НАУЧНЫЙ ОТДЕЛ

ИНФОРМАТИКА

УДК 519.688

КВАНТОВЫЕ КОМПЬЮТЕРЫ И КВАНТОВЫЕ АЛГОРИТМЫ. Часть 1. КВАНТОВЫЕ КОМПЬЮТЕРЫ

В. М. Соловьев

Соловьев Владимир Михайлович, кандидат технических наук, доцент кафедры математической кибернетики и компьютерных наук, Саратовский государственный университет им. Н. Г. Чернышевского, начальник Поволжского регионального центра новых информационных технологий, svm@sgu.ru

В работе изложены принципы функционирования квантовых компьютеров. Приведены конкурентные преимущества квантовых вычислений. Представлены варианты построения идеального квантового компьютера. Проанализирован вычислительный процесс в квантовом компьютере с позиции сложности алгоритмов. Даны примеры реализации узлов квантового компьютера на основе коммуникационных квантовых схем. Описана работа сферы Блоха и визуализация состояния кубита. Рассмотрены основные проблемы, препятствующие созданию квантовых компьютеров.

Ключевые слова: квантовые вычисления, квантовый компьютер, квантовые алгоритмы, кубит, сфера Блоха, базисные состояния, квантовый гейт, квантовая суперпозиция, квантовая запутанность, декогеренция.

DOI: 10.18500/1816-9791-2015-15-4-462-477

ВВЕДЕНИЕ

В области обработки информации всё явственнее нарастает конкуренция между квантовыми и классическими законами природы. В настоящее время эта конкуренция обострилась, во-первых, вследствие невозможности решить некоторый класс вычислительных задач на классическом компьютере, из-за отсутствия эффективных алгоритмов[a]. В то же время квантовые вычисления (quantum computation, QC), используя парадоксы квантовой механики, позволяют решить эти задачи. Во-вторых, квантовая механика становится «локомотивом» развития современной технологической базы (в наноэлектронике, атомной промышленности, лазерных технологиях, а теперь и в информационных технологиях). Современные квантовые технологии могут поддерживать совершенно новые алгоритмы

[a]В теории сложности эффективным алгоритмом считается тот, который состоит из полиномиального числа операций, а время его выполнения полиноминально возрастает с размером решаемой задачи. Эффективные алгоритмы, относящиеся к классу полиномиальных, используют ограниченное количество вычислительных ресурсов. Неэффективные же алгоритмы требуют экспоненциально больших ресурсов, которые даже суперкомпьютеры не могут обеспечить.

вычислений (квантовые алгоритмы), основанные на принципах квантовой механики. По оценкам известного американского физика Джона Уилера примерно треть ВВП США основывается на достижениях квантовой механики [1, 2]. В-третьих, эксперименты с узлами квантовых компьютеров позволяют понять, как обрабатывается информация в природе. Один из лучших способов понять законы природы — это создать устройство, которое иллюстрировало бы этот закон [3, 4]. При этом для развития самой квантовой механики приходится решать специфические квантовые проблемы, которые за исключением простейших современные классические компьютеры могут решить за время, превышающее механический ресурс всей вселенной[2]. Для решения таких задач необходимы квантовые компьютеры. Однако, несмотря на впечатляющие успехи квантовой механики в изучении фундаментальных законов природы, полномасштабная практическая реализация ее в информационных технологиях тормозится сложностью организации и описания квантовых систем. Поэтому, поняв, как работают квантовые компьютеры, можно значительно расширить вычислительные возможности современных информационных технологий.

1. ПРИНЦИПЫ ПОСТРОЕНИЯ КВАНТОВОГО КОМПЬЮТЕРА

Информация, обрабатываемая современными классическими компьютерами, представляется в них двоичным кодом (битами). В любой момент времени бит может находиться в одном из двух состояний — логическом 0 или 1. Квантовые же компьютеры обрабатывают информацию на основе квантовых вычислений[3], используя кубиты (квантовые биты, q-биты, qubits), являющиеся квантовой суперпозицией состояний[4] 0 и 1, записанной следующим образом $p_0|0\rangle + p_1|1\rangle$[5]. В теории квантовых вычислений такая запись является описанием (списком) квантовых состояний. Она означает, что кубит состоит из списка квантовых состояний и может принимать значение 0 с вероятностью $|p_0|^2$ и значение 1 с вероятностью $|p_1|^2, (|p_0|^2 + |p_1|^2 = 1)$. Причем эти вероятности могут быть выражены комплексными числами. Квантовые компьютеры называют еще квантовыми машинами Тьюринга[6], имеющими теоретические сходства с недетерминированными[7] и вероятностными[8] компьютерами и отличающиеся от них характером изменения состояния Δ:

$$\Delta : Q \times \Gamma \to P(Q \times \Gamma \times \{L, R\} \times \mathbf{C}_{[0,1]}),$$

где: Q — конечное множество состояний, Γ — алфавит ленты, L, R — направление движения ленты (на ячейку влево — L, на ячейку вправо — R), $\mathbf{C}_{[0,1]} = \{p \in \mathbf{C} | p|^2 \leqslant 1\}$ — вероятностный элемент,

[2]Число элементарных частиц во вселенной приблизительно равно 10^{78}. При моделировании методом конечных элементов квантовых свойств атома железа, состоящего из ядра и 26-ти электронов, вращающихся в трехмерном пространстве необходимо решить уравнение Шредингера в конфигурационном пространстве размерностью 78 ($26 \times 3 = 78$). При очень грубой расчетной сетке $10 \times 10 \times 10$ понадобиться просчитать 10^{78} узлов, что сравнимо с механическим ресурсом вселенной.

[3]Квантовые вычисления — это обработка квантовыми системами информации, полученной в квантово-механических явлениях.

[4]Квантовая суперпозиция — это суперпозиция альтернативных (взаимоисключающих, наложенных) квантовых состояний, когда наблюдаемая величина не имеет конкретного значения, а ее измерения являются вероятностными. Суть принципа суперпозиций в том, что если сложить несколько разных решений в линейном уравнении, то их сумма тоже будет решением.

[5]Для описания квантовой системы используются специальные bracket (скобка) обозначения, алгебраический формализм введенный П. А. М. Дираком. Так бра-вектор $\langle y|$ обозначает вектор строку, а кет-вектор $|\rangle$ — вектор столбец, обычно обозначающий квантовые состояния.

[6]Квантовая машина Тьюринга (универсальный квантовый компьютер) — это абстрактная машина (теоретическая модель), используемая для реализации любого квантового алгоритма, выраженного формально. Она описывается кортежем: $M_N = (Q, \Sigma, \Gamma, \Delta, q_0, q_{accept}, q_{rejept})$, где Q — конечное множество состояний, Σ — входной алфавит, не содержащий пустой символ $\sqcup$ (пробел), Γ — алфавит ленты, содержащий пустой символ $\sqcup \in \Gamma$ и $\Sigma \subset \Gamma$, Δ — конечное множество допустимых состояний, q_0 — начальное состояние, q_{accept} — принимаемое состояние, q_{rejept} — отвергнутое состояние [14].

[7]Недетерминированная машина Тьюринга (nondeterministic Turing machine, NTM) — это теоретическая (мысленная) модель проведения экспериментов для изучения возможностей компьютера. В отличие от детерминированной машины Тьюринга NTM может иметь не одно, а целый набор действий для конкретной ситуации (неограниченный параллелизм).

[8]Вероятностная машина Тьюринга (probabilistic Turing machine) — это NTM, выбирающая случайным образом из любого состояния и значений на ленте один из нескольких возможных переходов. От NTM она отличается тем, что вместо недетерминированного перехода машина выбирает один из вариантов с некоторой вероятностью (параллелизм, ограниченный вероятностью).

учитывающий состояние k кубитов, где $\Sigma^k|p|^2 = 1$. Такие компьютеры реализуют квантовые алгоритмы, которые являются реалистическими моделями квантовых вычислений, использующими квантовые схемы.

2. КВАНТОВЫЕ ВЫЧИСЛЕНИЯ

Классические (не квантовые) алгоритмы подразумевают конечную последовательность инструкций, или шаг за шагом выполняемые процедуры. Аналогичным образом, квантовые алгоритмы также подразумевают пошаговое выполнение процедур, выполняемых на квантовом компьютере. Все классические алгоритмы выполнимы также и на квантовом компьютере, однако термин квантовый алгоритм, как правило, используется для алгоритмов, учитывающих особенности квантовых вычислений (квантовую суперпозицию, квантовую запутанность[9] и т. д.). Все алгоритмы, реализуемые на квантовом компьютере, могут быть реализованы и на классическом компьютере, а все проблемы, неразрешимые с помощью классических компьютеров остаются неразрешимыми и с помощью квантовых компьютеров. Однако интерес к квантовым компьютерам оправдан тем, что некоторые алгоритмы (например, переборного типа) могут быть выполнены на них гораздо быстрее, чем на классических компьютерах. Наибольший интерес, в этой связи, вызывает класс BPP-алгоритмов[10], расширенный в настоящее время и на квантовые алгоритмы $BPP \subseteq BQP$ (рис. 1).

