\psi(t)\rangle = \sum_{n,m} c_n U_{mn}(t) |n\rangle$$

— это и есть результат на выходе компьютера.

Главная проблема, стоящая перед создателями квантовых компьютеров, — борьба с потерей когерентности квантовых состояний, или так называемой *декогерентизацией*, обусловленной взаимодействием кубитов с окружающей средой, помехами в процессе выполняемых вычислительных операций и различными случайными ошибками. Для ее решения в настоящее время интенсивно разрабатываются различные методы подавления декогерентизации и исправления ошибок: так, очень важно обеспечить, чтобы система кубитов была как можно слабее связана с окружением. Все возможные операции на входе данного компьютера, локальные преобразования, соответствующие алгоритму вычисления, способы подавления декогерентизации и исправления случайных ошибок в совокупности играют здесь роль того, что называют программным обеспечением (software).

## Из чего его построить?

При выборе конкретной схемы квантового компьютера необходимо прежде всего решить три задачи: во-первых, выбрать физическую систему, представляющую требуемую систему кубитов, во-вторых, определить физический механизм, реализующий необходимое для выполнения двухкубитовых операций взаимодействие между кубитами, и, в-третьих, найти способы селективного управления кубитами и измерения их состояния на выходе. Все это можно отнести к аппаратному обеспечению (hardware) квантового компьютера.

Кроме того, при создании полномасштабного квантового компьютера, превосходящего по производительности любой классический, на каких бы физических принципах первый ни работал, следует выполнить пять основных требований:

— физическая система, представляющая квантовый регистр, должна иметь достаточно большое число  $L > 10^3$  различаемых кубитов;

— нужно обеспечить условия для инициализации состояния  $L$ -кубитового входного регистра  $|0_1, 0_2, 0_3, \dots, 0_L\rangle$ ;

— время декогерентизации должно превышать по крайней мере в  $10^4$  раз время выполнения основных квантовых операций (время такта);

— требуемая совокупность квантовых логических операций из определенного набора двухкубитовых и однокубитовых операций\* должна выполняться за время такта;

— состояние квантового регистра на выходе нужно измерять с высокой надежностью.

Какие объекты могут соответствовать этим критериям? В экспериментальном плане сейчас активно развиваются два направления развития элементной базы будущих квантовых компьютеров.

Одно из них предполагает использовать в качестве квантовых регистров цепочку кубитов из ионов или нейтральных атомов с двумя низколежащими колебательными уровнями, удерживаемых в силовых ловушках в вакууме при температурах порядка  $10^{-6}$  К (такие

\* Как было доказано, логическую квантовую операцию любой сложности можно представить с помощью набора только двухкубитовых и однокубитовых операций.



Рис.5. ЯМР-спектрометр высокого разрешения фирмы «Bruker», использующийся для выполнения многих типов квантовых операций на ансамблях органических молекул.

сверхнизкие температуры достигаются с помощью лазерного охлаждения). Первый прототип квантового компьютера на этих принципах был предложен австрийскими физиками И.Цираком и П.Цоллером еще в 1995 г., а сейчас над ним наиболее интенсивно работают в США (Лос-Аламосская национальная лаборатория — LANL, Национальный институт стандартов и технологий — NIST). Одной из основных проблем остается получение достаточно большого числа кубитов в квантовом регистре (пока не удалось создать квантовый регистр даже с двумя-тремя кубитами).

В другом подходе кубитами служат атомы с ядерными спинами  $I = \frac{1}{2}$ , принадлежащие молекулам органических жидкостей [7]. Данные объекты привлекательны тем, что практически независимые молекулы-компьютеры в жидкости действуют параллельным образом, одновременно. Управлять ими можно при комнатных температурах с помощью операций над большим ансамблем молекул, хорошо известных в технике ядерного магнитного резонанса (ЯМР), рис.5. Устройство такого рода получило название ансамблевого ЯМР-квантового компьютера. Первые предложения были сформулированы в 1997 г. несколькими группами исследователей из Массачусетского технологического института и из Лос-Аламосской национальной лаборатории, а также из Кларендонской лаборатории в Оксфорде (Великобритания). В том же году были выпол-

