Квантовая механика и развитие информационных технологий[1]

Ю.И. Богданов, А.А. Кокин, В.Ф. Лукичев, А.А. Орликовский, И.А. Семенихин, А.Ю. Чернявский

Аннотация. Представлено общее введение в проблематику квантовых информационных технологий и квантовых компьютеров. В основе новых технологий лежат квантовые биты информации - кубиты, способные находиться не только в базисных состояниях «ноль» и «единица», но и в квантовой суперпозиции этих состояний. Надежды ученых и инженеров связаны с тем, что квантовые компьютеры, когда они будут созданы, станут незаменимыми при моделировании квантовых систем, а также при решении некоторых других задач, которые недоступны классическим компьютерам.

Ключевые слова: информационные технологии, квантовые компьютеры, кубиты, квантовые вентили, нанотехнологии, высокопроизводительные вычисления.

Введение. Закон Мура и развитие информационных технологий

Бурный рост информационных технологий (ИТ) оказывает огромное влияние на жизнь всего современного мирового сообщества. Неуклонно возрастает число людей, работающих в этой области, ИТ широко востребованы в науке, образовании и промышленности, создается глобальное информационное пространство с использованием сети Интернет, радикально меняются традиционные концепции телевидения, радио, средств коммуникации и т.п.

Исторический анализ показывает, что информационные технологии растут экспоненциально быстро. В целом, развитие ИТ следует так называемому закону Мура, который основан на эмпирических наблюдениях, сделанных сотрудником Intel Гордоном Муром еще на заре интегральной микроэлектроники в 1965 году [1].

Проанализировав развитие микроэлектроники в течение нескольких первых лет с момента ее рождения, Мур представил прогноз, согласно которому число транзисторов в микросхеме будет удваиваться примерно каждые 2 года.

Интенсивное развитие микроэлектроники на протяжении последних более чем 50 лет вполне соответствует закону Мура. Для иллюстрации, на Рис. 1 представлена зависимость числа транзисторов в микропроцессорах за период с 1971 по 2011 годы. Представленная зависимость демонстрирует удвоение числа транзисторов каждые два года. Построено по данным компаний Intel (www.intel.com) и AMD (www.amd.com).

Фактически, экспоненциальному закону Мура приближенно следуют самые различные характеристики полупроводниковых устройств: увеличение скорости обработки данных, рост объема памяти, уменьшение критического размера технологии, снижение стоимости изделия в расчете на отдельный транзистор и т.п. Такое экспоненциальное улучшение характеристик приборов привело к резкому повышению роли микроэлектроники во всех областях экономики и социальной сферы. В результате, информационные технологии стали локомотивом развития современной цивилизации начиная со второй половины 20-го века и по сей день.

Технология суперкомпьютеров и параллельных вычислений также не стоит в стороне от

[1] Работа выполнена при поддержке Программы Президиума РАН по фундаментальным исследованиям.

описываемых тенденций и пытается использовать выгоды, даваемые законом Мура. Каждый раз, когда на пути дальнейшего увеличения производительности возникало, на первый взгляд, непреодолимое препятствие, находилось решение, позволяющее его обойти. Например, после того, как тактовая частота процессоров перестала увеличиваться в связи с проблемами отвода тепла, получили широкое распространение многоядерные архитектуры. В вычислениях стали использоваться графические процессоры, содержащие многие сотни процессорных ядер.

Ожидается, что тенденция, описываемая законом Мура, сохранится примерно до 2020 года. На фундаментальном уровне, предел миниатюризации транзисторов, в любом случае, ограничен размерами атомов. Ожидается, однако, что существенные трудности, вызванные неконтролируемым квантовым туннелированием, возникнут еще раньше (начиная с технологии примерно ниже 15 нанометров для затворов размером в 5 нанометров и менее). В суперкомпьютерной области дальнейшему экспоненциальному возрастанию вычислительной мощности может помешать такое же экспоненциальное увеличение потребляемой компьютером электроэнергии. Уже сейчас самые мощные петафлопсные суперкомпьютеры потребляют мегаватты электроэнергии. Если провести простую экстраполяцию, то для работы экзафлопсного суперкомпьютера потребуются уже гигаватты.

Тенденции, описываемые законом Мура, смогут продолжаться и после 2020 года, если на смену имеющимся технологиям придут новые технологии, такие как оптические, молекулярные и квантовые компьютеры. Нижеследующий текст посвящен описанию надежд, которые исследователи в области квантовых информационных технологий (КИТ) связывают с квантовыми компьютерами. В настоящее время квантовая информатика представляет собой новую, быстро развивающуюся отрасль науки, связанную с использованием квантовых систем для реализации принципиально новых методов коммуникации и вычислений (квантовые каналы связи, квантовая криптография, квантовый компьютер) [2-8]. Мы увидим, что некоторые основополагающие квантовые эффекты, которые сейчас зачастую рассматриваются как помеха на пути технологии микро- и наноэлектроники, могут оказаться источником радикальных новаций в области вычислений.

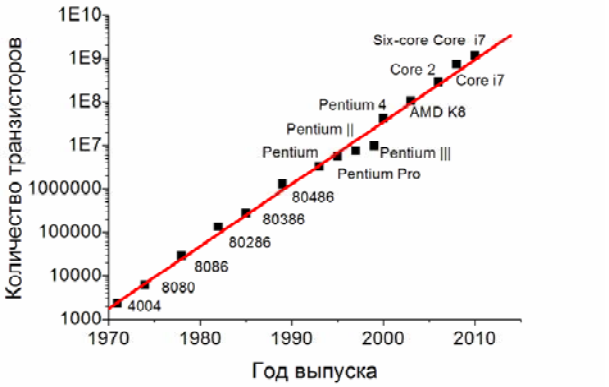

Рис. 1. Зависимость числа транзисторов в микропроцессорах от времени выпуска

По оценке известного американского физика Джона Арчибальда Уилера (1911- 2008), примерно одна треть ВВП (валового внутреннего продукта) Соединенных Штатов Америки непосредственно основана на достижениях квантовой механики. Это и не удивительно, если учесть, что на этой науке построена практически вся электроника, нанотехнологии, лазерные технологии, атомная промышленность, новые химические материалы и препараты и т.п. Успешное развитие указанных отраслей невозможно без проведения подробных расчетов квантовых систем, таких как наноструктуры, сложные химические и биологические молекулы, новые лекарства и т.п. Однако, несмотря на впечатляющие успехи в изучении фундаментальных законов Природы, полномасштабное моделирование сложноорганизованных квантовых систем все еще остается практически неосуществимой задачей.

Проиллюстрируем сказанное примером. Для полномасштабного моделирования квантовых свойств атома железа нужно рассматривать движение всех его 26 электронов в трехмерном пространстве, что приводит к необходимости решать уравнение Шредингера в конфигурационном пространстве размерности 26*3=78 (и это без учета спинов электронов, которые делают динамику еще более сложной). Если взять весьма грубую сетку, которая делит каждую координату всего на 10 частей, то

понадобится 10^{78} узлов для реализации соответствующей разностной схемы. Такого рода моделирование никогда не сможет быть осуществлено хотя бы потому, что полное число элементарных частиц во Вселенной, таких как протоны и нейтроны, также «всего» порядка 10^{78}. Таким образом, для моделирования всего одного и далеко не самого сложного атома требуется ресурс, который превышает механический ресурс всей Вселенной.

