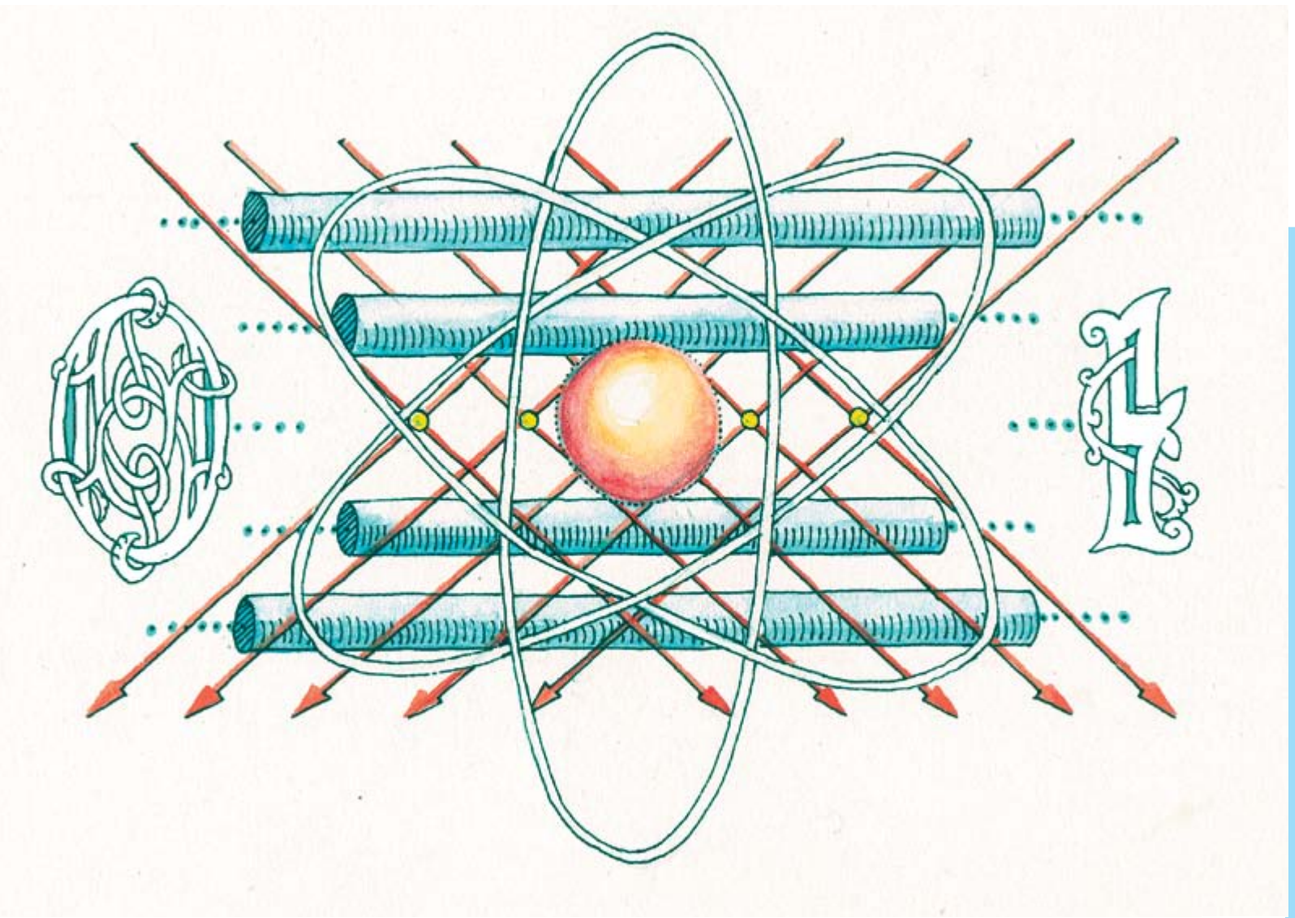
Потеснят ли квантовые компьютеры классические?