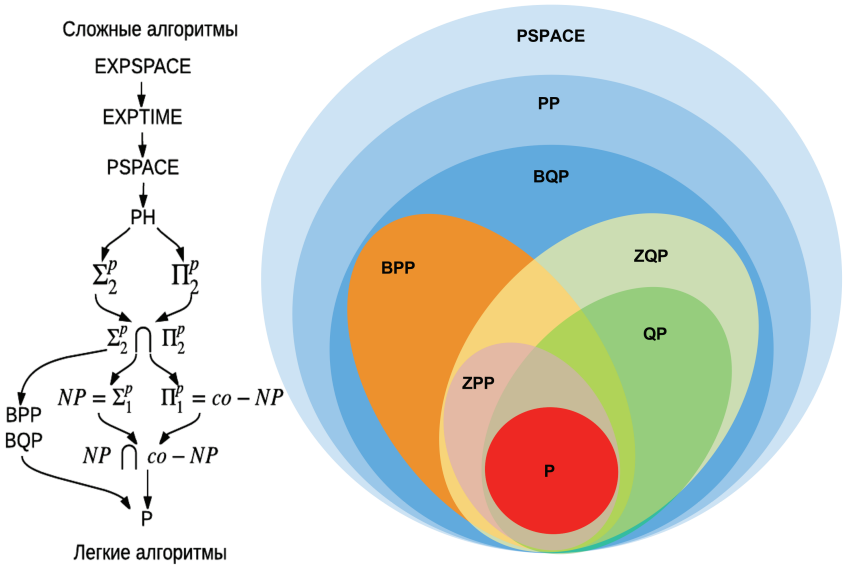

Рис. 1. Диаграмма включения классов сложности алгоритмов

[9]Квантовая запутанность (quantum entanglement) — это, с одной стороны, невозможность представления вектора состояния квантовой системы в виде прямого произведения векторов состояний, составляющих ее частей, а с другой — это взаимозависимость частей, когда они ведут себя как единое целое. При этом квантовое состояние каждой части не может быть описано независимо друг от друга. Запутанность следует из математического формализма квантовой механики. В соответствии с первым постулатом квантовой механики состояние квантовой системы полностью описывается её волновой функцией. Однако в некоторых случаях квантовым системам не удаётся приписать собственные волновые функции, а только одну на всех. Такое состояние и есть запутанность.

[10]В теории алгоритмов классом P (polynomial) называют «быстрые» алгоритмы решения задач, время работы которых полиноминально зависит от размера входных данных. Класс P как наиболее узкий класс сложности может принадлежать также алгоритмам класса BPP (bounded-error, probabilistic, polynomial), дающим «быстрые» (за полиномиальное время) решения с высокой вероятностью. Иерархия классов сложности алгоритмов: P — polynomial; BPP — bounded-error, probabilistic, polynomial; (BQP, QP, ZQP — класс квантовых алгоритмов); BQP — bounded-error quantum polynomial; QP — quantum polynomial-time; ZQP — zero-error quantum polynomial-time; P/Poly — non uniform polynomial-time; NP — nondeterministic polynomial; co-NP — complement of NP; PH — polynomial-time hierarchy; ZPP — zero-error probabilistic; PSPACE — polynomial-space; EXPTIME — exponential time (EXP); EXPSPACE — exponential space.

С. Смейл доказал, что с точки зрения сложности алгоритмов $BPP \not\supseteq NP$, это нечто похожее на $P \neq NP$ [5]. Однако условия BPP накладывают меньше ограничений, чем условия P, что расширяет круг практического использования BQP-алгоритмов (нахождение периода, факторизация, дискретный логарифм и т. д.). В таких алгоритмах допускается производить те или иные вычисления в зависимости от полученных результатов. Требуется, чтобы правильный ответ получался в «большинстве» случаев. Выполняя параллельно множество вычислений, можно получить правильный результат с очень большой вероятностью. Так, например, в квантовом алгоритме факторизации Шора[11] количество операций зависит от числа десятичных знаков и пропорционально квадрату разрядности числа [6], а в самом известном классическом алгоритме решета числового поля (general number field sieve) количество шагов растет экспоненциально и быстро выходит за границы возможностей современных компьютеров (рис. 2).

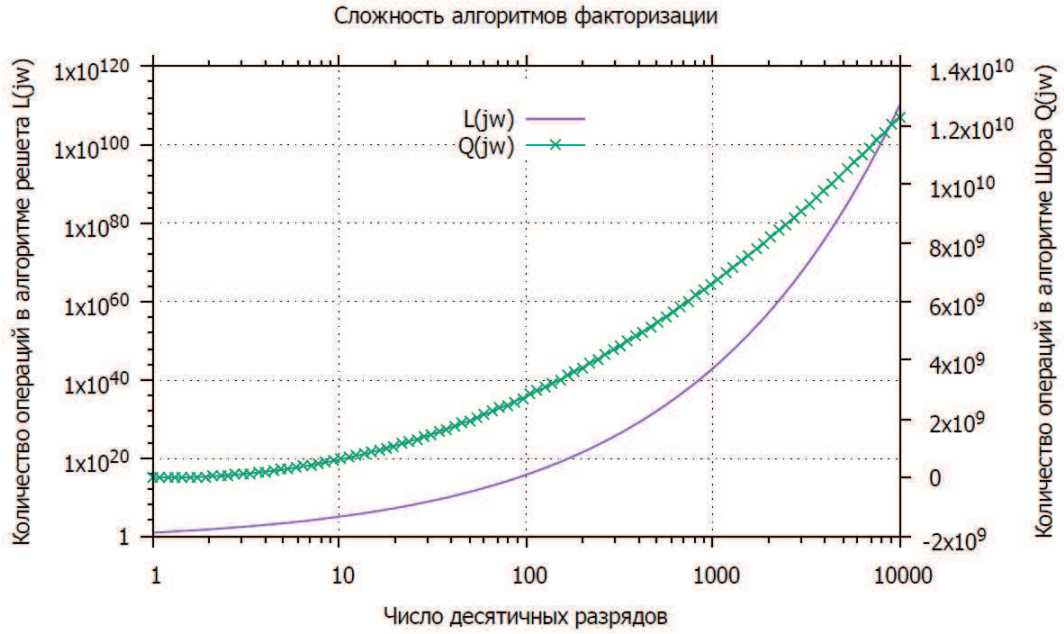

Рис. 2. Сравнение алгоритмов факторизации

Например, будущие суперкомпьютеры эксафлопсной[12] производительности позволят факторизовать 512-значное число приблизительно за 500 тысяч лет. Эту же факторизацию квантовый компьютер, выполняющий 10^6 операций в секунду, выполнит приблизительно за 2.5 минуты. Такие возможности квантовых компьютеров проявляются потому, что преобразования в квантовых вычислениях выполняются одновременно одной операцией. При этом квантовый компьютер, работающий с k кубитами, может выполнить параллельно 2^k операций. Квантовые алгоритмы, как правило, быстро выдают все возможные результаты и правильные, и неправильные, а выбранный результат только с некоторой вероятностью является правильным. Для повышения вероятности правильного результата в квантовых алгоритмах специально увеличивается кратность операций, которые подбираются таким образом, чтобы неправильные результаты с большой вероятностью взаимно уничтожались, и вероятность правильного результата увеличивалась.

Квантовые алгоритмы выполняются с использованием квантовых схем, которые служат моделями квантовых вычислений, включающих последовательности квантовых вентилей (квантовых логических

[11] Алгоритм Шора — это алгоритм разложения числа на простые множители, был предложен П. Шором в 1994 году. Практическая значимость алгоритма в том, что с его помощью можно компрометировать криптографические системы с открытым ключом.

[12] Производительность суперкомпьютера 1 Petaflops = 10^{15} операций с плавающей точкой в секунду была достигнута в 2008 году, в 2019 году планируется достигнуть производительности суперкомпьютеров в 1 Exaflops = 10^{18} операций с плавающей точкой в секунду.