Мы видим, что квантовые задачи, за исключением простейших, являются алгоритмически очень сложными (практически неосуществимыми) для вычислений на классическом компьютере. Из этого, давно известного и, на первый взгляд, негативного наблюдения Фейнман в 1982 г. сумел сделать позитивный вывод [9, 10]. Раз Природа с успехом решает эти задачи, то, может быть, и мы могли бы использовать квантовые системы в качестве некоторой новой элементной базы для вычислений. Компьютеры, основанные на квантовых логических элементах, могли бы быть намного более мощными по сравнению со своими классическими собратьями. Интересно, что за два года до Фейнмана в 1980 г. похожие идеи выдвигал российский математик Юрий Манин в своей небольшой, но очень содержательной книге «Вычислимое и невычислимое» [11].

1. Алгоритм Шора и некоторые другие квантовые алгоритмы

Важным примером, на котором можно продемонстрировать радикальное преимущество квантовых алгоритмов над классическими, является так называемая задача факторизации, связанная с разложением целого числа на простые множители. Оказывается, что в то время как умножение многозначных чисел - это алгоритмически простая задача, обратная задача (разложение на множители) алгоритмически очень сложная (обладает экспоненциальной сложностью).

Наилучший известный на сегодня классический алгоритм факторизации некоторого числа (так называемый метод решета числового поля - general number field sieve) требует для реализации следующее число операций:

$$L_{class} \approx \exp\left(\left(64/9\right)^{1/3} n^{1/3} \left(\ln\left(n\right)\right)^{2/3}\right), \qquad (1)$$

где $n = k \cdot \ln(10)$ - число двоичных знаков, а k- число соответствующих десятичных знаков, задающих это число.

Квантовый алгоритм факторизации, предложенный П. Шором в 1994 году, требует выполнения числа операций, выражаемого следующей формулой [12]:

$$L_{quant} \approx n^2 \ln\left(n\right) \ln\left(\ln\left(n\right)\right). \qquad (2)$$

Сравнение формул (1) и (2) показывает, что алгоритм Шора превращает экспоненциально сложный алгоритм в алгоритм полиномиальной сложности. Например, современный классический суперкомпьютер петафлопсного диапазона (10^{15} операций с плавающей запятой в секунду) позволяет разложить число с $k = 500$ десятичными знаками за 5 миллиардов лет. Ту же задачу квантовый компьютер мегагерцового диапазона (1 млн. операций в секунду) решает за 18 секунд. Аналогично, для числа с $k = 1000$ десятичными знаками трудоемкость классического алгоритма составляет $4 \cdot 10^{20}$ лет, а квантового – 84 секунды. Очевидно, что даже переход к суперкомпьютерам экзафлопсного диапазона (10^{18} операций в секунду) не изменит существенно ситуацию.

В основе экспоненциального ускорения в алгоритме Шора лежит так называемое квантовое преобразование Фурье. Для массива комплексных амплитуд длины N число операций, необходимых для осуществления квантового преобразования Фурье, есть величина порядка $O\left(\left(\log N\right)^2\right)$. Отметим, что самые быстрые классические алгоритмы выполняют преобразование Фурье за $O\left(N\left(\log N\right)\right)$ операций (так называемое быстрое преобразование Фурье). Таким образом, квантовый алгоритм имеет экспоненциальное преимущество по сравнению со своим классическим аналогом. Пусть, например, имеется 1000- кубитовое состояние ($n = 1000$). Ему отвечает вектор состояния, описываемый $N = 2^n = 1{,}07 \cdot 10^{301}$ комплексными числами. Для осуществления классического быстрого преобразования потребуется проделать порядка $N \log_2 N = 1{,}07 \cdot 10^{304}$ операций. В то же время квантовое преобразование над рассматриваемым

вектором осуществляется примерно за $\left(\log_2 N\right)^2 = 1 \cdot 10^6$ операций.

Важно отметить следующее. Все известные на сегодня алгоритмы разложения числа на простые множители на классическом компьютере являются экспоненциально сложными. Если бы удалось доказать, что полиномиального алгоритма в задаче факторизации чисел не существует вообще, то тем самым удалось бы доказать абсолютное превосходство квантовых алгоритмов над вероятностными классическими. Этот результат установил бы неравенство классов сложности BPP и PSPACE, вопрос о взаимоотношении которых является одной из ключевых открытых проблем современной теоретической информатики.

Еще один важный метод, иллюстрирующий квантовый параллелизм и имеющий важное методическое значение дает алгоритм Дойча-Джозсы. Суть этого результата заключается в следующем. Рассматривается функция $f(x)$ с n-битовой областью определения и 1- битовым множеством значений (n - число кубитов). Переменная x может принимать n различных значений x=0,1,… N-1, где $N=2^n$. Заранее известно, что функция $f(x)$ может быть только одного из двух типов: постоянная функция или так называемая сбалансированная функция. Для постоянной функции $f(0)=f(1)=\ldots=f(N-1)$. Если функция сбалансирована, то $f(x)=0$ для некоторых x и $f(x)=1$ для остальных значений аргумента, причем значения $f(x)=0$ и $f(x)=1$ встречаются одинаково часто (в этом и заключается сбалансированность). Пусть, например, имеется функция $f(x)$ с 10-ти битовой областью определения. Тогда для некоторых 512 значений x получим $f(x)=0$, а для остальных 512 значений x получим $f(x)=1$. Задача Дойча-Джозсы как раз и состоит в том, чтобы отличить постоянную функцию от сбалансированной. Оказывается, что алгоритм Дойча-Джозсы позволяет с достоверностью решить такую задачу посредством одного единственного обращения к вычислителю, который определяется некоторым унитарным преобразованием U_f. В то же время, при классическом рассмотрении задачи Дойча-Джозсы, для того чтобы с достоверностью отличить постоянную функцию от сбалансированной может потребоваться до $2^{n-1}+1$ обращений к устройству, производящему вычисление функции $f(x)$.

В качестве еще одного замечательного результата стоит упомянуть алгоритм Гровера, который направлен на решение задач перебора, например, поиска записи в неструктурированной базе данных. Алгоритм Гровера обеспечивает поиск решения за $O\left(\sqrt{N}\right)$ шагов в базе из N элементов. Заметим, что классический алгоритм не способен решить задачу быстрее, чем за $O(N)$ шагов. Фактически, при помощи алгоритма Гровера можно получать квадратичное ускорение на NP полных задачах.

Заметим, что алгоритм Гровера, как и квантовое преобразование Фурье, смогут найти широкое применение в качестве важнейших составных частей при моделировании квантовых систем на квантовых компьютерах. В то же время, алгоритм факторизации Шора имеет большое значение для задач криптографии. Создание полномасштабных квантовых компьютеров и соответствующая реализация алгоритма Шора сделают беззащитными системы классической криптографии с открытым ключом, такие как RSA код, который сейчас используют для защиты информации в банковской сфере и Internet.

Таким образом, квантовые компьютеры, когда они будут созданы, позволят решать задачи полномасштабного моделирования сложноорганизованных квантовых систем, недоступные никаким классическим компьютерам, а также некоторые другие важные задачи.