нены первые эксперименты на ядерных спинах двух атомов водорода  $^1\text{H}$  в молекулах 2,3-дибромотиофена  $\text{SCH}:(\text{CBr})_2:\text{CH}$  и на трех ядерных спинах — одном в атоме водорода  $^1\text{H}$  и двух в изотопах углерода  $^{13}\text{C}$  в молекулах трихлорэтилена  $\text{CCl}_2:\text{CHCl}$ . Позднее были осуществлены квантовые операции на других жидкостях с числом спинов-кубитов в молекуле  $L = 5,6,7$ . На жидкостных ЯМР квантовых компьютерах были продемонстрированы гроверовский алгоритм поиска данных, квантовая коррекция ошибок, квантовая телепортация, алгоритм факторизации Шора и другие операции. Однако у этого направления есть существенное ограничение: ЯМР-квантовые компьютеры на молекулах органической жидкости из-за слабости сигнала (он уменьшается экспоненциально с ростом числа кубитов) не смогут иметь число кубитов больше 20—30.

Видимо, указанные два пути в ближайшем будущем не приведут к созданию полномасштабного многокубитового квантового компьютера. То, что удалось сделать, следует рассматривать скорее как модельные прототипы будущих квантовых компьютеров, полезные для отработки принципов квантовых вычислений и проверки квантовых алгоритмов. Более обещающими направлениями могут оказаться, на наш взгляд, следующие.

Во-первых, использование в качестве квантовых состояний кубитов двух спиновых или двух зарядовых электронных состояний в полупроводниковых наност-



руктурах (например, в квантовых точках, формируемых в гетероструктурах) либо со спин-спиновым магнитным, либо с электрическим взаимодействием между кубитами соответственно. Однако, несмотря на активные поисковые работы, проводимые уже несколько лет в исследовательских центрах фирмы IBM, практических результатов достигнуть еще не удалось.

Во-вторых, реализация кубитов на основе различных зарядовых состояний куперовских пар в квантовых точках, связанных переходами Джозефсона, как это предложил Д.В.Аверин в 1998 г. [8]. Здесь есть надежда создать электронные квантовые устройства высокой степени интеграции на одном кристалле, с электрическим управлением кубитами, без громоздких ЯМР-установок. Пока удалось сформировать и исследовать один сверхпроводниковый кубит.

Но наиболее важные, ближайшие перспективы открываются перед твердотельными ЯМР-квантовыми компьютерами. Остановимся на них подробнее.

В 1998 г. австралийский физик Б.Кейн [9] представил в роли кубитов обладающие ядерным спином  $I = 1/2$  донорные атомы фосфора (изотоп  $^{31}\text{P}$ ), которые им-

планируются в приповерхностный слой кремниевой структуры (рис.6). Таким способом можно попытаться построить полномасштабные вычислительные устройства с практически неограниченным числом кубитов. Правда, температуры придется использовать достаточно низкие, чтобы электроны донорных атомов занимали только самое нижнее спиновое  $S$ -состояние в магнитном поле. В полях с индукцией  $B \geq 2$  Тл это

соответствует температурам  $T < 0.1$  К. Первые шаги по реализации подобной схемы уже предприняты в специально организованном в 2000 г. Австралийском центре технологии квантовых компьютеров. Работы в этом направлении ведутся и в Физико-технологическом институте РАН.

Каждый донорный атом должен располагаться с достаточной точностью под «своим» управляющим металлическим затвором А, отделенным от поверхности кремния тонким диэлектриком (например, окисью кремния толщиной порядка 20 нм). Вместе атомы образуют линейную решетку произвольной длины с периодом  $l$ .