элементов): это строительные элементы квантовых схем, являющиеся аналогами логических элементов обычных цифровых схем классического компьютера, реализующих основные булевы функции (логический базис). Таким образом, квантовые схемы выполняют физические преобразования на логическом базисе элементарных преобразований (квантовых гейтах, quantum gates). Так, например, на вход конкретной квантовой схемы может подаваться k кубитов, а результат её работы, однозначно задаваемый значениями на базисных состояниях[13], будет носить вероятностный характер и представляться матрицей $2^k \times 2^k$. Как известно, логические элементы классического компьютера не обратимы, то есть по значению на выходе, например, логического элемента «И» нельзя однозначно установить входные значения. Для обратимых логических элементов (теоретически они возможны и в классическом компьютере), какими и являются квантовые логические элементы, однозначно можно определить входные значения любой длины. На основе таких элементов создаются реверсивные квантовые схемы, реализующие обратимые функции в пространстве k кубитов. На основе реверсивных схем могут быть созданы обратимые машины — узлы квантовых компьютеров. Создание реальных квантовых компьютеров (не имитаторов и не моделей)[14] усложняет декогеренция[15], проявляющаяся при физическом соединении таких узлов.

Схема идеального[16] квантового компьютера в самом общем виде представлена на рис. 3.

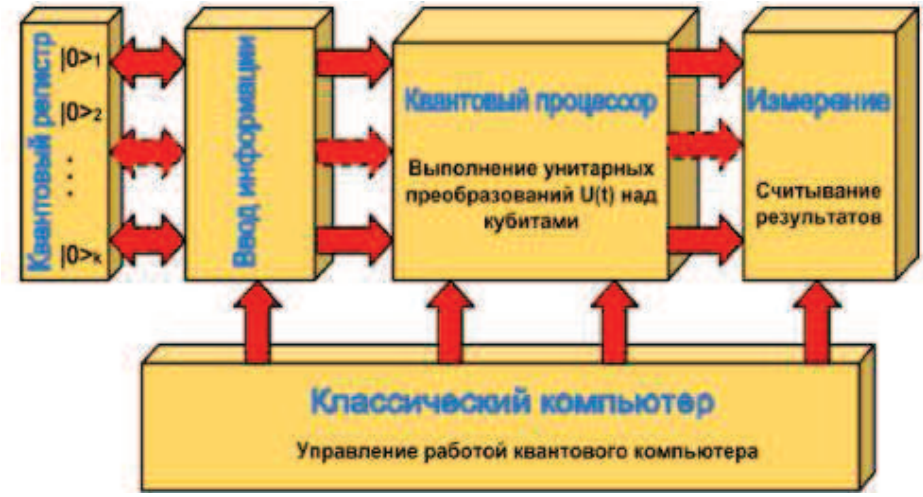

Рис. 3. Схема идеального квантового компьютера

Она может быть реализована k-кубитными регистрами[17], представляющими собой квантовый процессор (аналог классического процессора), управляемый сигналами с обычного компьютера. Кроме того, в схему идеального квантового компьютера входит система измерения состояния кубитов, считывающая результаты и замыкающая контур управления квантовым компьютером. Квантовый процессор, кроме основного, может включать дополнительные регистры, играющие вспомогательную роль. Состояния идеального квантового компьютера всегда когерентны и описываются разложением в 2^k

[13]Базисные состояния — это набор ортогональных друг другу кубитов. Если ограничиваться двумя квантовыми состояниями $|0\rangle$ и $|1\rangle$, то базис будет состоять из двух кубитов.

[14]В настоящее время нет однозначного мнения ученых, что первый коммерческий квантовый компьютер Orion канадской фирмы D-Wave, использующий адиабатические квантовые вычисления, является реально квантовым (http://old.computerra.ru/offline/2007/677/310169/).

[15]Декогеренция — спонтанный распад сложных квантовых состояний, делающий невозможным длинные квантовые вычисления с использованием большого числа кубитов. Декогеренция носит фундаментальный характер и ее нигде не удается избежать, как своеобразную «силу трения» в квантовых системах, сводящуюся к проблеме коллапса волновой функции при измерении, которая до сих пор не решена.

[16]Идеальный квантовый компьютер, во-первых, не взаимодействует с окружающей средой, создающей помехи его работе и нарушающей когерентность его квантовых состояний (декогеренция); во-вторых, он управляется внешними импульсными сигналами (лазерными, СВЧ и т.д.), не имеющими «контакта» с квантовой средой.

[17]Регистр из k кубитов может в суперпозиции хранить и параллельно выполнять 2^k вычислений. Например, классический трехразрядный регистр в каждый момент времени может хранить одно трехразрядное число, а регистр из трех кубитов одновременно может хранить восемь чисел и выполнять восемь вычислений.

базисе $|i_1 \dots i_k\rangle$, $i_1, ..., i_k = \{0, 1\}$:

$$|\psi\rangle = \sum_{i_1,\dots,i_k} p_{i_1,\dots,i_k} |i_1, ..., i_k\rangle, \tag{1}$$

где: $|\psi\rangle$ — суперпозиция состояний в 2^k-мерном векторном пространстве (волновая функция ψ в векторном виде), $|i_1 \dots i_k\rangle$ — 2^k базисных ортов этого пространства, $p_{i_1,\dots,i_k}$ — проекция вектора $|\psi\rangle$ на направления ортов $|i_1 \dots i_k\rangle$. Процесс вычисления на квантовом компьютере — это преобразование (1) одного вектора состояния $|\psi_i\rangle$ в другое $|\psi_{i+1}\rangle$ путем умножения вектора $|\psi_i\rangle$ на унитарную матрицу U размерности $2^k \times 2^k$:

$$|\psi_{i+1}\rangle = U(2^k \times 2^k)|\psi_i\rangle. \tag{2}$$

Обычно работа квантового компьютера, как и старт обычного компьютера, начинается с состояния инициализации. При этом состояние его кубитов $|0_1 \dots 0_k\rangle$ достигается охлаждением до сверхнизких температур или путем управления этим состоянием. Информация во входном квантовом регистре с помощью импульсных воздействий преобразуется в когерентную суперпозицию базисных ортогональных состояний $|\psi_i\rangle$. Далее эту информацию обрабатывает квантовый процессор в соответствии с алгоритмом решения задачи. Этот алгоритм реализует матрица преобразования $U(2^k \times 2^k)$, а информация по решаемой задаче содержится в векторе $|\psi_{i+1}\rangle$ и получить ее можно путем измерения состояния кубитов, то есть определением вероятности нахождения кубита в квантовых состояниях, определяемых базисом. Таким образом, выше приведенное выражение (2) для $|\psi_{i+1}\rangle$ может служить моделью вычислений на квантовом компьютере. Для этого нужно создать в квантовой среде кубиты, заставить её вычислять[18] (обрабатывать информацию с использованием кубитов) в соответствии с преобразованиями $U|\psi_i\rangle$, предварительно инициализировав, и далее измерить и выдать результат. Такая модель вычислений, реализованная в идеальном квантовом компьютере (рис. 3), является вероятностной аналого-цифровой. Аналоговая часть («аналоговый компьютер») — это собственно квантовая среда (квантовый процессор, выполняющий унитарные преобразования) и измеритель[19] состояния кубитов. Цифровая часть — это классический управляющий компьютер, на котором пользователь получает результат вычислений. Такого сочетания аналоговых и цифровых частей с вероятностным представлением решения не имели ни классические аналоговые компьютеры прошлого, ни современные классические цифровые компьютеры. Эта модель квантовых вычислений выполняет преобразование начального вектора состояний кубитов

$$|\psi_i\rangle = \sum_x p_x^i |x\rangle \tag{3}$$

в конечный вектор

$$|\psi_{i+1}\rangle = \sum_x p_x^{i+1} |x\rangle, \tag{4}$$

через непрерывный ряд вероятностных состояний. Динамика преобразований (3), (4) — это передача во времени изменений аналоговых величин (амплитуд) $p_x(t)$ в интервале $0 \leqslant |p_x| \leqslant 1$. За это отвечает цифровая часть квантового компьютера, реализующая управление.

Управление вычислительным процессом в k-кубитном квантовом компьютере связано с преобразованием 2^k компонент векторов $|\psi_i\rangle \to |\psi_{i+1}\rangle$ в соответствии с матрицей преобразований $U(2^k \times 2^k)$. Даже на современном классическом суперкомпьютере трудно реализовать эти преобразования из-за очень большого количества операций, выполняемых при разложении матрицы $U(2^k \times 2^k)$ в упорядоченное множество произведений матриц [7]:

$$U(2^k \times 2^k) = \prod_{i,j} U_i(2 \times 2) \otimes U_j(2^2 \times 2^2). \tag{5}$$

[18] Известный специалист в области квантовых вычислений Сет Ллойд (Seth Lloyd) считает, что для того чтобы заставить квантовую среду вычислять (обрабатывать информацию), ее надо очаровать, воздействуя определенным образом [3].