Важно отметить, что на пути создания квантового компьютера и квантовых алгоритмов встает множество задач, которые в силу экспоненциального роста сложности относительно числа кубитов требуют больших вычислительных ресурсов. Например, для анализа работы шестнадцатикубитового квантового регистра требуется работа с матрицами размера $2^{16} \times 2^{16}$. Работа с такими матрицами неподвластна современным персональным компьютерам, однако может быть проделана при помощи суперкомпьютеров. Примеров успешного применения высокопроизводительных вычислений в квантовой информатике довольно много.

Конечно же, добавление лишь нескольких десятков кубитов поднимает данные задачи на уровень, недоступный никаким суперкомпьютерам, но это как раз и означает, что использование наиболее прогрессивных вычислительных технологий является критически важным фактором для развития КИТ.

2. Кубит vs. бит (логический анализ)

Основным элементом квантового компьютера является квантовый бит (кубит), представляющий собой двухуровневую квантовую систему. В качестве кубитов могут выступать ионы, атомы, электроны, фотоны, спины атомных ядер, структуры из сверхпроводников и многие другие физические системы. Проведем краткое сравнение кубита с физической реализацией классического бита информации на основе двоичного триггера с двумя устойчивыми состояниями.

Так же как и классический бит, кубит может находиться в двух базисных состояниях $|0\rangle$ и $|1\rangle$. Пусть в качестве кубита выступает, например, атом. Пусть, как показано на Рис. 2, $|0\rangle$ - это основное состояние, а $|1\rangle$ - некоторое возбужденное долгоживущее состояние. Именно эти состояния и образуют кубит. Конечно, кроме указанных состояний, у атома есть и много других состояний (одно из таких состояний, обозначенное как $|2\rangle$, представлено на рисунке). Однако мы можем сделать так, что все другие возбужденные состояния остаются невозмущенными, если будем управлять кубитом с помощью лазерного излучения, частота которого близка к частоте перехода ω_{01} между состояниями кубита $|0\rangle$ и $|1\rangle$ (только этот переход оказывается в резонансе с полем лазера, все остальные степени свобода атома будут практически заморожены). Пусть вначале атом не возбужден, т.е. находится в состоянии $|0\rangle$. Перевод системы из состояния $|0\rangle$ в состояние $|1\rangle$ осуществляется с помощью так называемого π-импульса, который задается путем выбора длительности импульса лазерного излучения и напряженности его электрического поля. Если же атом находится в возбужденном

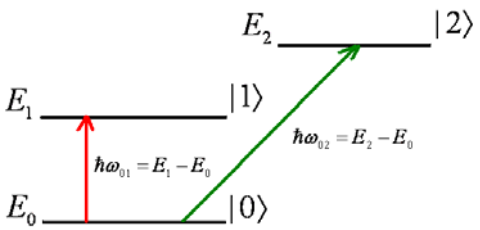

Рис. 2 Квантовый бит (кубит) на примере энергетических уровней атомов

состоянии (на уровне $|1\rangle$) и на него еще раз подействовать π-импульсом, то атом перескочит обратно в состояние $|0\rangle$. Такое поведение полностью аналогично поведению классического бита и, если бы все ограничивалось этим, то не было бы никакой разницы между классической и квантовой информацией.

Однако давайте теперь рассмотрим, что произойдет, если подействовать на атом не π-импульсом, а импульсом вдвое меньшей длительности, т.е. импульсом $\pi/2$? В этом случае атом начнет свой переход из состояния $|0\rangle$ в состояние $|1\rangle$, но не успеет завершить его. В результате, как оказывается, возникнет состояние квантовой статистической неопределенности, которое мы можем условно записать как состояние суперпозиции $\left(|0\rangle+|1\rangle\right)/\sqrt{2}$. В этой записи нет ничего таинственного. Она означает, что кубит может с вероятностью ½ оказаться в состоянии $|0\rangle$, а с такой же вероятностью ½ - в состоянии $|1\rangle$ (см. ниже). Здесь $1/\sqrt{2}$ - амплитуда вероятности, а вероятность, в соответствии с законами квантовой механики, есть квадрат модуля амплитуды. Такое поведение кубита обусловлено его фундаментальной информационной ограниченностью (между показанными на рисунке уровнями $|0\rangle$ и $|1\rangle$ просто нет никаких «полочек», на которых атом мог бы «остановиться» по пути от одного состояния к другому).

Как хорошо известно, поведение классического бита информации совсем другое. Например, в микросхемах на основе ТТЛ, логический ноль представляется определенным низким напряжением в диапазоне от нуля до 0.8 В, в то время как логическая единица – определенным уровнем высокого напряжения в диапазоне

от 2.4 до 5.0 В. При этом, конечно, в системе физически возможны и любые другие промежуточные значения напряжения между логическими нулем и единицей, которые фактически отвечают неисправности схемы. В отличие от квантового бита, классический бит представляет собой физическую систему с практически неограниченным числом степеней свободы и состояний, среди которых условно выбираются «ноль» и «единица». Таким образом, самое главное (и фундаментальное) отличие кубита от классического бита состоит в том, что в основе первого лежит естественное квантование информации, в то время как в основе второго - искусственная дискретизация аналогового сигнала.

Информационная ограниченность квантовых систем приводит к необходимости их статистического описания. Согласно квантовой механике, состояние физической системы задается с помощью таких объектов как волновая функция и матрица плотности, которые, образно говоря, составляют “полный каталог знаний”, позволяющий правильно рассчитать вероятности исходов любых будущих измерений. Таким образом, в самой сердцевине квантовой теории оказывается вероятностный (статистический) аспект. Индивидуальные результаты наблюдений становятся объективно случайными; другими словами, квантовые случайные события происходят самопроизвольно и не определяются какими- либо явными или скрытыми причинами, в отличие от классических случайных событий, которые связаны с субъективными случайностями. Действительно, результаты классических испытаний, таких как бросание монеты или игральной кости, только выглядят как случайные из-за нашего незнания точных начальных условий (заметим попутно, что для того, кто оснащен измерительной аппаратурой, скоростной видеосъемкой и т.п., ничего случайного в рассматриваемых явлениях нет; такой наблюдатель вполне может предсказать результат испытания “на лету” и даже может сам управлять этим результатом, вовремя подхватив, например, брошенную монету).

Важно отметить, что статистическая неопределенность квантовых систем, в отличие от классических, является управляемой. Так, упомянутое выше состояние $\left(|0\rangle+|1\rangle\right)/\sqrt{2}$ не несет в себе никакой энтропийной неопределенности. Энтропия этого состояния оказывается равной нулю, поскольку посредством преобразования $-\pi/2$ (либо, что то же самое, $3\pi/2$) оно может быть обратно приведено в состояние «ноль». Такое управление было бы невозможно, если бы мы имели просто классическую ситуацию, когда половина представителей ансамбля находятся в состоянии «ноль», а половина - в состоянии «единица». В классическом случае вероятность является субъективной, поскольку пользователь просто «не знает» «истинного» состояния дел.