Управлять однокубитовыми квантовыми операциями по отдельности предполагается путем селективного воздействия резонансных радиочастотных импульсов на ядерные спины определенных доноров. Для этого с помощью электрического поля, создаваемого потенциалом затворов А, перераспределяется электронная плотность вблизи ядра. В результате благодаря так называемому сверхтонкому взаимодействию ядерного спина с электронным происходит требуемая настройка резонансной частоты ядерного спина. Величину взаимодействия между ядерными спинами соседних доноров, которое обеспечивает выполнение двухкубитовых операций, предлагается регулировать с помощью электрических потенциалов на промежуточных затворах J, позволяющих изменять сте-

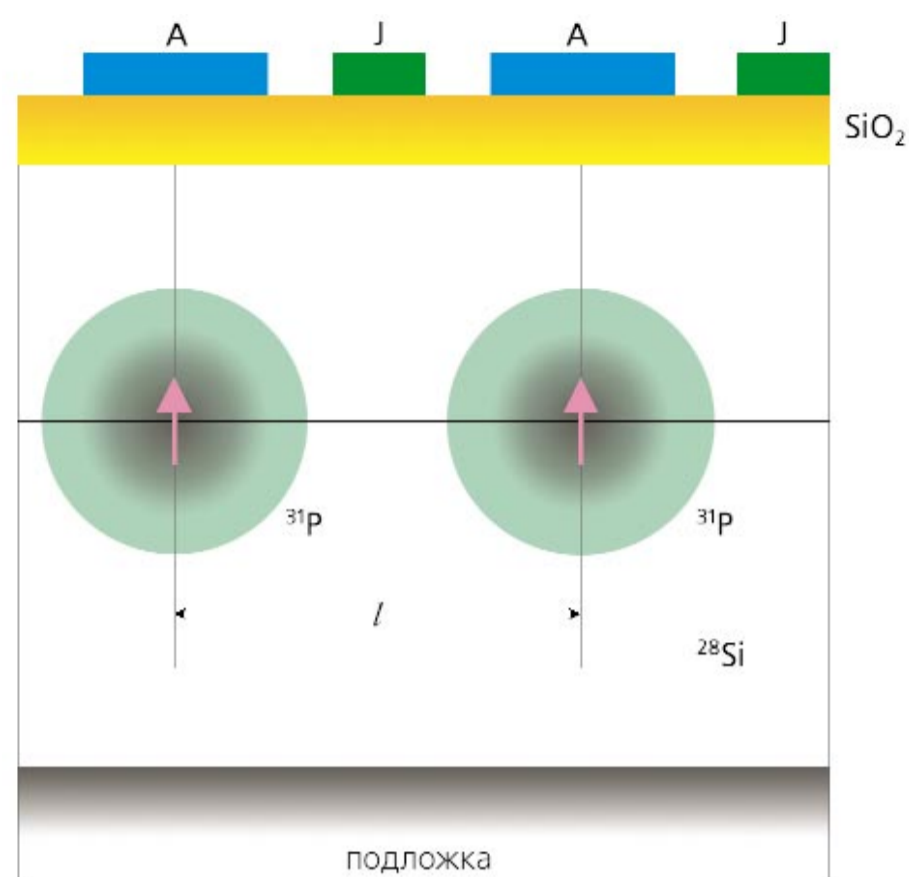


Рис.6. Схематическое изображение двух ячеек структуры модели Кейна,  $l = 20$  нм.

пень перекрытия волновых функций электронов атомов фосфора. Необходимое для этого расстояние  $l$  должно быть порядка 20 нм.

Для формирования таких структур следует обратиться к современной нанотехнологии, в частности к методами эпитаксиального выращивания, к зондовой нанолитографии в сверхвысоком вакууме на основе сканирующих туннельных и атомно-силовых микроскопов, к электронно-лучевой и рентгеновской литографии. Кроме того, чтобы исключить взаимодействие кубитов с окружением, сам кремний должен быть достаточно хорошо очищен от своего изотопа  $^{29}\text{Si}$ , обладающего, как и атом фосфора, спином  $I = 1/2$  (в естест-

венном кремнии его около 4.7%). Возможность создания подобного полномасштабного квантового компьютера интенсивно исследуется в настоящее время (как экспериментально, так и теоретически) в Австралийском центре технологии квантовых компьютеров.

Были предложены также и несколько вариантов измерения состояний индивидуальных кубитов, но ни один из них пока не реализован. В качестве альтернативы рассматривались различные ансамблевые модификации твердотельных ЯМР-квантовых компьютеров [10].