Текст Ю. В. Владимирова, В. Н. Задков
Физический факультет и Международный учебно-научный лазерный центр МГУ имени М. В. Ломоносова
Иллюстрация Александр Желонкин



Современные технологии наноэлектроники позволяют массово создавать чипы с разрешением в десятки нанометров, а в лабораториях – и с атомным разрешением. Элементарные логические вентили таких устройств вскоре будут состоять из десятков или даже единичных атомов, так что эти устройства уже не будут подчиняться законам классической физики и в игру вступит их квантовая природа. Первым это отметил нобелевский лауреат, физик Ричард Фейман в своей знаменитой речи на ужине ежегодного съезда американского физического общества еще в 1959 году Из такого рода квантовых логических устройств можно построить квантовый компьютер. Вопрос в том, каковы его преимущества и потеснят ли квантовые компьютеры классические?

Классический бит может принимать только два возможных логических состояния - 0 и 1, которые в физике принято наглядно изображать состояниями единичного вектора (вверх и вниз соответственно) на единичной сфере состояний этого вектора, которая называется в физике сфере Блоха. **Квантовый бит информации (кубит) может принимать, в отличие от классического бита, не два, а бесконечное число состояний**, поскольку он описывается нормированной на единицу линейной комбинацией двух базисных состояний |0> и |1> (аналоги состояний 0 и 1 классического бита). При этом вектор состояний кубита может оканчиваться в любой точке на сфере Блоха, в том числе и совпадая со значением |0> (вверх) или |1> (вниз). Пространство состояний, в котором «живет»′ кубит, называется гильбертовым пространством и его размерность равна 2 для одного кубита (два в степени N – для N кубитов). Замечательным и принципиально важным с точки зрения хранения и обработки информации является также тот факт, что **регистр квантовой памяти (набор кубитов) хранит информацию куда более эффективно, чем любая классическая память.** Так, N кубитов «живут» в 2^N-мерном гильбертовом пространстве (например, для N кубитов $2^N = 2^{16} = 65536$) и операции над ними осуществляются поворотом вектора их состояния в этом пространстве за один шаг. На классическом же компьютере для хранения в его памяти информации о состоянии N кубитов требуется 2^N–1 комплексных чисел, а операции над ними требуют экспоненциально растущих с ростом числа кубитов ресурсов.

Иными словами, преимущество квантового компьютера перед классическими – самое важное и единственное – состоит в использовании многомерности гильбертова пространства состояний квантовой системы, которое растет как 2^N (N – число кубитов) и присущему самой природе квантового мира **параллелизму** (поворот вектора состояния системы в этом пространстве за один шаг). В этом смысле квантовые компьютеры могут быть отнесены к категории **параллельных вычислителей**.

Квантовые вычисления

Для описания изменений, которые происходят с состоянием квантовых вычислительных систем, используется язык т. н. квантовых вычислений. По аналогии с классическим компьютером, который состоит из электрических схем, содержащих провода и логические элементы (ЛЭ), квантовый компьютер строится из квантовых схем, состоящих из каналов связи и элементарных квантовых ЛЭ, позволяющих передавать квантовую информацию и манипулировать ею. По аналогии с классическими ЛЭ, простейшими квантовыми логическими элементами являются однокубитовый элемент NOT и двухкубитовые элементы (см. врезку). Существует т. н. *теорема полноты*, которая говорит, что любой многокубитовый ЛЭ может быть составлен из CNOT и однокубитовых элементов. Наиболее известным трехкубитовым ЛЭ является, например, обратимый ЛЭ Тоффоли.

Важным является вопрос, можно ли любому классическому ЛЭ сопоставить квантовый ЛЭ, как, например, для NOR и CNOT? Ответ оказывается отрицательным, поскольку многие классические ЛЭ *необратимы*. (Еще в 1961 году исследователь из IBM Рольф Ландауер показал, что любое самое совершенное классическое вычислительное устройство на базе необратимой логики выделяет тепло при потере любого бита информации в нем. Известно, однако, что организация вычислений с помощью т. н. консервативной или «сохраняющей» логики без уничтожения информации не подпадает под принцип Ландауера и позволяет создавать энергоэффективные процессоры).

Например, по выходному значению элемента XOR невозможно определить, каковы были входные состояния, т. е. происходит безвозвратная потеря информации. В противоположность этому унитарные квантовые элементы всегда обратимы, и, следовательно, результат, полученный на выходе квантового ЛЭ, всегда может быть инвертирован другим квантовым ЛЭ. Поэтому квантовые схемы не всегда могут использоваться для непосредственного моделирования классических схем. Однако любую классическую схему можно заменить эквивалентной, которая содержит только обратимые ЛЭ, например ЛЭ Тоффоли. То есть квантовый ЛЭ Тоффоли, как и классический, можно использовать для моделирования необратимых классических ЛЭ. А это значит, что квантовые компьютеры могут

выполнять любые вычисления, которые возможно осуществить на классическом компьютере.
Преимущество квантового компьютера перед классическим, однако, не в этом, а в высокой степени параллелизма операций в многомерном гильбертовом пространстве состояний квантового компьютера. Вопрос лишь в том, существуют ли такие алгоритмы квантовых вычислений, которые позволяют это преимущество реализовать.

