

ФУНДАМЕНТАЛЬНЫЕ ИССЛЕДОВАНИЯ

УДК 53:621.373.8:681.3

Из итогов XX века: от кванта к квантовым компьютерам.

I. Физические основы и принципы построения квантового компьютера

К.А.Валиев, А.А.Кокин

Физико-технологический институт Российской АН

Дано представление о физических основах и принципах построения квантовых компьютеров - новом направлении вычислительной техники.

*"Где начало того конца, которым
оканчивается начало?"*

Козьма Прутков "Плоды Раздумья".

Немного о рождении квантовой физики

В канун XX века 14 декабря 1900 г. немецкий физик и будущий нобелевский лауреат Макс Планк доложил на заседании Берлинского физического общества о фундаментальном открытии квантовых свойств теплового излучения. Этот день считается днем рождения квантовой теории. В физике родилось понятие *кванта* энергии и среди других фундаментальных постоянных появилась постоянная Планка $\hbar = 1,38062 \cdot 10^{-23}$ Дж/К. Таким образом, в 2000 г. весь мир отмечает 100-летний юбилей постоянной Планка, а с ним и юбилей квантовой физики.

Открытие Планка, появившаяся затем в 1905 г. теория фотоэлектрического эффекта А.Эйнштейна и создание в 1913 г. Н.Бором первой квантовой теории атомных спектров стимулировали создание и бурное дальнейшее развитие *квантовой теории* и экспериментальных исследований квантовых явлений. Уже в 1925 г. В.Гайзенберг предложил матричный вариант квантовой механики, а в 1926 г. Э.Шредингер сформулировал 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 квантовый принцип, сформулированный тогда же В.Паули. Анализ квантово-механической задачи о движении электрона во внешнем периодическом поле, создаваемом атомными остатками в кристаллической решетке, 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 зоны. Однако у полупроводников ширина запрещенной зоны достаточно мала и через нее за счет теплового возбуждения с заметной вероятностью могут пере-

брасываться электроны. В 1931 г. А.Вильсоном было показано, что проводимость полупроводников имеет место лишь при наличии незаполненных зон. Ток, создаваемый электронами не полностью заполненных зон, оказывается эквивалентным току, создаваемому некоторыми квазичастицами с положительным зарядом - дырками, заполняющими уровни, не занятые электронами. При этом длина свободного пробега электронов и дырок в кристалле определяется рассеянием их на искажениях идеального периодического потенциала примесями, дефектами и колебаниями кристаллической решетки. Полупроводники, в зависимости от преобладания числа 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. являются проявлением *квантовых свойств твердого тела*. В результате, уже в начале 30-х гг. 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 теорию явлений выпрямления и возникновения фотоэдс в таких переходах.

Квантовая теория твердого тела - научная база микроэлектроники и наноэлектроники

Прикладное значение p - n -переходов не сразу было должным образом оценено. Электроника того времени развивалась исключительно на основе вакуумных электронных ламп и специалисты-электронщики мало интересовались полупроводниками. Только после изобретения в 1948 г. сотрудниками Bell Laboratories Дж.Бардиным и В.Брэттенем точечно-контактного кристаллического триода на основе германия n -типа, названного транзистором, и появления работы В.Шокли в 1949 г. по квантовой теории плоскостных диодов и транзисторов начался беспрецедентный качественный прорыв в полупроводниковой электронике. Авторы этих работ были отмечены Нобелевской премией. Позднее Дж. Бардин получил вторую Нобелевскую премию за создание вместе с Л.Купером и Дж.Шриффером квантовой теории сверхпроводимости.

Заметим, что этот прорыв не мог быть достигнут на пути дальнейшего развития только вакуумной электроники. Для этого потребовались совершенно новые идеи, которые и появились в результате исследований в совершенно другой области физики - в квантовой теории полупроводников. Новой технической области потребовались специалисты с глубоким знанием физики полупроводников и ее квантовых основ.

Важную роль в дальнейшем развитии полупроводниковой электроники сыграло позднее изобретение кремниевой *планарной технологии*, основанной на контролируемой диффузии примесей в локальных областях в приповерхностном слое кремниевой пластины, и создание в 1959 г. на фирме Fairchild Semiconductor первого *планарного биполярного транзистора* на кремнии. Рождение *микроэлектроники* принято относить именно к этой дате. Несколько позже был создан первый полевой транзистор со структурой металл - окисел - полупроводник (МОП-транзистор) на кремнии, выполненный также по планарной технологии. Он стал в дальнейшем одним из основных элементов 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 (тогда п/я 2021) в Зеленограде в 1965 г. В том же году начал готовить специалистов в области микроэлектроники новый вуз - Московский институт электронной техники в Зеленограде.