[19] Измерения в квантовом компьютере — это передача информации от одного квантового регистра другому, связанному с классическим управляющим компьютером.

В квантовом компьютере разложение (5) одновременно выполняется отдельным кубитом за счет квантового параллелизма, основанном на вычислениях суперпозиций базовых состояний. Это позволяет ему при интерпретации команд одновременно принимать несколько значений, находясь в состоянии квантового запутывания. Как данные в кубите могут содержать множество значений сразу, так и квантовый компьютер может выполнять множество интерпретированных команд одновременно. Однако квантовый параллелизм отличается от классических параллельных вычислений компьютера. Как правило, классический высокопроизводительный компьютер состоит из нескольких процессоров или вычислительных ядер. При этом, как правило, один процессор или ядро выполняют одну вычислительную задачу. В случае квантового параллелизма один квантовый процессор выполняет сразу несколько задач. В выражении (5) каждая матрица $U_i(2 \times 2)$ описывает операцию на отдельном кубите, а матрица $U_j(2^2 \times 2^2)$ преобразует векторы состояний пар кубитов. Таким образом, число сомножителей в разложении (5) определяется числом однокубитовых и двухкубитовых операций, необходимых для реализации квантовых алгоритмов. Поэтому BQP алгоритмы относят к эффективным, так как общее число операций полиноминально от числа используемых кубитов в квантовом компьютере.

3. УЗЛЫ КВАНТОВОГО КОМПЬЮТЕРА

Однокубитовые операции описывают состояние отдельного кубита, а двухкубитовые операции в квантовом алгоритме описывают взаимосвязь одного кубита (контролируемого) с другим (контролирующим), могут быть и многокубитовые операции, составляющие квантовый регистр. Связь кубитов требует физического взаимодействия между ними. Эту связь реализуют квантовые гейты, переводящие кубиты из одного состояния в другое, то есть работающие с суперпозицией. Наиболее известными гейтами являются: гейт NOT, гейт Адамара (Hadamard gate, H), X-, Y-, Z-гейт Паули (Pauli-X, -Y, -Z gate), гейт фазового сдвига (phase shift gate, R), гейт обмена (swap gate, SWAP), гейт контролируемого НЕ (Controlled NOT, CNOT), гейт Тоффоли (Toffoli gate, Controlled Controlled NOT, CCNOT), гейт Фредкина (Fredkin gate) и т. д. Как и в классическом логическом базисе, действия гейта на кубиты описываются таблицей истинности, отражающей изменения базисных состояний. При этом матрица гейта умножается на столбец значений кубитов, участвующих в действии гейта. На основе гейтов могут быть созданы квантовые логические элементы и узлы квантового компьютера. Как и в классическом компьютере, эти элементы могут быть представлены в графической форме, где кубиты изображаются горизонтальными линиями, а действие гейта на кубит (или несколько кубитов) соответствующей квантовой схемой. Таким образом, квантовый алгоритм создается на основе коммуникационной квантовой схемы, где слева находится начальное состояние, а справа — конечное. Эта схема и каузальная (причинно-следственная) структура определяют квантовые вычисления. Работа квантового узла заключается в реализации квантового алгоритма путем прохождения кубитов через гейты.

В соответствии с квантовым алгоритмом узел реализует квантовые вычисления. Например, квантовый гейт NOT (аналог классического инвертора НЕ) выполняет следующее однокубитовое преобразование состояния: $NOT : |\psi_i\rangle \to NOT : (p_0|0\rangle + p_1|1\rangle) \to NOT : |\psi_{i+1}\rangle \to NOT : (p_0|1\rangle + p_1|0\rangle)$. Преобразование однокубитовых состояний выполняют унитарные матрицы размерности 2×2. На их основе можно построить неограниченное число гейтов, среди которых наиболее известными матрицами являются: матрица Адамара (H), матрица фазового сдвига (R), матрицы Паули, реализующие соответствующие X-, Y-, Z-гейты и т. д. (рис. 4):

$$H \equiv \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}, \qquad R_\varphi \equiv \begin{pmatrix}1 & 0\\ 0 & e^{i\varphi}\end{pmatrix}, \qquad X \equiv \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}, \qquad Y \equiv \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}, \qquad Z \equiv \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}.$$

Самым распространенным гейтом, выполняющим двухкубитовые операции, является CNOT (контролируемое НЕ), изображенный на рис. 5.

Наименование	Обозначение	Состояние выхода при входе (a $\|0\rangle$ + b $\|1\rangle$)	Унитарная матрица
Элемент Паули X	X	b $\|0\rangle$ + a $\|1\rangle$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Элемент Паули Y	Y	-i{b $\|0\rangle$ - a $\|1\rangle$ }	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
Элемент Паули Z	Z	a $\|0\rangle$ - b $\|1\rangle$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Элемент Адамара	H	$\frac{a+b}{\sqrt{2}}\|0\rangle + \frac{a+b}{\sqrt{2}}\|1\rangle$	$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
Фазовый элемент	S	a $\|0\rangle$ + ib $\|1\rangle$	$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
Элемент $\pi/8$	T	a $\|0\rangle$ + $e^{i\pi/8}$ b $\|1\rangle$	$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/8} \end{pmatrix}$
Элемент тождественного преобразования	I	a $\|0\rangle$ + b $\|1\rangle$	$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
Элемент измерения		Проекция на $\|0\rangle$ и $\|1\rangle$	

Рис. 4. Однокубитовые гейты

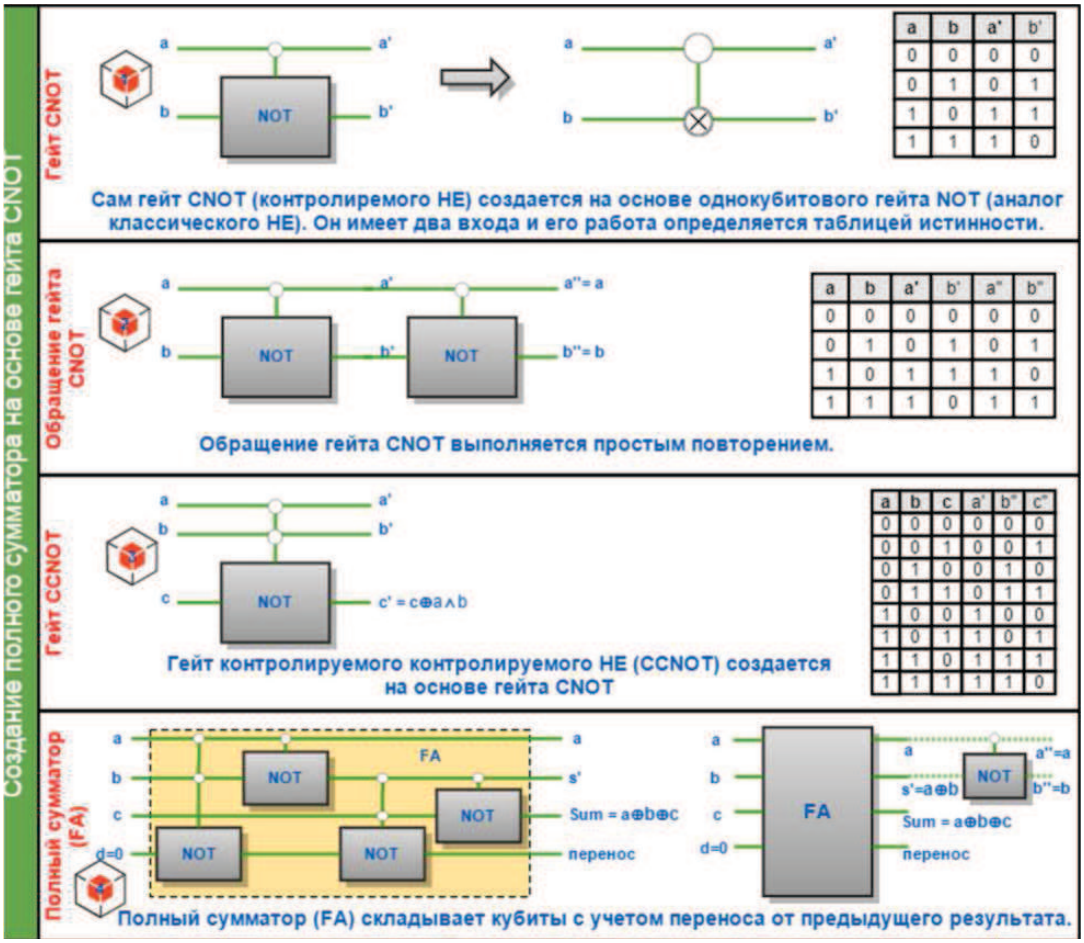

Рис. 5. Квантовый узел на основе гейта, контролируемого НЕ

Это аналог классического логического элемента исключающее ИЛИ (логическое сложение, XOR), являющегося основой построения большинства узлов классического компьютера (например, сумматора).