Квантовые алгоритмы

Такие алгоритмы существуют, но их немного. В их основе лежит т .н. *квантовый параллелизм*. Существует три класса квантовых алгоритмов, имеющих преимущество над известными классическими алгоритмами (см. врезку выше).
Первый основан на квантовом

Преимущество квантового компьютера перед классическими состоит в использовании многомерности гильбертова пространства состояний квантовой системы

преобразовании Фурье. К этому классу относится алгоритм Дойча–Джоза, который заключается в определении, является ли функция двоичной переменной f(x) постоянной (принимает либо значение 0, либо 1 при любых аргументах) или сбалансированной (для половины области определения принимает значение 0, для другой половины – 1), а также алгоритмы Шора для задач факторизации и вычисления дискретного логарифма. Сравнение времени факторизации чисел, представленных разным числом бит на классическом и квантовом компьютерах, приведено на рисунках. Второй класс алгоритмов – это квантовый алгоритм поиска (алгоритм Гровера) – быстрый квантовый алгоритм решения задачи поиска в пространстве из N элементов. Квантовый алгоритм Гровера позволяет решить задачу поиска за время порядка квадратного корня из классического, что является огромным ускорением. Наконец, третий класс алгоритмов – квантовое моделирование, при котором квантовый компьютер используется для моделирования самой квантовой системы.

Size of modulus (bits)	1,024	2,048	4,096
Factoring time in 1997	10^7 years	$3x10^{17}$ years	$2x10^{31}$ years
Factoring time in 2006	10^9 years	$5x10^{15}$ years	$3x10^{29}$ years
Factoring time in 2015	2,500 years	$7x10^{13}$ years	$4x10^{27}$ years
Factoring time in 2024	38 years	10^{12} years	$7x10^{25}$ years
Factoring time in 2033	7 months	$2x10^{10}$ years	10^{24} years
Factoring time in 2042	3 days	$3x10^8$ years	$2x10^{22}$ years

Время факторизации на классическом компьютере

Size of modulus (bits)	512	1,024	2,048	4,096
Quantum memory (qubits)	2,564	5,124	10,244	20,484
Number of quantum gates	$3x10^9$	$3x10^{10}$	$2x10^{11}$	$2x10^{12}$
Quantum factoring time	33 seconds	4.5 minutes	36 minutes	4.8 hours

Время факторизации на квантовом компьютере

Как работает квантовый компьютер?

Принципиальная схема работы любого квантового компьютера выглядит следующим образом (см. врезку). Ее основной компонент – квантовый регистр – совокупность определенного числа кубитов.
Прежде чем осуществить ввод информации в квантовый компьютер, необходимо провести подготовку начального состояния кубитов регистра – *инициализацию*. В результате этой операции все кубиты регистра должны быть переведены в основные базисные состояния так, что состояние регистра можно записать как $|0_1>, |0_2>, |0_3>, ..., |0_N> \equiv |0_1, 0_2, 0_3, ..., 0_N>$. Задача инициализации сама по себе является сложной и в случае, когда в роли кубитов, например, выступают атомы или ионы, - для перевода регистра в основное состояние требуется глубокое охлаждение (до температур порядка единиц микрокельвин), и в случае фотонов – необходимо использовать поляризационные методы.
После того как регистр данных переведен в основное состояние, каждый кубит регистра можно перевести в неосновное состояние $|1>$ путем селективного воздействия (например, при помощи импульсов внешнего электромагнитного поля), а весь регистр при этом

перейдет в суперпозицию базисных состояний, задающую число в двоичной системе.
На следующем этапе необходимо произвести ввод информации, т. е. преобразовать состояние входного регистра в когерентную суперпозицию базисных состояний. Это можно сделать, например, при помощи импульсных воздействий на систему. В таком виде информация поступает на вход основного элемента квантового компьютера – квантового процессора, выполняющего последовательность квантовых логических операций. Последним этапом является считывание результата, т. е. измерение состояния кубитов на выходе.