Успехи в развитии кремниевой микроэлектроники наглядно выражаются так называемым *законом Г.Мура*, согласно которому число транзисторов в кристалле одной интегральной схемы (ИС), начиная с 1959 г., в течение первых 15 лет удваивалось каждый год, а затем и до сих пор такое удвоение происходит приблизительно за 1,5 года. По экспоненциальному закону уменьшаются со временем и характерные размеры элементов ИС. В декабре 1999 г. появилось сообщение о разработке в Калифорнийском университете в Беркли технологии изготовления МОП-транзистора на островке кремния в форме плавника с рекордной эффективной длиной канала 18 нм и хорошими характеристиками, а также матрицы соответствующих тестовых структур. Экстраполяция тенденции уменьшения размеров приборов показывает, что атомные размеры в твердотельной технологии могут быть достигнуты уже через 20 лет.

Основой современного цифрового компьютера является совокупность макроскопических полупроводниковых базисных элементов - *классических битов* с двумя возможными логическими *булевыми состояниями* "0" и "1" и логических элементов-вентилей, которые производят локальные логические операции над состояниями этих элементов для того, чтобы получить в результате определенное конечное состояние на выходе.

Логические состояния в каждом бите - это, например, два значения тока в определенном проводнике или потенциала на нем, рассматриваемые как макроскопические некогерентные классические величины. В этом смысле современные цифровые компьютеры, несмотря на исходную квантовую природу физических процессов, происходящих в полупроводниковых элементах, рассматриваются как *классические*. Вычисление в любом компьютере представляет собой процесс, в ходе которого происходит определенные для каждой логической операции нелинейные взаимодействия потоков информации друг с другом и их преобразование. Соответствующие процессы происходят на физическом уровне и с носителями информации - некогерентными сигналами, т.е. с токами и напряжениями.

Последние два десятилетия характеризовалось также освоением новых не кремниевых материалов и интенсивными поисками новых физических принципов для приборов с характерными размерами, сравнимыми с длиной волны Де-Бройля (порядка 20 нм), для которых существенны более тонкие по сравнению с массивными полупроводниками квантовые свойства. Это квантовые ямы, нити и точки. Такие структуры потребовали новой технологии, которая получила название *нанотехнологии*.

Примером *нанoeлектронных* полупроводниковых приборов могут служить, в частности, транзисторы с резонансным туннелированием и транзисторы на горячих электронах с резонансным туннелированием, характеристики которых существенным образом определяются свойствами электронных квантовых состояний и квантовым характером эволюции этих состояний в полупроводниковых структурах. Существует и много других типов *нанoeлектронных* приборов, физические процессы внутри которых имеют квантовый характер и требуют для своего описания применения квантовых методов. Однако по-прежнему в *нанoeлектронных* приборах, как и в традиционных микроэлектронных приборах, обрабатывается информация, передаваемая некогерентными классическими сигналами, носителями которых являются электрические токи и напряжения.

Важной проблемой, с которой пришлось столкнуться особенно при переходе в область *нанoeлектронных* устройств, является проблема уменьшения рассеиваемой энергии в процессе вычислительных операций. Мысль о возможности "*логически обратимых*" операций, не сопровождающихся рассеянием энергии, впервые высказал Р.Ландауер еще в 1961 г. [1]. Существенный шаг в ее решении был сделан в 1982 г. Ч.Беннеттом [2], который показал, что универсальный цифровой компьютер типа вы-

числительной 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). К типичным обратимым универсальным вентилям относятся вентили Фредкина и Тоффоли.

Возникновение идеи о квантовых вычислениях

Дальнейший прогресс микроэлектроники и вычислительной техники до недавнего времени виделся на пути увеличения степени интеграции, быстродействия 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, на основе которого были построены различные логические элементы и элементы памяти.

Любая классическая двухуровневая система, как и квантовая, имеет основное $|0\rangle$ и не основное $|1\rangle$ базисные состояния. Примером классической двухуровневой системы является известный в микроэлектронике инвертор, осуществляющий операцию НЕ. В зависимости от того заняты ли эти состояния с вероятностями $P(0) = 1$, $P(1) = 0$ или $P(0) = 0$, $P(1) = 1$, мы имеем *булевы логические* состояния "0" или "1".