Заметим, что безэнтропийными являются все так называемые чистые состояния. Любое такое состояние можно посредством вполне определенного преобразования привести в состояние «ноль». Любое чистое состояние может быть задано посредством вектора состояния (волновой функции) в гильбертовом пространстве. Представленные выше обозначения, введенные Дираком, такие как $|0\rangle$, $|1\rangle$, $\left(|0\rangle+|1\rangle\right)/\sqrt{2}$ и т.п., как раз дают примеры векторов квантовых состояний. При этом состояния логического нуля и единицы оказываются ортогональными друг другу: $\langle 1|0\rangle=0$. Фундаментальное правило, открытое Борном и фон Нейманом и определяющее статистический аспект квантовой теории, гласит, что вероятность обнаружить систему в состоянии $|\varphi\rangle$ при условии, что она была приготовлена в состоянии $|\psi\rangle$, задается квадратом модуля их скалярного произведения:

$$F=\left|\langle\varphi|\psi\rangle\right|^2. \qquad (3)$$

Введенная величина F называется степенью согласованности или вероятностью совпадения квантовых состояний (fidelity). Если, например, $|\psi\rangle=\left(|0\rangle+|1\rangle\right)/\sqrt{2}$, а $|\varphi\rangle=|0\rangle$, то $\langle\varphi|\psi\rangle=1/\sqrt{2}$ и $F=1/2$.

Заметим, что наряду с чистыми состояниями существуют и так называемые смешанные состояния, описываемые в рамках формализма матрицы плотности и соответствующие некогерентным смесям чистых состояний. Смешанные состояния обладают энтропией, которую можно вычислить по формуле фон Неймана:

$$S = -\sum_j \lambda_j \log_2 \lambda_j . \quad (4)$$

Эта формула является квантовым аналогом формулы Шеннона (причем, в роли вероятностей выступают собственные значения матрицы плотности λ_j). Заметим, однако, что исторически формула фон Неймана возникла раньше, в 1932 г., в то время как Шеннон ввел свою энтропию только в 1948 г. Более того, по свидетельству Шеннона, сама идея использовать термин «энтропия» была подсказана ему фон Нейманом в частной беседе.

Смешанные состояния несут в себе ненулевую энтропию, обусловленную информационной связью квантовой системы с ее окружением. Эта связь приводит к своеобразному «уходу» информации из системы в окружение, в результате теряется квантовая когерентность системы и возможность автономного управления ее состоянием. Фактически вместо состояния собственно исходной квантовой системы возникает единое состояние более крупного объекта «система + окружение» (этим состоянием, однако, зачастую трудно или даже невозможно управлять практически).

3. Представление состояния кубита на сфере Блоха

Квантовое состояние кубита представляет собой суперпозицию двух базисных состояний физической системы:

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle = c_0\begin{pmatrix}1\\0\end{pmatrix} + c_1\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}c_0\\c_1\end{pmatrix}, \quad (5)$$

где условие $|c_0|^2 + |c_1|^2 = 1$ задает нормировку полной вероятности состояния кубита.

Оказывается, что все множество квантовых состояний кубита можно наглядно представить на так называемой сфере Блоха, очень похожей на глобус. Каждое чистое однокубитовое состояние задается точкой на сфере Блоха, положение которой определяется полярным θ и азимутальным φ углами (Рис. 3):

$$|\psi\rangle = \begin{pmatrix}\cos\left(\frac{\theta}{2}\right)\exp\left(\frac{-i\varphi}{2}\right)\\ \sin\left(\frac{\theta}{2}\right)\exp\left(\frac{i\varphi}{2}\right)\end{pmatrix}. \quad (6)$$

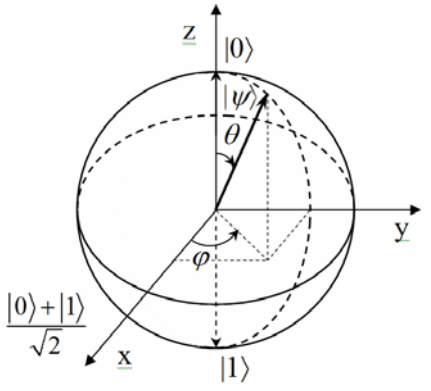

Рис. 3 Кубит на сфере Блоха

Кубит «живет» одновременно в абстрактном двумерном гильбертовом пространстве и в обычном трехмерном евклидовом пространстве. Вычислительные операции задаются посредством унитарных вращений на сфере Блоха. Оператор унитарных вращений на угол θ относительно единичной оси $\vec{n}$ определяется следующей формулой:

$$R_{\vec{n}}(\theta) = \exp\left(-i\theta\frac{\vec{\sigma}\vec{n}}{2}\right) = \cos\left(\frac{\theta}{2}\right)I - \sin\left(\frac{\theta}{2}\right)\vec{\sigma}\vec{n}\ , (7)$$

где $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$ - матрицы Паули, I - единичная матрица.

Параметры вращения на сфере Блоха (направление оси вращения и величина угла поворота) задаются теми физическими воздействиями, которые мы оказываем на квантовый объект (напряженностями полей, частотами, поляризациями, длительностью воздействий и т.п.). Аналогичное утверждение справедливо не только для отдельного кубита, но и для регистра из N кубитов (только теперь гильбертово пространство имеет размерность 2^N)

Таким образом, каждой точке сферы Блоха соответствует некоторое состояние кубита и каждому состоянию кубита - некоторая точка на сфере Блоха. Например, состояние $|0\rangle$ соответствует северному полюсу, а состояние $|1\rangle$ - южному полюсу. При воздействии $\pi/2$ импульса на невозмущенный атом, кубит движется от северного полюса до экватора вдоль некоторого меридиана (другими словами, происходит вращение вокруг оси y на Рис. 3).

Заметим, что, если бы мы взяли импульс не $\pi/2$, а вдвое короче, т.е. $\pi/4$, то кубит

в процессе своей эволюции остановился бы не на экваторе, а на широте 45 градусов в северном полушарии, а если бы мы взяли импульс $3\pi/4$, то оказались бы уже в южном полушарии на широте 45 градусов и т.д. Вообще, всегда можно подобрать некоторое воздействие на кубит, которое переведет его из одной произвольно заданной точки на сфере Блоха в любую другую, наперед заданную. Все преобразования такого рода принято называть унитарными вращениями. С помощью таких вращений можно осуществлять «навигацию» кубита на сфере Блоха (например, мы можем направить его из Москвы в Рио-де-Жанейро).

Но следует помнить, что эта красивая картинка только визуализация неопределенности квантового состояния. Как бы ни двигался кубит по глобусу, придуманному Блохом, он все равно в конце концов окажется либо на северном полюсе, либо на южном. Чем ближе кубит к северному полюсу, тем вероятнее, что при измерении он будет обнаружен в состоянии $|0\rangle$, а чем ближе он к южному полюсу, тем вероятнее, что он будет обнаружен в состоянии $|1\rangle$. В результате измерения происходит так называемый квантовый скачок. И где бы ни находился кубит, в результате квантового скачка он всегда оказывается на полюсе (северном или южном).