Прототипы квантовых компьютеров

Построение работающего прототипа квантового компьютера является одним из вызовов физики XXI века. В настоящее время уже построены прототипы, оперирующие с десятками кубит, но вопрос о масштабировании таких устройств пока является открытым. Принципиальная проблема, которую сама Природа создала на пути масштабирования квантовых вычислительных устройств, – это проблема быстрой декогеренции квантовых состояний кубитов из-за их взаимодействия с окружающей средой. Если бы не эта проблема, квантовый компьютер можно было бы масштабировать до масштабов Вселенной. Ведь Вселенная – самая большая из известных нам физических систем и на подчиняется законам квантовой физики.
Недавно ученый из США С. Лойд подсчитал, что представляет из себя Вселенная с информационной точки зрения. По его оценкам, Вселенную можно рассматривать как квантовый компьютер с емкостью памяти 10^{90} бит, который за время своего существования (со времени большого взрыва) выполнил 10^{120} элементарных логических операций.
Во многих лабораториях в США, Европе, России, Японии и Австралии разрабатываются различные прототипы квантовых вычислительных устройств, базирующихся на следующих основных технологиях: (i) твердотельные квантовые точки на полупроводниках, (ii) сверхпроводящие элементы (джозефсоновские переходы, сквиды и др.), (iii) ионы в вакуумных ловушках Пауля (или атомы в оптических ловушках), (iv) смешанные технологии (например, фотоны в линейных оптических системах, фотоны в микрорезонаторах и др.).
На рубеже XX-XXI веков во многих научных лабораториях были созданы однокубитные квантовые процессоры. Вскоре был продемонстрирован жидкостной ЯМР-квантовый компьютер (IBM, до 7 кубит). В 2005 году был построен двухкубитный квантовый процессор на сверхпроводящих элементах (NEC, Япония). Примерно в это же время прототипы до десятка кубит были продемонстрированы на ионах и атомах в ловушках (США, Австрия, Германия). В 2009 году исследователи из Йельского университета (США) создали первый простейший твердотельный квантовый компьютер – двухкубитный сверхпроводящий чип, который был способен выполнять простейшие квантовые алгоритмы. Команда ученых из Бристольского университета (Великобритания) также создала полупроводниковый чип для квантовых вычислений, основанный на принципах квантовой оптики и использующий обычные оптические элементы (зеркала, преломляющие пластинки и т. п.). На этом чипе была продемонстрирована работа алгоритма Шора.
В феврале 2007 года канадская компания D-Wave Systems (www.dwavesys.com) представила первый работающий прототип квантового компьютера Orion, основанный на 16-кубитовом чипе. В декабре 2008 года компания дала старт проекту распределенных вычислений на базе адиабатических квантовых алгоритмов, реализуемых на адиабатических сверхпроводящих квантовых компьютерах D-Wave. 11 мая 2011 года был представлен компьютер D-Wave One, созданный на базе 128-кубитного процессора (см. врезку), который оперирует внутри криогенной системы внутри антимагнитной камеры (чтобы устранить влияние внешних магнитных полей) размером 10 кв. м. ????
В планах компании – масштабировать чип до 1024 кубитов, и она заключила контракт с корпорацией Lockheed Martin на разработку и применение таких квантовых процессоров для нужд корпорации.
В России физикой квантовой информации и разработкой прототипов квантовых компьютеров и квантовых вычислительных устройств занимается ряд исследовательских групп в Физико-технологическом институте РАН, Физическом институте им. Лебедева РАН, Институте спектроскопии РАН, Институте лазерной физики РАН, МГУ, МФТИ, и ряде других.
До создания полноценного квантового компьютера, однако, еще далеко.
В ближайшие 20-30 лет, видимо, будут созданы работающие прототипы квантовых компьютеров с практически значимым числом кубитов, чтобы выполнять квантовые алгоритмы для решения реальных задач, прежде всего квантовой физики, материаловедения и т. п., а также специализированные квантовые компьютеры типа разрабатываемых компанией D-Wave Systems.
Отметим, что когда такие квантовые компьютеры созданы, они станут эффективнее классического компьютера лишь для решения ограниченного класса задач, которые мы обсуждали выше.
Так что ответ на вопрос в заголовке статьи – потеснит ли квантовый компьютер классические? – отрицательный. Нет, в обозримом будущем не потеснит.