Двухкубитовая операция CNOT, выполняемая квантовой системой, включает процесс эволюции двух кубитов под воздействием гамильтониана их взаимодействия[20]. В процессе эволюции один кубит управляет другим, используя энергию взаимодействия. При этом второй кубит инвертируется, если первый находится в состоянии $|1\rangle$, в противном случае, он остается без изменений. При этом начальное состояние кубитов $|\psi_i^1\rangle = (p_0^1|0\rangle + p_1^1|1\rangle), |\psi_i^2\rangle = (p_0^2|0\rangle + p_1^2|1\rangle)$, эволюционирует в следующее состояние:

$$|\psi_{i+1}^{12}\rangle = p_0^1p_0^2|00\rangle + p_0^1p_1^2|01\rangle + p_1^1p_0^2|11 + p_1^1p_1^2|10\rangle \equiv \begin{pmatrix} p_0^1p_0^2 \\ p_0^1p_1^2 \\ p_1^1p_0^2 \\ p_1^1p_1^2 \end{pmatrix}. \tag{6}$$

Соединяя в коммуникационную квантовую схему гейты CNOT, можно получить сложные узлы квантового компьютера (например, сумматор рис. 5). Пространство состояний такой квантовой системы представляет собой тензорное произведение пространств состояний, входящих в нее систем. При этом если одна система находится в состоянии $|\psi_1\rangle$, а другая в состоянии $|\psi_2\rangle$, то квантовая система будет находиться в состоянии $|\psi_1\rangle \otimes |\psi_2\rangle$.

4. ОПРЕДЕЛЕНИЕ СОСТОЯНИЯ КУБИТОВ

Как следует из коммуникационной квантовой схемы, кубит может находиться в одном из возможных состояний, определяемых гейтом. Кроме того, кубит — это минимальное количество информации, хранящейся в квантовом компьютере. Носителем такой информации является квантовая среда (аналоговая часть квантового компьютера), базисные состояния которой кубит представляет линейной суперпозицией. Визуализацию состояния кубита можно представить с помощью сферы Блоха (рис. 6).

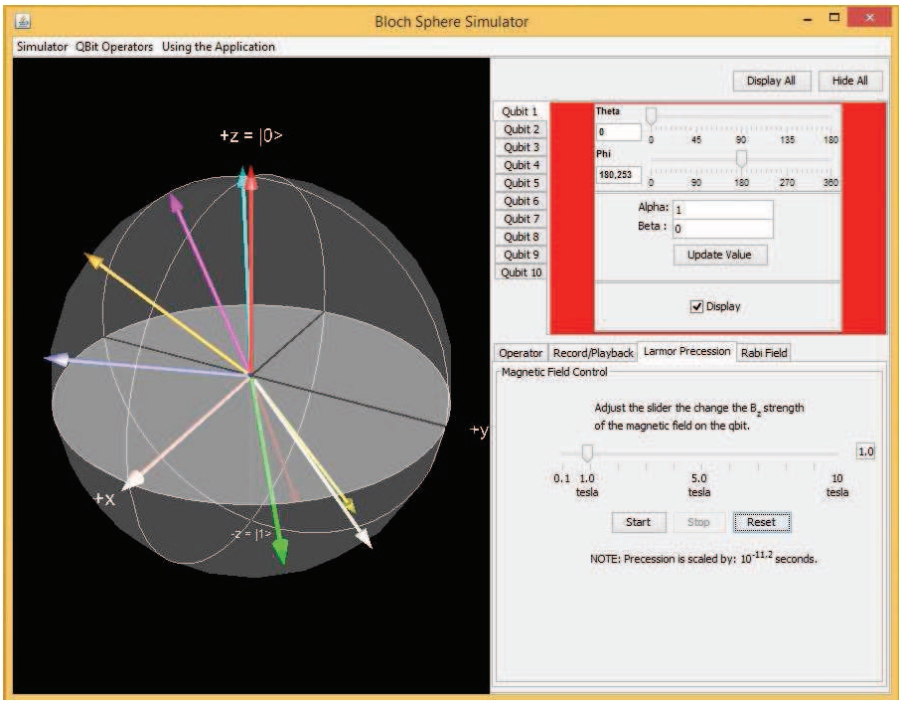

Рис. 6. Сфера Блоха

[20]Гамильтониан H — это оператор, определяющий изменение во времени состояния квантовой среды. Он изменяет волновую функцию (вид уравнения Шредингера $ih(d|\psi\rangle/dt) = H|\psi\rangle$) и одновременно является оператором полной энергии системы.

Классический бит на поверхности сферы Блоха может находиться только в точках $|0\rangle$ «логический 0» и $|1\rangle$ «логическая 1», а остальная часть сферы является для него недоступной. Состояние же кубита может быть отображено с помощью любой точки на поверхности сферы Блоха, описывающей «чистые» состояния квантовой среды, которые всегда когерентны. Смешанные же квантовые состояния являются некогерентными и могут быть отображены на шаре Блоха. Таким образом можно представить состояние любой квантовой системы, характеризуемой ортонормированными волновыми функциями. Для реализации аналоговой части квантового компьютера нужна квантовая система, векторы состояний которой $|\psi\rangle$ образуют гильбертово[21] двумерное векторное пространство. Компоненты этих двумерных векторов имеют следующий вид: $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}, |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}, |\psi\rangle = p_0\begin{pmatrix}1\\0\end{pmatrix} + p_1\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}p_0\\p_1\end{pmatrix}$. Здесь $|0\rangle$ и $|1\rangle$ состояния, служащие ортами в двумерном гильбертовом пространстве кубита. Проекции состояний $|\psi\rangle$ на орты равны амплитудам p_0 и p_1 в суперпозиции: $\langle 0|\psi\rangle = p_0, \langle 1|\psi\rangle = p_1$. В общем виде амплитуды в p_0 и p_1 — это комплексные числа вида $p = |p|e^{i\varphi}$, тогда выражение (3) при переходе кубита из состояния $|0\rangle$ в состояние $|1\rangle$ будет иметь следующий вид:

$$|\psi\rangle = e^{i\varphi_{p_0}}\left[|p_0| + |p_1|\, e^{i(\varphi_{p_1} - \varphi_{p_0})}\right]. \tag{7}$$

Общий фазовый множитель в выражении (7) не влияет на состояние кубита, так как фаза в начальном состоянии $|0\rangle$ может иметь произвольное значение. Отсюда следует, что вектор $|\psi\rangle$ определяется параметрами p_0, p_1 и разностью фаз $(\varphi_{p_1} - \varphi_{p_0})$. Значения p_0, p_1 получаются многократным вычислением в базисе $|0\rangle$ и $|1\rangle$ как вероятностный результат. Разность фаз $(\varphi_{p_1} - \varphi_{p_0})$ вычисляется на основе матрицы унитарных преобразований U выражения (5). При этом вращения вектора состояния кубита на сфере Блоха рассматривается как элементарные однокубитовые вычислительные операции. Обычно параметры вращения (направление оси, угол поворота и т. д.) определяются параметрами физических полей (напряженностью, частотой, поляризацией, длительностью воздействия и т. д.), воздействующих на квантовую среду и управляющих динамикой квантовой системы. Значит, всегда можно подобрать некоторое воздействие на квантовую систему, которое переведет ее из одного произвольного состояния, заданного точкой на сфере Блоха, в другое. Для определения состояния квантовой системы, как видно на рис. 3, его нужно измерить.

Квантовые измерения описываются набором операторов в пространстве состояний системы $\{\langle\psi|M_m^\dagger, M_m|\psi\rangle\}$ [7]. Если состояние квантовой системы до измерения было $|\psi\rangle$, то вероятность получения результата измерения m будет $p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$, а состояние квантовой системы после измерения будет описываться следующим выражением: $\dfrac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$. Операторы измерения должны удовлетворять требованию полноты [7] $\sum(M_m^\dagger M_m) = 1$, следовательно, $\sum p(m) = \sum\langle\psi|M_m^\dagger M_m|\psi\rangle = 1$.