4. Квантовое измерение и квантовый скачок

Измерение является весьма сильным стрессовым воздействием на квантовую систему. Рассмотрим эту операцию на примере типичных измерений в атомах. Вспомним, что наряду с кубитовыми состояниями $|0\rangle$ и $|1\rangle$ у атома имеется и много других состояний. Рассмотрим одно из них, которое на Рис. 2 обозначено как $|2\rangle$. Удобно в качестве уровня $|2\rangle$ выбрать такой, который в отличие от уровня $|1\rangle$ является не долгоживущим, а короткоживущим. Это означает, что атом, оказавшись на этом уровне, долго там не задерживается, а весьма быстро перескакивает в основное состояние $|0\rangle$ (при таком перескоке, конечно, излучается фотон, который уносит имевшуюся у атома энергию возбуждения). До сих пор существование этого состояния не имело для нас решительно никакого значения, поскольку лазерное поле, которое мы использовали, было резонансным только по отношению к переходу между состояниями $|0\rangle$ и $|1\rangle$, а все другие состояния атома для этого поля практически не существовали. Но теперь сделаем активным переход между уровнями $|0\rangle$ и $|2\rangle$. Для этого используем лазерное излучение соответствующей частоты, близкой к частоте ω_{02} этого перехода. Теперь атом получает возможность активно эволюционировать между состояниями $|0\rangle$ и $|2\rangle$. Если уровень $|0\rangle$ окажется заселен, то новое лазерное поле неизбежно приведет к заселению и уровня $|2\rangle$, но поскольку время жизни на этом уровне мало, атом быстро излучит фотон в случайном направлении в пространстве и снова скатится на уровень $|0\rangle$, откуда под действием того же лазерного поля снова поднимется вверх, снова излучит фотон и снова скатится вниз (и так много раз подряд, в результате получится, что атом «засветится» - это явление называется лазерной флуоресценцией).

А теперь вспомним, что до измерения атом находился не в состоянии $|0\rangle$, не в состоянии $|1\rangle$, а в некотором состоянии квантовой статистической неопределенности (суперпозиции), которое мы описали ранее. Теперь, после того как мы сделали активным переход между состояниями $|0\rangle$ и $|2\rangle$, атом не может больше находиться в состоянии «задумчивости», он вынужден сделать выбор между двумя несовместимыми альтернативами: либо свалиться в состояние $|0\rangle$ и начать активно флуоресцировать, либо «спрятаться» от внешнего лазерного воздействия в состоянии $|1\rangle$, которое нечувствительно к прилагаемому лазерному полю. В результате, кубит, находящийся в произвольной точке сферы Блоха, вынужденно совершит квантовый скачок и окажется либо на северном полюсе (в состоянии $|0\rangle$), либо на южном полюсе - в состоянии $|1\rangle$. При этом если кубит осуществлял свою «навигацию» в северном полушарии, то, скорее всего, с вероятностью более 50% в соответствии с формулой (3) в

результате квантового скачка он окажется на северном полюсе, а если он был в южном полушарии, то, скорее всего, окажется на южном полюсе (конечно, не исключено, что кубит из широт северного полушария окажется на южном полюсе и, наоборот, кубит из широт южного полушария окажется на северном полюсе, но вероятность такого рода процессов заведомо ниже 50%).

Таким образом, имеет место своеобразный «закон инерции квантовой информации», согласно которому «всякая квантовая система продолжает удерживаться в своем состоянии квантовой статистической неопределенности, пока и поскольку информационное воздействие со стороны окружения не понуждает ее сделать выбор между различными альтернативами в пользу какой- то одной». В нашем примере, пока переход между состояниями $|0\rangle$ и $|2\rangle$ не был освещен, атому не было никакой нужды выбирать между $|0\rangle$ и $|1\rangle$, поэтому он мог бы находиться очень долго в состоянии «задумчивости» и «нерешительности»: выбрать $|0\rangle$ или $|1\rangle$? Но как только переход $|0\rangle$-$|2\rangle$ был освещен ярким светом, ему пришлось выбирать: либо быть в нуле, тогда нужно светиться, флуоресцировать, либо же «прятаться» на «темной» энергетической полке $|1\rangle$, нечувствительной к лазерному излучению с частотой ω_{02}.

5. Системы кубитов и квантовая запутанность

Двухкубитовое состояние представляет собой суперпозицию 4-х базисных состояний:

$$|\psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle, \quad (8)$$

где $|c_{00}|^2 + |c_{01}|^2 + |c_{10}|^2 + |c_{11}|^2 = 1$.

Основным ресурсом квантовых вычислений служит явление запутанности, не имеющее классического аналога. Явление квантовой запутанности приводит к тому, что квантовое состояние многокубитовой системы не сводится к описанию состояний отдельных кубитов, ее составляющих. Входя в состав квантового регистра, отдельный кубит как бы теряет свою индивидуальность, становясь частью единого целого.

Состояние системы, образованной двумя подсистемами, называется незапутанным, если оно может быть представлено в виде тензорного произведения векторов состояний отдельных кубитов:

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle. \quad (9)$$

В противном случае состояние называется запутанным. Для регистра из двух кубитов состояние (8) незапутанное, если выполняется условие:

$$c_{00}c_{11} - c_{01}c_{10} = 0. \quad (10)$$

Так, состояние $|\psi\rangle = \frac{1}{2}\left(|00\rangle - |01\rangle + |10\rangle - |11\rangle\right)$ является незапутанным, поскольку может быть представлено в виде тензорного произведения $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$. Напротив, состояние $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$ является запутанным, т.к. не может быть записано в виде прямого произведения состояний отдельных кубитов (представленное в этом примере состояние называется синглетным).

Мы видели, что двухкубитовое чистое состояние описывается четырьмя комплексными числами, аналогично можно показать, что трехкубитовое состояние задается с помощью 8-ми комплексных амплитуд, а состояние квантового регистра из N кубитов посредством 2^N комплексных чисел. Такой регистр описывается посредством $2^{N+1} - 2$ действительных параметров (две степени свободы вычитаются в силу условия нормировки, а также из-за произвола в выборе общей (глобальной) фазы состояния).

Заметим, что если бы в Природе не было явления запутанности, то для описания состояния квантового регистра было бы достаточно $2N$ действительных чисел (по два параметра на каждый кубит для описания его положения на сфере Блоха). Например, для регистра из 1000 кубитов без учета запутанности имеем только 2000 параметров, а с учетом запутанности таких параметров становится более чем 10^{300}.

Важно отметить, что возможность экспоненциального ускорения квантовых алгоритмов, о которой говорилось выше, основывается на ресурсе запутанности. Если максимальная

запутанность во время выполнения квантового алгоритма полиномиально зависит от числа кубитов, то такой квантовый алгоритм может быть промоделирован на классическом компьютере с полиномиальной памятью и за полиномиальное время.

Теория квантовой запутанности изучена далеко не полностью и ставит перед исследователями множество фундаментальных математических и физических задач.

Мы видим, что запутанность - это основной ресурс для новых квантовых информационных технологий. Для управления запутанностью может служить специальный логический квантовый вентиль (gate) CNOT (Controlled NOT – Управляемое НЕ). Вентиль CNOT меняет состояние управляемого (target) кубита при условии, что управляющий кубит находится в состоянии $|1\rangle$.

Действие оператора CNOT на базисные состояния двухкубитового регистра описывается следующей таблицей (таблица истинности):

$$\text{CNOT:} \quad \begin{array}{l} |00\rangle \to |00\rangle \\ |01\rangle \to |01\rangle \\ |10\rangle \to |11\rangle \\ |11\rangle \to |10\rangle \end{array}. \qquad (11)$$

Графически вентиль CNOT представлен на Рис. 4

Унитарное преобразование CNOT задается следующей матрицей

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \qquad (12)$$

Преобразование CNOT может переводить незапутанные состояния в запутанные, например $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |1\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |11\rangle)$ в синглет $\frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$.