В квантовом случае возникает намного более богатая ситуация. Волновая функция квантовых состояний двухуровневой системы - квантового бита, получившего в дальнейшем название *кубита* (quantum bit или qubit) [3], может представлять собой *суперпозицию* базисных состояний (вектор состояния) следующего вида $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, где α , β - комплексные амплитуды состояний, при этом $|\alpha|^2 + |\beta|^2 = 1$. Помимо вероятностей $P(0) = |\alpha|^2$ и $P(1) = |\beta|^2$ заполнения базисных состояний $|0\rangle$ и $|1\rangle$ состояние кубита характеризуется *когерентными* или *интерференционными* слагаемыми в вероятности состояния $|\psi\rangle$, определяемыми произведениями комплексных амплитуд $\alpha\beta^*$ и $\alpha^*\beta$. Состояние квантового бита в отличие от классического может изменяться не только путем изменения вероятностей $P(0)$ и $P(1)$, но и более тонко путем изменения амплитуд состояний α и β , что соответствует поворотам вектора состояния $|\psi\rangle$ в так называемом гильбертовом двумерном пространстве состояний. В этом и состоит принципиальное различие классического и квантового бита.

Кардинально новой оказалась идея о *квантовых вычислениях*, впервые высказанная советским математиком Ю.И.Маниным в 1980 г. [4], и которая стала активно обсуждаться лишь после опубликования в 1982 г. статьи американского физика-теоретика нобелевского лауреата Р.Фейнмана [5]. Он обратил внимание на способность изолированной квантовой системы из L двухуровневых квантовых элементов находиться в когерентной *суперпозиции* из 2^L булевых состояний, характеризующейся 2^L комплексными числами и увеличенной до 2^L размерностью соответствующего гильбертова пространства. Ясно, что для описания такого квантового состояния в классическом вычислительном устройстве потребовалось бы задать 2^L комплексных чисел, т.е. понадобились бы *экспоненциально большие* вычислительные ресурсы. Отсюда был сделан обратный вывод о том, что эффективное численное моделирование квантовых систем, содержащих до сотни двухуровневых элементов, практически недоступно классическим компьютерам, но может эффективно осуществляться путем выполнения логических операций на квантовых системах, которые действуют на суперпозиции многих квантовых состояний.

Поскольку законы квантовой физики на микроскопическом уровне являются линейными и обратимыми, то и соответствующие квантовые логические устройства, производящие операции с когерентными (чистыми) квантовыми состояниями отдельных кубитов, оказываются также *логически и термодинамически обратимыми*, а квантовые вычислительные операции представляются *унитарными операторами* (или матрицами $2^L \times 2^L$) в 2^L -мерном гильбертовом пространстве. Квантовые вентили аналогичны соответствующим обратимым классическим вентилям, но в отличие от классических они способны совершать *унитарные операции над суперпозициями состояний*. Выполнение унитарных логических операций над кубитами предполагается осуществлять с помощью соответствующих внешних воздействий, которыми управляют классические компьютеры. Р.Фейнман предложил и первую схему квантового обратимого компьютера [6].

Основные факторы, определяющие ускорение квантовых вычислений

Элементарным шагом при квантовых вычислениях является унитарная операция над L -кубитовой суперпозицией состояний регистра из L кубитов, при этом выполняется параллельная обработка сразу всех 2^L комплексных амплитуд, тогда как для классического компьютера подобная операция потребовало бы 2^L отдельных элементарных шагов. Такое свойство называется *квантовым параллелизмом* в работе квантовых устройств, оно приводит к экспоненциальному ускорению вычислительного процесса. В этом заключается одно из главных преимуществ квантовых компьютеров по сравнению с классическими цифровыми компьютерами. Вычислительный процесс носит характер интерференции - комплексные амплитуды состояний многих кубитов могут складываться конструктивно и деструктивно. Так построен, например, знаменитый алгоритм Л.Гровера *поиска в неструктурированной базе данных* [7].

Одним из наиболее интересных свойств квантовых состояний, принципиально отличающих их от классических, является *запутывание* (entanglement) состояний, которое представляет собой когерентную суперпозицию состояний нескольких квантовых элементов, определяющее своеобразную *нелокальную* корреляцию этих состояний, возникающую при взаимодействии кубитов. Такие состояния получили название *запутанных* (entangled) состояний. Запутанные состояния играют очень важную роль в различных процессах передачи и обработки квантовой информации. Хотя понятие *запутывания* (entanglement) было введено еще Э.Шредингером под названием Verschränkung в 1935 г., большое внимание оно привлекло к себе лишь с 1993 г. в связи с обнаруженной Ч.Беннеттом с сотр. [8] теоретической возможностью использования его для передачи (*телепортации*) неизвестного для отправителя A квантового состояния двухуровневой системы к получателю B без реального перемещения самого элемента. Эта мысль стала далее основной для развития принципиально нового метода секретной передачи информации (*криптографии*). В последнее время квантовое явление телепортации активно обсуждается с точки зрения организации быстрых квантовых вычислений в многокубитовых системах.