Измерение состояния кубитов как неотъемлемая функция квантового компьютера является стрессовым воздействием на квантовую систему в виде квантового скачка. Это объясняется тем, что до измерения квантовая система находилась в некотором состоянии квантовой статистической неопределённости (суперпозиции), а после измерения эта неопределенность снимается. Измерение можно представить аналогом двухкубитовой операции, описываемой выражением (6). Только здесь в регистре из двух кубитов второй кубит участвует не в операции CNOT, а «измеряет» состояние первого. Это измерение основано на явлении запутанности посредством нелокальной[22] квантовой корреляции, не имеющем аналога в классической физике и являющегося контринтуитивным [11]. В классической физике по полному описанию системы всегда можно описать части этой системы. В квантовой же

[21] Гильбертово пространство — обобщение евклидова пространства, допускающее бесконечную размерность. Это линейное векторное пространство над полем вещественных или комплексных чисел, в котором для любых двух элементов определено скалярное произведение.

[22] Квантовая нелокальность — это непроявленные состояния квантовой системы [9]. В квантовой механике известны состояния полной запутанности (состояния Бэлла), являющиеся уникальным нелокальным свойством частиц. В этом случае поведение частиц синхронно, но не связано с их локальной связью (нелокально).

системе, находящейся в запутанном состоянии, этого сделать нельзя, так как информации, дающей полное описание квантовой системы, недостаточно для описания частей, из которых она состоит. Таким образом, для измерений, для квантовой телепортации[23], для квантовых вычислений необходимо реализовать запутанность квантовой системы, когда за счет высокого уровня корреляции, обусловленной взаимодействием, одна часть её будет «знать», что были выполнены измерения на другой части. Запутанные состояния — это основа парадигмы квантовой информатики и их реализация является одной из самых сложных задач при создании квантовых компьютеров. Эта задача выполнима пока на очень короткое время[24]. В настоящее время квантовая запутанность — это уже привычная физическая величина (не математическая абстракция), изменяющаяся от нуля до единицы. В зависимости от этой величины квантовая система может состоять из отделимых локальных частей, которые либо слабо связаны друг с другом (мера запутанности равна нулю), либо квантовая система составляет единое неделимое целое (мера запутанности равна единице), находясь в нелокальном состоянии, когда нет никаких классических «проявленных» объектов. Мера запутанности зависит от интенсивности взаимодействий в квантовой системе [8]. Следовательно, управляя взаимодействием и манипулируя мерой квантовой запутанности, можно управлять квантовыми вычислениями, измерять и выводить результаты. По мере взаимодействия с окружением, когда мера запутанности между подсистемами квантового компьютера постепенно уменьшается, в нем «проявляются» результаты в виде локальных объектов. Этот процесс очень упрощенно можно пояснить как проявление изображения на фотобумаге, помещенной в проявитель (взаимодействие с окружением). Запутанность только намного сложнее, так как нет заранее экспонированной «картинки», она «размазана» по фотобумаге (аналогично голографическому изображению) и поэтому невидима. Все элементы находятся в суперпозиции и у них нет «видимых» локальных форм, но по мере взаимодействия с окружением суперпозиция постепенно разрушается и проявляется то или иное классическое «видимое» состояние. Этот процесс декогеренции «растаскивает» в разные стороны то, что было единым целым (невидимым), придает определенные формы, которые становятся видимыми с привычной классической точки зрения. Обратный процесс управления мерой запутанности (рекогеренция) может её увеличивать (дистиллировать), что аналогично превращению снимка, обработанного проявителем, в чистый лист фотобумаги, то есть возврат к исходному суперпозиционному состоянию. В этом случае квантовая система полностью лишается самостоятельности и не может изменяться независимо от своих подсистем, так как даже небольшие деградационные изменения одной подсистемы приводят к изменению остальных, что может дестабилизировать квантовую систему. Таким образом мера квантовой запутанности может контролироваться и целенаправленно изменяться квантовым компьютером в процессе обработки информации, которая количественно выражается через энтропию фон Неймана[25]. Это позволяет описывать квантовый компьютер в терминах информатики и рассматривать изменение меры запутанности как процессы обмена информацией в нём. В этом случае уменьшение меры запутанности соответствует передаче информации из квантовой системы в окружение при взаимодействии с ним. Запутанная квантовая система в терминах квантовой информации — это единое информационное поле, вычисления в котором одновременно содержат все возможные правильные и неправильные реализации. Задача квантовых вычислений, кроме всего, — свести к минимуму неправильные реализации.

Для вычислений в квантовом компьютере необходимо как минимум два k-кубитных регистра. В один регистр будет заноситься аргумент, а в другой результат вычислений. Процедура вычислений рассматривается как работа того или иного гейта, преобразующего аргумент в выходные значения: $f : \{0,1\}^{k_1} \to \{0,1\}^{k_2}$. Например, рассмотренный выше гейт CNOT, реализующий функцию $f : (x, y) \to (x, x \otimes y)$, выполняет вычислительные процедуры над четырьмя аргументами, как видно из выражения (6). Процедура квантовых вычислений функции f (аналог суммирования по модулю 2

[23]Квантовая телепортация — это передача квантового состояния на расстояние при помощи квантовой пары и классического канала связи. При этом состояние квантовой системы в точке отправления при измерении разрушается, а в точке приема воссоздается вновь. Квантовая телепортация не передает энергию или вещество, а передает только информацию.

[24]В настоящее время кубиты функционируют только при очень низкой температуре ($-233.4\,C$) и рекордное время составляе пока 39 минут. За это время с ними можно выполнить до 20 млн операций [15].

[25]Энтропия фон Неймана — это основная физическая характеристика энергоинформационного процесса, показывающая изменение информации при изменении энергии.

в классическом компьютере) можно представить следующим образом. Вначале в один из k-кубитных регистров заносятся все значения аргумента x, которые затем переводятся в суперпозиционное состояние в другом регистре: $f(x) \to |0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle + \ldots + |2^k - 1\rangle|f(2^k - 1)\rangle$. Такое запутанное состояние двух регистров, где записана вся таблица истинности, описывает операцию сложения по модулю 2. В классическом компьютере для двухразрядного аргумента вычисление функции $f(x)$ пришлось бы проводить 4 раза или использовать четыре рабочих ресурса. В квантовом же компьютере, используя суперпозиционные состояния, вычисления позволяют сразу получить результат. Но воспользоваться этими преимуществами квантовых вычислений далеко не просто из-за особенностей измерений состояний кубитов. Суперпозиционное состояние, возникающее в результате вычисления, из-за запутанности описывает, в большей степени, общее поведение квантовой системы (например, функции f). Поэтому квантовые вычисления более эффективны в задачах, исследующих общие свойства систем.

Основываясь на выражениях (6) и (7), запутанное состояние квантовой системы при измерении может быть представлено следующим образом[26]:

$$|\psi\rangle_{12} = |0\rangle_1|1\rangle_2 + e^{i(\varphi_1 - \varphi_2)}|1\rangle_1|0\rangle_2. \tag{8}$$

Разность фаз $(\varphi_1 - \varphi_2)$ определяется внутренними свойствами квантовой системы. Особенностью запутанного состояния (8) является то, что ни один из двух кубитов не несет в себе определенного значения, а о квантовой системе известно лишь то, что один из двух кубитов является предметом измерения и результат этого измерения носит случайный характер. Это же подтверждает и свойство квантовой нелокальности, когда кубиты находятся на произвольном расстоянии во время измерения [9]. Способы получения и наблюдения квантовой запутанности вытекают из выражения (8). Во-первых, это может быть квантовая система, которая физически реализует свойство нелокальности. Например, частица с целым спиновым числом, распавшаяся на две частицы с противоположными спинами и с сохранением внутреннего углового момента. В этом случае выражение (8) может быть представлено в следующем виде: $|\psi\rangle_{12} = (|\uparrow\rangle_1|\downarrow\rangle_2 + |\downarrow\rangle_1|\uparrow\rangle_2)$, где $|\uparrow\rangle_1$ — частица 1 со спином вверх, $|\downarrow\rangle_2$ — частица 2 со спином вниз. Тогда измерение сводится к определению антипараллельных спинов частиц. Во-вторых, это может быть квантовая система, состояние которой определяется в виде отдельных компонент выражения (8). Например, спонтанное параметрическое преобразование состояния фотонов $|H\rangle_1|V\rangle_2$ и $|V\rangle_1|H\rangle_2$, генерирующее пары запутанных фотонов [10]. В этом случае запутанные фотоны 1 и 2 имеют разные плоскости поляризации (H — горизонтальную и V — вертикальную). При прохождении таких поляризованных фотонов через преобразующую систему (нелинейный кристалл) из-за различия скоростей света в плоскостях H и V временные интервалы соответствующих фотонов будут отличаться. Таким образом, слагаемые выражения (8) можно разделить, а тем самым выделить и определить запутанное состояние квантовой системы, используя методику квантового ластика (quantum eraser)[27]. Каждый из рассмотренных методов может быть использован для получения и наблюдения запутанных состояний. В общем виде это означает следующее: полностью запутанные или частично запутанные состояния в той или иной форме могут быть приведены к описанным выше.