Было показано, что любое квантовое вычисление может быть выполнено с помощью универсального набора одно- и двухкубитовых элементарных операций. В качестве универсального может служить набор из произвольных однокубитовых вращений на сфере Блоха

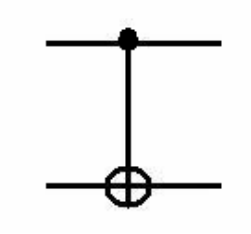

Рис. 4. Графическое изображение двухкубитового элемента CNOT

Верхний кубит является управляющим, нижний - управляемым. Символом $\oplus$ обозначена однокубитовая операция NOT над управляемым кубитом, когда управляющий кубит находится в состоянии $|1\rangle$

и двухкубитового элемента CNOT [13]. Так же, как и для классических компьютеров, можно обойтись и конечным числом гейтов, но в этом случае мы получим не точное произвольное преобразование, а его приближение с любой точностью.

Таким образом, состояние квантового процессора потенциально несет в себе огромное количество информации, поскольку N квантовых битов (кубитов) описываются 2^N комплексными числами (амплитудами). При этом, каждая амплитуда отвечает соответствующему классическому состоянию N-битной системы. Операция всего лишь на одном кубите может менять **сразу все** 2^N амплитуд состояния квантового процессора. Это явление лежит в основе квантового параллелизма.

Заметим, что такой параллелизм отличается от классического, в котором мы выполняем операции одновременно на многих процессорах или процессорных ядрах. В квантовом случае мы работаем с множеством амплитуд, но на одном физическом процессоре. В классических параллельных вычислениях увеличение производительности требует соответствующего, как правило, линейного физического масштабирования системы, при этом возрастают и ограничения на ее работу. Если использование небольшого количества ядер одного процессора накладывает не слишком сильные требований на параллельные алгоритмы, то использование кластеров заставляет решать проблему относительно медленной передачи данных между узлами. Использование графических адаптеров также ставит некоторые проблемы, например,

необходимость организации большого числа потоков и соответствующего взаимодействия центрального процессора с графическим адаптером. Вообще же, чем более параллельна классическая система, тем больше ограничений она накладывает на свое использование. И квантовые компьютеры здесь не являются исключением: несмотря на экспоненциальное число изменяющихся амплитуд за одну операцию, типы таких операций сильно ограничены. Существует, однако, еще одно кардинальное отличие. При работе квантового процессора отсутствует прямой доступ к отдельным амплитудам. Квантовый алгоритм должен, используя ограниченное число доступных простых операций, увеличить амплитуду, соответствующую классическому N-битному набору – правильному ответу задачи. В силу указанной особенности, эффективное использование квантового параллелизма представляет собой весьма нетривиальную задачу.

6. Общие требования, необходимые для реализации квантовых компьютеров

На Рис. 5 представлена схема идеального квантового компьютера [2, 3].

Следуя ДиВинченцо (DiVincenzo) [14], опишем пять условий, необходимых для реализации квантового компьютера.

1. Масштабируемые физические системы с хорошо определенными кубитами. Считается, что степень интеграции уровня $N = 1000$ (“один квантовый килобит”) обеспечит вычисления, заведомо недоступные никакому классическому компьютеру во Вселенной.

2. Возможность инициализации регистра кубитов в виде простого квантового состояния, принятого в качестве основного, например $|000...\rangle$.

3. Время декогерентизации (из-за взаимодействия с окружающей средой, «портящего» состояние), многократно превосходящее время выполнения отдельных элементарных операций (необходимо иметь ресурс времени, достаточный для выполнения алгоритма)

4. Универсальный набор квантовых вентилей (это ключевое требование для всей концепции

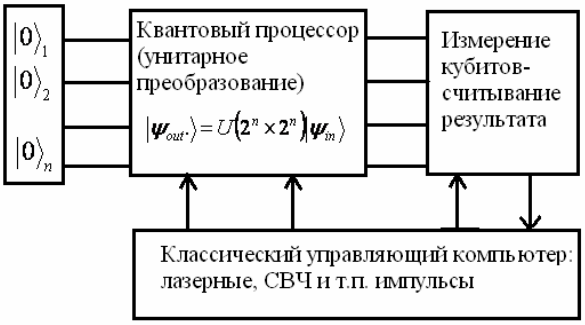

Рис. 5. Блок-схема идеального квантового компьютера

квантовых вычислений). Как уже отмечалось выше, универсальный набор образуют, например, произвольные однокубитовые элементы совместно с двухкубитовым элементом CNOT. Считается, что для реализации полномасштабного квантового компьютера нужно, чтобы отдельные квантовые вентили были изготовлены с прецизионно высокой точностью, при этом отклонение реального логического вентиля от идеального характеризуется вероятностью ошибки, которая не должна превышать величины порядка 10^{-4}-10^{-5} ($F = 0.9999 - 0.99999$).

5. Возможность измерения состояний отдельных кубитов на выходе квантового алгоритма с высокой точностью и надежностью.

Важно отметить, что наряду с описанной стандартной концепцией квантовых вычислений, в основе которой лежит универсальный набор квантовых логических вентилей, существуют и другие подходы. Примером может служить модель адиабатических квантовых вычислений [15]. Адиабатический квантовый компьютер основан на контролируемой адиабатической (т.е. достаточно медленной) эволюции многокубитовой квантовой системы. Рассматриваемая эволюция заканчивается в такой конфигурации, в которой гамильтониан системы обеспечивает решение поставленной задачи (система при этом все время находится в основном состоянии, которое медленно меняется со временем вместе с гамильтонианом). В этом случае стандартные требования ДиВинченцо должны быть модифицированы. Необходимо потребовать, в частности, чтобы в распоряжении исследователя имелся достаточно богатый набор возможных взаимодействий, способных изменять параметры гамильтониана системы

в широком диапазоне, а также, чтобы система была в достаточной мере охлаждена, и длительное воздействие не выводило бы систему из основного состояния.

Другим примером альтернативного подхода к квантовым вычислениям может служить так называемый односторонний квантовый компьютер (one-way quantum computer) [16-18]. В этом случае в качестве ресурса используется определенное запутанное состояние, называемое кластерным состоянием. Квантовое вычисление формируется посредством выбора различных однокубитовых измерений рассматриваемого кластерного состояния, при этом измерения необратимым образом разрушают запутанность, имевшуюся в исходном состоянии. Известно, что квантовые компьютеры на кластерных состояниях, равно как и адиабатические квантовые компьютеры эквивалентны по своей вычислительной мощности стандартным квантовым компьютерам на квантовых логических вентилях, но, возможно, их реализация окажется технологически более простой [17, 19].

Одним из основополагающих элементов успеха современных компьютерных технологий является наличие развитой теории кодов коррекции ошибок. На первый взгляд, серьезным препятствием для квантовых вычислений является непрерывное, а не дискретное, как у классического компьютера, множество ошибок. Однако, как оказалось, существуют коды, способные исправлять и квантовые шумы. Например, существует код, кодирующий один кубит пятью и позволяющий исправить произвольную квантовую ошибку в одном кубите. Примечательно, что многие (если не большинство) квантовых кодов использует при построении классические коды коррекции, например, линейные.