Перечень возможных приложений запутанного состояния уже достаточно велик. Свойство запутывания квантовых состояний лежит и в основе многих квантовых алгоритмов. Оно является одним из корней ожидаемых успехов квантовых вычислительных процессов, поскольку открывает принципиально новые возможности кодирования информации, обеспечения помехозащищенности и более эффективного управления информацией.

С ожидаемым экспоненциальным ускорением квантовых вычислений обычно связывают перспективы решения так называемой *NP-полной* (Nondeterministic polynomial-time complete) *проблемы*, т.е. проблемы решения таких задач, для которых это решение очень трудно найти с помощью классических цифровых компьютеров, хотя очень

просто это решение проверить. Такие задачи относятся к классу *невычислимых* в том смысле, что они не могут быть решены на классических компьютерах за время, полиномиально зависящее от числа битов L , представляющих задачу.

Квантовый алгоритм факторизации, предложенный П.Шором в 1994 г. [9], позволяющий производить разложение n -значного числа на простые множители за время, полиномиально зависящее от n , т.е. с экспоненциальным ускорением по сравнению с самыми мощными классическими алгоритмами, стал одним из основных побуждений для интенсивного развития квантовых методов вычислений и изобретения алгоритмов, которые позволяют решать некоторые NP-проблемы. Считается, что алгоритм Шора уже сейчас позволит найти применение квантовым компьютерам весьма скромных размеров (десятки кубитов) для целей квантовой криптографии, квантовой коммуникации.

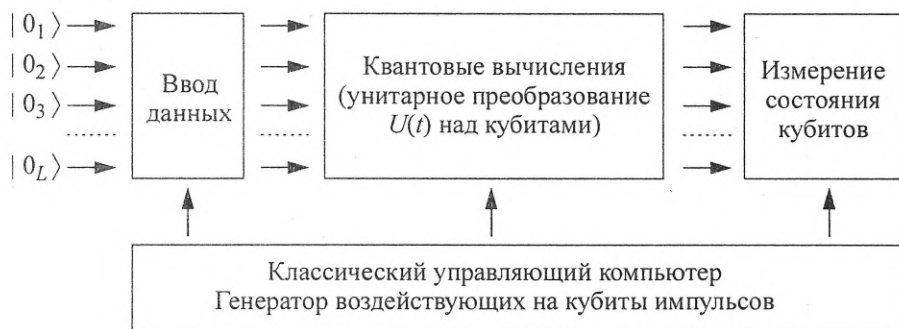
Одним из важных приложений квантовых вычислений возможно окажется также моделирование поведения широкого класса многочастичных квантовых систем, отмечавшееся еще Р.Фейнманом [5]. Задачи такого рода могут стать особенно актуальными в связи с быстрым продвижением современной нанотехнологии все глубже в область нанометровых масштабов и необходимостью прямого моделирования электронных процессов в приборах нанoeлектроники, в том числе и в многокубитовых квантовых устройствах, а также в связи с потребностью моделирования физических свойств различных сложных органических молекулярных и биологических систем, искусственных полупроводниковых и магнитных материалов и структур.

Структура квантового компьютера

Квантовые методы выполнения вычислительных операций, а также передачи и обработки информации уже начинают воплощаться в реально функционирующих экспериментальных устройствах, что стимулирует усилия по реализации *квантовых компьютеров* - этого нового направления в вычислительной технике.

В последнее время число публикаций по квантовой теории информации и квантовым вычислениям резко возросло, появились и экспериментальные работы.

Принципиальная схема работы любого квантового компьютера может быть представлена следующим образом [10, 11] (рисунок). Основной его частью является квантовый регистр - совокупность некоторого числа L кубитов. До ввода информации в компьютер все кубиты регистра должны быть приведены в основные базисные (булевы) состояния, т.е. в состояние $|0_1\rangle, |0_2\rangle, |0_3\rangle, \dots, |0_L\rangle \equiv |0_1, 0_2, 0_3, \dots, 0_L\rangle$. Эта операция называется подготовкой начального состояния или *инициализацией* (initializing). Далее каждый кубит подвергается селективному воздействию, например, с помощью импульсов внешнего электромагнитного поля, управляемых классическим компьютером, которое переведет основные базисные состояния определенных кубитов в не основные состояния $|0\rangle \Rightarrow |1\rangle$. При этом состояние всего регистра перейдет в суперпозицию базисных



Схематическая структура квантового компьютера

состояний вида $|n\rangle = |n_1, n_2, n_3, \dots, n_L\rangle$, где $n_i = 0, 1$, задающую бинарное представление числа $n = \sum_{i=1}^L n_i 2^i$.