При измерении суперпозиция разрушается, так как не существует суперпозиции измерений [9]. Следовательно, при измерении нет суперпозиции состояний, а есть мгновенное описание изменения квантового состояния (волновой функции). Это нелокальный процесс мгновенного измерения приводит к коллапсу волновой функции (редукции фон Неймана[28]). Измерение тесно связано с мысленным

[26] Строго говоря, это лишь часть всех возможных состояний запутанности, их частный случай.

[27] Квантовый ластик (quantum eraser) — эксперимент с интерферометром, позволяющий изучить механизм квантовой запутанности. В ходе физического эксперимента каждый из запутанных фотонов направляется в разные устройства анализа, что позволяет манипулировать информацией о каждом фотоне.

[28] Редукция фон Неймана — это математический прием описания редукции волновой функции, а не физический процесс, так как распространяется быстрее скорости света. Однако некоторые исследователи считают редукцию фон Неймана физическим процессом, для которого необходимо разработать новую теорию.

экспериментом кота Шредингера[29], поясняющим взаимное влияние квантовой системы и измерения. Это влияние сводит измерение (выбор) к взаимодействию между квантовой системой и её окружением, что приводит к их запутыванию. Коллапс волновой функции при измерении тесно связан с декогеренцией, так как «запутанное» измерение неминуемо сопровождается этим объективным физическим процессом [11]. Вследствие этого к внутренней запутанности квантовой системы, которой компьютер может управлять и которая ему подвластна, добавляется запутанность с окружением (распад единства квантовой системы, возникновение ошибок, неточностей, мешающих факторов и т. д.). Здесь можно говорить о «свертывании» исходного пространства состояний квантовой системы в пространство состояний меньшего размера, когда исходный вектор состояния делится на части — на свою собственную (внутреннюю) и внешние. Декогеренция и связанные с ней ошибки — это одна из главных проблем на пути создания квантового компьютера. В упрощенном виде эти ошибки можно представить двумя уровнями. На первом уровне ошибки, которые присутствуют в каждом компьютере, в том числе и классическом (ошибки вычислений, работы аппаратных платформ, операторов и т. д.). Эти ошибки современные компьютеры умеют эффективно исправлять. В квантовых вычислениях в настоящее время тоже стали успешно с ними справляться[30]. Второй уровень ошибок в квантовых компьютерах гораздо сложнее, так как кубиты крайне нестабильны и подвержены декогеренции, что нарушает связи внутри квантовых систем. Как упоминалось ранее, квантовый процессор на время вычислений нужно максимально изолировать от окружающей среды и охладить. Но из-за декогеренции в результате внутренних процессов этого тоже недостаточно, чтобы избавиться полностью от ошибок второго уровня. Их можно сделать только достаточно редкими, чтобы квантовый компьютер смог эффективно работать. По оценкам некоторых исследователей, это потребует до 99% вычислительной мощности квантового компьютера, но и оставшегося 1% хватит для решения многих задач [12]. Работа квантового компьютера предполагает измерение состояния k-кубитных регистров, например, для получения информации о решении задачи по завершению вычислений. В теоретическом плане больших сложностей в процедуре такого измерения состояний нет. Однако физическая реализация измерения состояний квантовой системы, представляемой кубитами, сопряжены с решением весьма сложных технологических проблем. Они связаны с преодолением трудностей измерения состояния отдельных частиц и коррекции ошибок. По существу, для каждого квантового компьютера нужна разработка своего физического метода измерения и коррекции ошибок, которая является одной из самых трудных с точки зрения физической реализации. Одним из путей решения этой задачи является увеличение времени декогеренции t_{dc}, которое должно быть значительно больше времени выполнения вычислительных операций t_{op}. Кроме того, время декогеренции уменьшается с ростом числа кубитов и для k-кубитного регистра оно будет существенно меньше времени декогеренции одного кубита. Отношение $n = t_{dc}/t_{op}$ показывает, сколько вычислительных операций можно выполнить пока квантовый компьютер сохраняет когерентное состояние, при котором кубиты связаны друг с другом, а не с окружающей средой за счет декогеренции. Для некоторых физических реализаций это отношение приведено в табл. 1 [7].

Таблица 1

Время декогеренции и выполнения вычислительной операции

Измерения при физической реализации	Время декогеренции (t_{dc}, с)	Время выполнения операции (t_{op}, с)	Количество операций (n)
Ядерный спин	$10^{-2} - 10^{8}$	$10^{-3} - 10^{-6}$	$10^{-5} - 10^{14}$
Электронный спин	10^{-3}	10^{-7}	10^{4}
Ионная ловушка	10^{-1}	10^{-14}	10^{13}
Оптические решетки	10^{-5}	10^{-14}	10^{9}
Квантовые точки	10^{-6}	10^{-9}	10^{3}

[29]Мысленный эксперимент с котом Шредингера описывает положение кота в ящике. В ходе эксперимента фотон падает на полупрозрачное зеркало, и его волновая функция регистрируется датчиком. Поскольку зеркало полупрозрачное, датчик может обнаружить фотон, а может не обнаружить. Если датчик обнаруживает фотон, то срабатывает пистолет, убивающий кота. Если датчик не обнаруживает фотон, то кот остается жив.

[30]Google совместно с Калифорнийским университетом стабилизировали цепочку из девяти кубитов и устранили в ней ошибки [16].

Физическая реализация квантовой системы (аналоговая часть квантового компьютера) в настоящее время возможна при условии эффективного наблюдения двух уровней ее состояния (например, статического и возбужденного). В табл. 2 приведены квантовые явления, обладающие такими состояниями и реализованные в той или иной мере.

Таблица 2

Физическая реализация квантовых систем

Квантовая среда	Квантово-механические явления	Кодирование информации	$\|1\rangle$	$\|1\rangle$
Фотоны	Поляризация света	Плоскостью поляризации	Горизонтальная	Вертикальная
	Фоковское состояние[1]	Фоковским состоянием	Вакуумное состояние (отсутствие квантов)	Точно определенное количество квантов
	Временное кодирование[2]	Временем распространения	Короткое время	Длинное время
Когерентное состояние света	Сжатое состояние[3]	Квадратурой компонентой поля	Амплитудно-сжатое состояние	Фазово-сжатое состояние
Электроны	Спин электрона	Спином электрона	Спин вверх	Спин вниз
	Подсчет электронов	Зарядом	Нет электронов	Точно определенное количество электронов
Атомные ядра	Ядерный магнитный резонанс	Спином ядра	Спин вверх	Спин вниз
Ионы в ловушках	Квантовый электромагнитный резонанс	Спином внешнего электрона в ионе	Спин вверх	Спин вниз
Оптические ловушки (решетки)	Конденсат Бозе – Эйнштейна[4]	Спином атома	Спин вверх	Спин вниз
Контакты Джозефсона[5]	Заряд в сверхпроводнике	Зарядом	Разряженная сверхпроводящая область	Заряженная сверхпроводящая область
	Ток в сверхпроводнике	Направлением тока	Ток по часовой стрелке	Ток против часовой стрелки
	Фаза в сверхпроводнике	Фазой тока в сверхпроводнике	Фаза в статическом состоянии	Фаза в возбужденном состоянии
Квантовые точки[6]	Локализация электронов	Зарядом	Разряженная квантовая точка	Заряженная квантовая точка
	Спин квантовой точки	Спином квантовой точки	Спин вниз	Спин вверх

Примечание. [1]фоковское состояние — это квантовомеханическое состояние с точно определенным количеством элементарных частиц; [2]временное кодирование основано на различие времени прохождении одиночных фотонов через один из двух путей (например, в интерферометре Маха – Цендера); [3]сжатое состояние — это особый класс состояний квантовой системы, когда дисперсия флуктуаций одной из сопряженных компонент меньше другой (например, квадратуры амплитуды и фазы); [4]конденсат Бозе – Эйнштейна — это сильно охлажденное состояние бозонов (близко к абсолютному нулю), когда квантовые эффекты начинают проявляться на макроуровне (например, газ из атомов рубидия); [5]контакты Джозефсона — это соединение двух сверхпроводников, разделенных тонким слоем диэлектрика; [6]квантовые точки — это очень малые нанокристаллические полупроводниковые структуры, в которых начинают проявляться квантовые свойства.