В настоящее время предложены и активно развиваются различные варианты реализации квантовых компьютеров. Здесь мы только перечислим некоторые возможные варианты. Более подробные сведения можно найти в недавнем обзоре [8].

К числу наиболее перспективных направлений следует отнести квантовые компьютеры на ионах в ловушках, которые опираются на такие высокоразвитые технологии, как электромагнитные ловушки (Пауля, Пеннинга и др.), лазерное охлаждение ионов, лазерное селективное управление квантовыми состояниями ионов и др. В качестве логических состояний $|0\rangle$ и $|1\rangle$ кубита в таких системах очень часто рассматриваются определенные энергетические уровни щелочноземельных ионов в условиях, когда запрещены электрические дипольные переходы. Именно на ионах в ловушках достигнут имеющийся на сегодня рекорд по числу кубитов (14 кубитов в регистре). Соответствующий результат получен недавно в группе проф. Блатта из Инсбрука (Австрия) [20]. Правда, нужно отметить, что речь идет не о полном контроле над состоянием регистра, а только о генерации так называемых GHZ- состояний.

На первом этапе развития квантовых информационных технологий наибольшие успехи были достигнуты для жидкостных ансамблевых квантовых компьютеров, в качестве кубитов в которых выступали атомные ядра со спином 1/2. Эти успехи были связаны с тем, что существует хорошо отработанная техника ядерного магнитного резонанса (ЯМР), позволяющая воздействовать на ядерные спины в макроскопическом объеме жидкости, оставаясь при этом при комнатных температурах. Достигнутый в настоящее время уровень технологии позволяет управлять системами, содержащими вплоть до 12 кубитов. Однако в таком компьютере при комнатных температурах амплитуда сигнала ЯМР экспоненциально уменьшается с ростом числа кубитов, что и приводит к ограничению возможного числа кубитов до 20-30 и делает невозможным создание масштабируемого компьютера. Масштабируемый квантовый компьютер может быть реализован (по крайней мере в принципе), если ядерные спины регулярным образом разместить в твердотельной подложке. Таков, например, кремниевый квантовый компьютер на ядерных спинах донорных атомов фосфора с индивидуальным обращением к кубитам. Однако, к сожалению, в подобного рода системах до настоящего времени пока не было продемонстрировано достаточно существенных результатов.

Другая перспективная твердотельная модель – это квантовые компьютеры на электронных состояниях в квантовых точках в полупровод-

никовых структурах. Преимущества этой схемы обусловлены высокой скоростью выполнения логических операций, возможностью измерения состояний отдельных кубитов (благодаря более высокой интенсивности сигнала по сравнению с отдельными ядерными спинами), более простыми по сравнению с ЯМР способами управления кубитами, а также тем, что рассматриваемые устройства могут работать при более высоких температурах, чем твердотельные ЯМР квантовые регистры. Трудности реализации рассматриваемой модели связаны с жесткими требованиями к технологии изготовления многокубитовых регистров, а также малыми временами релаксации электронных состояний по сравнению с такими же временами для ядерных спинов.

Важное направление современных исследований задают сверхпроводниковые квантовые компьютеры. Рассматриваемые устройства основываются на макроскопических квантовых явлениях, включая суперпозицию и запутанность макроскопических квантовых состояний. Квантовые состояния сверхпроводниковых кубитов управляются электромагнитными полями, контролирующими заряд, магнитный поток и фазу на переходах Джозефсона (зарядовый, потоковый и фазовый кубиты соответственно). Наиболее значительные достижения последних лет связаны с экспериментальным доказательством когерентности макроскопических квантовых состояний, способных образовывать суперпозиции и интерферировать, а также с созданием и исследованием устройств из нескольких кубитов. Увеличение времен декогерентизации на несколько порядков с ~1 нс до ~10мс и более обеспечило возможность реализации простейших квантовых алгоритмов. Серьезные трудности на пути реализации сверхпроводниковых квантовых компьютеров связаны с необходимостью жесткого контроля технологии джозефсоновских переходов, с неконтролируемыми флуктуациями напряжения на затворах, а также с неустранимым паразитным взаимодействием кубитов с электромагнитным окружением, приводящим к декогерентизации квантовых состояний.

Основное достижение проведенных до сих пор исследований состоит в практической демонстрации справедливости физических принципов, лежащих в основе идеи квантовых вычислений. Основные препятствия на пути реализации концепции полномасштабных квантовых компьютеров состоят в недостаточном уровне развития технологии изготовления квантовых регистров, в трудностях измерения и контроля квантовых состояний квантового регистра и необходимой степени подавления декогерентизации. Достигнутая в настоящее время в экспериментах точность реализации, характеризуемая вероятностью совпадения F между теоретическим и экспериментальным квантовыми состояниями, составляет всего 60-80%, в то время как требуемая точность должна быть 99.99% и более.

Наиболее узкое место в развитии квантовых информационных технологий связано с отсутствием должной методологии контроля квантовых состояний и процессов. Такая, основанная на квантовых измерениях, методология призвана обеспечить интерфейс между разработкой элементной базы квантовых компьютеров и ее практическим воплощением.

С целью существенного повышения уровня исследований в рассматриваемой области в Физико-технологическом институте РАН разработана новая методология управления качеством и эффективностью квантовых информационных технологий, основанная на анализе полноты, адекватности и точности реализации квантовых вентилей. Методы численного анализа и статистического моделирования с учетом результатов технологических и экспериментальных исследований позволяют дать исчерпывающую оценку качеству и эффективности проектируемых квантовых регистров, сформулировать требования к экспериментальному оборудованию и технологии. Развитый подход позволяет наилучшим образом распорядиться имеющимися ресурсами для оптимизации процесса разработки квантовых информационных технологий.

Эффективность предложенного подхода была продемонстрирована в работах, выполненных Физико-технологическим институтом РАН совместно с группой профессора С.П. Кулика из МГУ им М.В. Ломоносова и группой доктора Марко Дженовезе (Marco Genovese) из

INRIM (Италия) [21-24]. Развитая методология может быть применена к кубитам самой разной физической природы [25, 26].

Заключение

Представлен краткий обзор перспектив и трудностей создания квантовых компьютеров, призванных обеспечить полномасштабное моделирование сложных квантовых систем, что имеет чрезвычайно важное научное и практическое значение.

Описаны возможности основных квантовых алгоритмов, включая алгоритмы Шора, квантового преобразования Фурье, Дойча - Джозсы и Гровера.

Рассмотрены основные свойства квантового бита (кубита), системы кубитов, а также общие требования, необходимые для реализации полномасштабного квантового компьютера.