При вводе информации в квантовый компьютер состояние входного регистра с помощью соответствующих импульсных воздействий преобразуется в соответствующую

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

В таком виде информация далее подвергается воздействию квантового процессора, выполняющего последовательность квантовых логических операций, определяемую унитарным преобразованием $\hat{U}(t)$, действующим на состояние всего регистра. К моменту времени t в результате преобразований исходное квантовое состояние становится новой

суперпозицией вида $|\psi(t)\rangle = \sum_{n,m} c_n \hat{U}_{mn}(t) |n\rangle$, которая и определяет результат преоб-

разования информации на выходе компьютера.

Совокупность всех возможных операций на входе данного компьютера, формирующих исходные состояния, а также осуществляющих унитарные локальные преобразования, соответствующие алгоритму вычисления, способы подавления потери когерентности - так называемой *декогерентизации* (decoherence) квантовых состояний и исправления случайных ошибок, играют здесь ту же роль, что и "программное обеспечение" (software) в классическом компьютере.

Литература

1. **Landauer R.** Irreversibility and heat generation in the computing process // IBM Journ. Res. Develop. - 1961. - Vol. 5, № 3. - P. 183 - 191. = **Ландауэр Р.** Необратимость и выделение тепла в процессе вычислений // Квантовый компьютер & квантовые вычисления: Пер. с англ. / Под ред. В.А.Садовниченко. - Ижевск, 1999. - Ч. 2. - С. 9 - 32.
2. **Bennett C.H.** The thermodynamics of computation. A Review // Intern. J. of Theor. Phys. - 1982. - Vol. 21, № 12. - P. 905 - 940.
3. **Schumacher B.** Quantum coding // Phys. Rev. - 1995. - Vol. A51, № 4. - P. 2738 - 2747.
4. **Манин Ю.И.** Вычислимое и невычислимое. - М.: Сов. Радио, 1980. - 128 с.
5. **Feynman R.** Simulating Physics with Computers // Intern. J. Theor. Phys. 1982. - Vol. 21, № 6/7. - P. 467 - 488 / **Фейнман Р.** Моделирование физики на компьютерах // Квантовый компьютер & квантовые вычисления: Пер. с англ. / Под ред. В.А.Садовниченко. - Ижевск, 1999. - Ч. 2. - С. 96 - 124.
6. **Feynman R.P.** Quantum mechanical computers // Foundation of Phys. - 1986. - Vol. 16, № 6. - P. 507 - 531. = **Фейнман Р.Ф.** Квантовомеханические компьютеры // Квантовый компьютер & квантовые вычисления: Пер. с англ. / Под ред. В.А.Садовниченко. - Ижевск, 1999. - Ч. 2. - С. 125 - 156.
7. **Grover L.K.** Quantum mechanics help in searching for a needle in a haystack // Phys. Rev. Lett. - 1997. - Vol. 78, № 2. - P. 325 - 328. = **Гровер Л.К.** Квантовая механика помогает найти иголку в стоге сена // Квантовый компьютер & квантовые вычисления: Пер. с англ. / Под ред. В.А.Садовниченко. - Ижевск, 1999. - Ч. 1. - С. 101 - 109.
8. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channel / **C.H.Bennett, G.Brassard, C.Cre'peau, et al.** // Phys. Rev. Lett. - 1993. - Vol. 70, № 13. - P. 1895 - 1899.
9. **Shor P.** Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer // SIAM J. Comp. - 1997. - Vol. 26, № 5. - P. 1484 - 1509. = **Шор П.** Полиномиальные по времени алгоритмы разложения числа на простые множители и нахождения дискретного логарифма для квантового компьютера // Квантовый компьютер & квантовые вычисления: Пер. с англ. / Под ред. В.А.Садовниченко. - Ижевск, 1999. - Ч. 2. - С. 200 - 247.
10. **Валиев К.А.** Квантовые компьютеры: могут ли они быть "большими"? // УФН. - 1999. - Т. 162, № 6. - С. 691 - 694.
11. **Валиев К.А.** Квантовая информатика: компьютеры, связь и криптография // Вестник РАН. - 2000. - Т. 70, № 8. - С. 688 - 705.