Из табл. 2 видно, что наиболее исследованными такими квантовыми двухуровневыми элементами являются спины (электронные или ядерные), которые описываются двухкомпонентными спиновыми волновыми функциями (спинорами). Они представляют собой векторы состояния в двухмерном гильбертовом пространстве $|0\rangle$ или $|1\rangle$. По аналогии двухуровневые элементы не спиновой природы также могут описываться псевдоспинорами и псевдоспинами. Квантовый двухуровневый элемент находится не только в одном из двух чистых базисных состояний, но и в обоих состояниях одновременно, соответственно выражению (1). Двухуровневый квантовый элемент и является кубитом, включающим более общее понятие, чем классический бит, так как допускает кодирование большего количества информации и может образовывать запутанные состояния.

ЗАКЛЮЧЕНИЕ

В настоящее время нет универсального промышленного (production) квантового компьютера, а имеются только экспериментальные образцы, реализующие отдельные подходы к его созданию. Они, как правило, существуют в лабораторных исследовательских (research) вариантах, но в то же время позволяют реализовывать элементы квантовых вычислений. При создании аппаратных платформ (hardware) квантовых компьютеров пока остаются нерешенными следующие проблемы:

– выбор физической квантовой среды, которая обеспечит возможность получения достаточного для восокопроизводительных вычислений числа, хорошо определенных и управляемых кубитов, содержащих обрабатываемую информацию в когерентной суперпозиции базисных ортогональных состояний $|\psi_i\rangle$;

– определение принципов селективного управления кубитами (проведение логических операций) и покубитового измерения их состояния на выходе;

– создание механизма взаимодействия между кубитами, основывающегося на квантовой запутанности, поддержании реверсивности вычислений, квантовом параллелизме и интерференции;

– уменьшение уровня квантовых ошибок и увеличение времени декогеренции.

Продолжение следует.

Библиографический список

1. *Богданов Ю. И., Кокин А. А., Лукичёв В. Ф., Орликовский А. А., Семенихин И. А., Черняв-ский А. Ю.* Квантовая механика и развитие информационных технологий // Информационные технологии и вычислительные системы. 2012. № 1. С. 17–31.
2. Closing in on quantum computing. URL : http:// www.wired.com/2014/10/quantum-computing-close (accessed 23, June, 2015).
3. *Ллойд С.* Программируя вселенную. Квантовый компьютер и будущее науки. М. : Альпина нонфикшн, 2014. 256 с.
4. *Валиев К. А.* Квантовые компьютеры и квантовые вычисления // УФН. 2005. Т. 175, № 1. С. 3–39.
5. *Смейл С.* О проблемах вычислительной сложности. Математическое просвещение. М. : МЦНТО, 2000. Сер. 3, вып. 4. С. 115–119.
6. *Shor P. W.* Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. 1996. arXiv: quant-ph/9508027. 28 p.
7. *Nielsen M., Chuang I.* Quantum Computation and Quantum Information. 10th Anniversary Edition. Cambridge Univ. Press, 2010. 698 p.
8. *Rieffe E. G., Polak W. H.* Quantum computing: a gentle introduction. Scientific and Engineering Computation. MIT Press, 2011. 389 p.
9. *Белинский А. В.* Квантовая нелокальность и отсутствие априорных значений измеряемых величин в экспериментах с фотонами // УФН. 2003. Т. 173, № 8. С. 905–909.
10. *Bouwmeester D., Ekert F., Zeilinger A.* The Physics of Quantum Information. Springer, 2000. 315 p.
11. *Менский М. Б.* Квантовые измерения и декогеренция. Модели и феноменология : пер. с англ. М. : Физматлит, 2001. 232 с.
12. *Прескилл Дж.* Квантовая информация и квантовые вычисления : в 2 т. Т. 2. М. : Рег. дин.; Ижевск : Ин-т компьют. исслед., 2011. 312 с.
13. Algebraic and Number Theoretic Algorithms. URL: http://math.nist.gov/ quantum/zoo/ (accessed 23, June, 2015).
14. *Venegas-Andraca S. E.* Quantum Walks for Computer Scientists. Synthesis Lectures on Quantum Computing. Morgan Claypool, 2008. 133 p.
15. *Kastrenakes J.* Researchers smash through quantum computer storage record. URL: http:// www.theverge.com/2013/11/14/5104668/qubits-stored-for-39-minutes-quantum-computer-new-record (accessed 23, June, 2015).
16. *Kelly J.* State preservation by repetitive error detection in a superconducting quantum circuit // Nature. Macmillan Publ. Ltd., 2015. Vol. 519. P. 66–69.

Quantum Computers and Quantum Algorithms. Part 1. Quantum Computers

V. M. Solovyev

Solovyev Vladimir Mihajlovich, Saratov State University, 83, Astrakhanskaya st., 410012, Saratov, Russia, svm@sgu.ru

The paper presents the principles of operation of quantum computers. Competitive advantages of quantum computing are shown and some variants of a construction of an ideal quantum computer proposed. We analyze also the computational process in a quantum computer from the point of view of the complexity of algorithms. Implementation of nodes of a quantum computer is exemplified based on quantum communication schemes. The operation of Bloch sphere and visualization of the state of the qubit are described. Major obstacles to the creation of quantum computers are considered.

Key words: quantum computing, quantum computers, quantum algorithms, qubit, Bloch sphere, basic state, quantum gates, quantum superposition, quantum entanglement, decoherence.

References

1. Bogdanov U. I., Kokin A. A., Lukichev V. F., Orlikovskij A. A., Semenihin I. A., Chernavskij A. U. Quantum mechanics and the development of information technology. *Information technologies and computer systems*, 2012, no. 1, pp. 17–31 (in Russian).
2. Closing in on quantum computing. Available at: http://www.wired.com/2014/10/quantum-computing-close (accessed 23, June, 2015).
3. Lloyd S. Programming universe. A quantum computer science and the future. Moscow, Alpina nonfiction, 2014, 256 p.
4. Valiev K. A. Quantum computers and quantum computing. *Successes of physical sciences*, 2005, vol. 175, no. 1, pp. 3–39.
5. Smale S. On the problems of computational complexity. Mathematical education. Moscow, MCNTO, 2000, Ser. 3, iss. 4, pp. 115–119.
6. Shor P. W. *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*. 1996. arXiv: quant-ph/9508027. 28 p.
7. Nielsen M., Chuang I. *Quantum Computation and Quantum Information*. 10th Anniversary Edition. Cambridge Univ. Press, 2010, 698 p.
8. Rieffe E. G., Polak W. H. *Quantum computing: a gentle introduction. Scientific and Engineering Computation*. MIT Press, 2011, 389 p.
9. Belinskij A. V. Quantum nonlocality and the absence of a priori values for measurable quantities in experiments with photons. *Successes of physical sciences*, 2003, vol. 173, no. 8, pp. 905–909.
10. Bouwmeester D., Ekert F., Zeilinger A. *The Physics of Quantum Information*. Springer, 2000, 315 p.
11. Menskij M. B. *Quantum measurement and decoherence. Models and phenomenology*: Trans. from English. Moscow, Fizmatlit, 2001, 232 p.
12. Preskill J. *Quantum information and quantum computation. Vol. 2.* Moscow, Izhevsk, SIC «Regular and Chaotic Dynamics», Institute of Computer Science, 2011, 312 p.
13. Algebraic and Number Theoretic Algorithms. Available at: http://math.nist.gov/ quantum/zoo/ (accessed 23, June, 2015).
14. Venegas-Andraca S. E. *Quantum Walks for Computer Scientists. Synthesis Lectures on Quantum Computing*. Morgan Claypool, 2008, 133 p.
15. Kastrenakes Jacob. Researchers smash through quantum computer storage record. Available at: http://www.theverge.com/2013/11/14/5104668/qubits-stored-for-39 - minutes - quantum - computer-new-record (accessed 23, June, 2015).
16. Kelly J. State preservation by repetitive error detection in a superconducting quantum circuit. *Nature*, Macmillan Publ. Ltd., 2015, vol. 519, pp. 66–69.