Литература

1. G.E. Moore Cramming more components onto integrated circuits// Electronics Magazine. 1965. V. 38. № 8. April 19.
2. Валиев К.А., Кокин А.А. Квантовые компьютеры: надежда и реальность. Ижевск. РХД. 2001. 352с.
3. Валиев К.А. Квантовые компьютеры и квантовые вычисления // УФН, 2005. том 175, №1. стр.3-39.
4. Нильсен М, Чанг И. Квантовые вычисления и квантовая информация. М. Мир. 2006. 824 с.
5. Прескилл Дж. Квантовая информация и квантовые вычисления. Том.1. М.-Ижевск. РХД. 2008. 464с.
6. Холево А.С. Введение в квантовую теорию информации. М. МЦНМО. 2002. 128с.
7. Физика квантовой информации. Квантовая криптография. Квантовая телепортация. Квантовые вычисления // Под. ред. Боумейстера Д., Экерта А., Цайлингера А.; Пер. с англ. под ред. Кулика С.П. и Шмаонова Т.А.. М. Постмаркет. 2002. 376с.
8. Богданов Ю.И., Валиев К.А, Кокин А.А. Квантовые компьютеры: достижения, трудности реализации и перспективы. Микроэлектроника. 2011. Т.40. №4. С.243-255.
9. Feynman R. Simulating Physics with Computers // Int. J. Theor. Phys. 1982. V.21. №6/7. P.467-488. См. перевод Фейнман Р. Моделирование физики на компьютерах // сб. «Квантовый компьютер и квантовые вычисления». Т.2. Ижевск. РХД. 1999. с.96-124.
10. Feynman R. Quantum Mechanical Computers // Found. of Phys. 1986. V.16. №6. P.507-531. См. перевод Фейнман Р. Квантовомеханические компьютеры // сб. «Квантовый компьютер и квантовые вычисления». Т.2. Ижевск. РХД. 1999. с.125-156.
11. Манин Ю.И. Вычислимое и невычислимое. М. Советское Радио. 1980. 128с.
12. Shor P. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. arXiv: quant-ph/ 9508027.1995. 28p.
13. Barenco A., Bennett C.H., Cleve C., DiVincenzo D.P., Margolus N., Shor P., Sleater T., Smolin J.A., Weinfurter H. Elementary Gates for Quantum Computation // Phys. Rev. A. 1995. V.52. №5. P.3457-3467
14. DiVincenzo D.P. The Physical Implementation of Quantum Computation. // Fortschr. der Phys., 2000, V.48, № 9-11, pp.771-783, arXiv:quant-ph/0002077.
15. Farhi E., Goldstone J., Gutmann S., Sipser M. Quantum Computation by Adiabatic Evolution // arXiv:quant-ph/0001106.
16. Raussendorf R., Briegel H. J. A one-way quantum computer.// Phys. Rev. Lett. 2001. V.86. P. 5188–5191.
17. Raussendorf R., Browne D.E., Briegel H.J. Measurement-based quantum computation on cluster states // Phys. Rev. A. 2003. V. 68. 022312.
18. Walther P., Resch K.J. Rudolph T., Schenck E., Weinfurter H., Vedral V., Aspelmeyer M., Zeilinger A. Experimental one-way quantum computing // Nature 2005. V.434. P.169–176.
19. Mizel A., Lidar D. A., Mitchell M. Simple proof of equivalence between adiabatic quantum computation and the circuit model. // Phys. Rev. Lett. 2007. 99, 070502.
20. T. Monz, P. Schindler, J.T. Barreiro, M. Chwalla, D. Nigg, W. A. Coish, M. Harlander, W. Hänsel, M. Hennrich, R. Blatt 14-Qubit Entanglement: Creation and Coherence // Phys. Rev. Lett. 2011. V.106, 130506
21. Bogdanov Yu.I., Brida G, Genovese M., Kulik S.P., Moreva E.V., and Shurupov A.P. Statistical Estimation of the Efficiency of Quantum State Tomography Protocols // Phys. Rev. Lett. 2010. V.105. 010404. 4p.
22. Богданов Ю.И., Кулик С.П., Морева Е.В., Тихонов И.В., Гавриченко А.К. Оптимизация протокола статистического восстановления поляризационных кубитов // Письма в ЖЭТФ. 2010. Т.91. вып.12. с.755-761.
23. Ю.И. Богданов, А.К. Гавриченко, К.С. Кравцов, С.П. Кулик, Е.В. Морева, А.А. Соловьев Статистическое восстановление смешанных состояний поляризационных кубитов // ЖЭТФ. 2011. Т.140. Вып.8. с. 224-235.
24. Yu. I. Bogdanov, G. Brida, I. D. Bukeev, M. Genovese, K. S. Kravtsov, S. P. Kulik, E. V. Moreva, A. A. Soloviev, A. P. Shurupov Statistical Estimation of Quantum Tomography Protocols Quality // Phys. Rev. A. 2011. V.84. 042108. 19 p.
25. Ю.И. Богданов Унифицированный метод статистического восстановления квантовых состояний, основанный на процедуре очищения // ЖЭТФ. 2009. Т.135. Вып.6.с.1068-1078.
26. Ю.И. Богданов, В.Ф. Лукичев, С.А. Нуянзин, А.А. Орликовский Квантовые шумы и контроль качества элементной базы квантовых компьютеров на сверхпроводниковых фазовых кубитах // Микроэлектроника (в печати).

Богданов Юрий Иванович. Заведующий лабораторией Физико-технологического института Российской академии наук (ФТИАН). Окончил Московский государственный университет им. М. В. Ломоносова в 1986 году. Доктор физико-математических наук. Автор более 120 научных трудов. Область научных интересов: квантовая информатика, физика квантовых компьютеров. E-mail: bogdanov@ftian.ru

Кокин Александр Александрович. Главный научный сотрудник Физико-технологического института Российской академии наук (ФТИАН). Окончил Уральский политехнический институт в 1954 году. Доктор физико-математических наук, профессор. Автор более 120 научных трудов. Область научных интересов: физика полупроводниковых приборов, физика квантовых компьютеров. E-mail: aakokin@mail.ru

Лукичев Владимир Федорович. Заместитель директора по научной работе Физико-технологического института Российской академии наук (ФТИАН). Окончил Московский государственный университет им. М.В. Ломоносова в 1978 году. Доктор физико-математических наук, профессор, член-корреспондент РАН. Автор более 70 научных трудов. Область научных интересов: физика сверхпроводников, микроэлектроника. E-mail: lukichev@ftian.ru

Орликовский Александр Александрович. Директор Физико-технологического института Российской академии наук (ФТИАН). Окончил Московский инженерно-физический институт в 1961 году. Доктор технических наук, профессор, академик РАН. Автор свыше 300 научных трудов, в том числе 2-х монографий. Область научных интересов: технологии кремниевой микро - и наноэлектроники, в том числе технологии МДП-транзисторов с длинами канала порядка 10 нм, включая квантовое описание характеристик таких транзисторов; технологии твердотельных квантовых компьютеров. E-mail: orlikovsky@ftian.ru

Семенихин Игорь Александрович. Старший научный сотрудник Физико-технологического института Российской академии наук (ФТИАН). Окончил Московский инженерно-физический институт в 2000 году. Кандидат физико-математических наук. Автор более 30 научных работ. Область научных интересов: высокопроизводительные вычисления, моделирование квантовых приборов и устройств. E-mail: isemenihin@mail.ru

Чернявский Андрей Юрьевич. Научный сотрудник Физико-технологического института Российской академии наук (ФТИАН). Окончил Московский государственный университет им. М. В. Ломоносова в 2005 году. Кандидат физико-математических наук. Автор 10 научных работ. Область научных интересов: квантовые вычисления, квантовая запутанность, искусственный интеллект, параллельные вычисления. E-mail: andrey.chernyavskiy@gmail.com