Итак, все последние три (из перечисленных и пока нереализованных конкурирующих) направления допускают произвольно большое число кубитов: для двух из них существуют уже отработанные приемы микро- и нанотехнологии создания полупроводниковых и сверхпроводниковых интегральных схем. Но кроме квантового регистра требуется наличие генераторов управляющих импульсов, использование низких температур и, следовательно, привлечение совсем не ми-

ниатюрных обслуживающих систему кубитов устройств, а в случае твердотельного ЯМР-квантового компьютера еще и использование магнита. Зато для твердотельного ЯМР-квантового компьютера можно указать на ряд важных достоинств: ядерные спины сами по себе являются кубитами, при низких температурах они характеризуются очень большими временами релаксации (и соответственно временами декогерентизации) по сравнению с электронными спинами. Технологические структуры нанометрового масштаба в полупроводниковых ЯМР-квантовых компьютерах предназначаются не для создания самих кубитов, как в случае сверхпроводниковых устройств, а лишь для управления кубитами и измерения их состояний. Определенные преимущества могут иметь ЯМР-квантовые компьютеры, работающие на принципе клеточно-автомата с использованием антиферромагнитных структур [11].

Какой подход первым выведет на финишную прямую — покажет время. Не исключено, что в ближайшем будущем появятся комбинированные варианты твердотельных квантовых компьютеров. Например, в одной структуре могут использоваться и ядерные спины, и квантовые точки с электронными спинами, если привлечь комбинированные методы обращения к кубитам (двойной электрон-ядерный магнитный резонанс, динамическую поляризацию ядерных спинов, оптическое детектирование ядерного магнитного резонанса и др.).

## Что впереди?

Если распространить закон Мура на область квантовых компьютеров, можно спрогнозировать, что через примерно 10 лет будут созданы простейшие фрагменты или прототипы твердотельного ЯМР-квантового компьютера. Это потребует привлечения многих технологических и схемотехнических достижений современной микро- и нанoeлектроники, а также разработки программ математического моделирования физических процессов в многокубитовых квантовых системах. Препятствий на пути еще немало. Пока не доведены до практики методы квантовых измерений состояний отдельного ядерного спина или их малых групп. Еще сла-

бо изучено влияние неидеальности управляющих кубитами импульсных последовательностей и многоуровневой сверхтонкой структуры энергетического спектра на декогерентизацию квантовых состояний. Не разработаны способы подавления декогерентизации, определяемой шумами в электронной измерительной системе, не опробованы квантовые методы коррекции ошибок для многокубитовых систем. От решения этих и других проблем во многом зависит дальнейшее развитие квантовой компьютерной техники.

Исключительные возможности квантовых компьютеров будут способствовать и революции в сфере вычислительной техники, и еще более глубокому пониманию физических законов в Природе. Заметим, что будущий квантовый компьютер не заменит классический компьютер, скорее всего он будет играть роль специального процессора, встроенного в обычную вычислительную систему, которому будут поручаться типично квантовые задачи. Заинтересовавшийся читатель может познакомиться более подробно с проблемами квантовых вычислений и квантовых компьютеров в нашей монографии [12]. ■

## Литература

1. Манин Ю.И. Вычислимое и невычислимое. М., 1980. С.128.
2. Feynman R. // Inter. Jour. Theor. Phys. 1982. V.21. №6/7. P.467—488.
3. Feynman R.P. // Foundation of Phys. 1986. V.16. №6. P.507—531.
4. Shor P. // SIAM Jour. Comp. 1997. V.26. №5. P.1484—1509.
5. Валиев К.А. // Успехи физ. наук. 1999. Т.162. №6. С.691—694.
6. Валиев К.А. // Вестн. РАН. 2000. Т.70. №8. С.688—705.
7. Jones J.A. // Fortschr. Phys. 2000. V.48. №9—11. P.909—924.
8. Averin D.V. // Solid State Comm. 1998. V.105. №12. P.2371—2374.
9. Kane B.E. // Nature. 1998. V.393. P.133—137.
10. Валиев К.А., Кокин А.А. // Микроэлектроника. 1999. Т.28. №5. С.326—337.
11. Kokin A.A. // Phys. Metal. Metallogr. 2001. V.92. Suppl.1. P.S150—S156.
12. Валиев К.А., Кокин А.А. Квантовые компьютеры: надежды и реальность. М.; Ижевск, 2001.