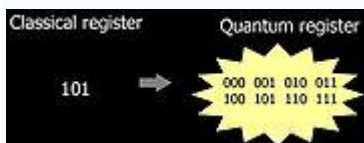


Квантовый компьютер

Материал из Википедии — свободной энциклопедии



3 кубита квантового регистра против 3 битов обычного

Квантовый компьютер — гипотетическое^[1] **вычислительное устройство**, которое путем выполнения **квантовых алгоритмов** существенно использует при работе **квантовомеханические** эффекты, такие как **квантовый параллелизм** и **квантовая запутанность**.

Содержание понятия «квантовый параллелизм» может быть раскрыто так: «Данные в процессе вычислений представляют собой квантовую информацию, которая по окончании процесса преобразуется в классическую путём измерения конечного состояния квантового регистра. Выигрыш в квантовых алгоритмах достигается за счет того, что при применении одной квантовой операции большое число коэффициентов суперпозиции квантовых состояний, которые в виртуальной форме содержат классическую информацию, преобразуется одновременно»^[1].

Под квантовой запутанностью, которую называют также **«квантовой суперпозицией»**, обычно понимается следующее: "Вообразите атом, который мог бы подвергнуться радиоактивному распаду в определенный промежуток времени. Или не мог бы. Мы можем ожидать, что у этого атома есть только два возможных состояния: «распад» и «не распад», /.../ но в квантовой механике у атома может быть некое объединенное состояние — «распада — не распада», то есть ни то, ни другое, а как бы между. Вот это состояние и называется «суперпозицией»^[2].

Базовые характеристики квантовых компьютеров в теории позволяют им преодолеть некоторые ограничения, возникающие при работе классических **компьютеров**.

Содержание

- [1 Теория](#)
 - [1.1 Кубиты](#)
 - [1.2 Вычисление](#)
 - [1.3 Алгоритмы](#)
 - [1.4 Квантовая телепортация](#)
- [2 Применение квантовых компьютеров](#)
 - [2.1 Специфика применения](#)
 - [2.2 Приложения к криптографии](#)
- [3 Реализации](#)
 - [3.1 Первый квантовый компьютер](#)
 - [3.2 D-Wave](#)
- [4 См. также](#)
- [5 Примечания](#)
- [6 Литература](#)

- [7 Ссылки](#)

Теория

Кубиты

Основная статья: [кубит](#)

Идея квантовых вычислений, впервые высказанная [Ю. И. Маниным](#)^[3] и [Р. Фейнманом](#)^[4] состоит в том, что квантовая система из L двухуровневых квантовых элементов (квантовых битов, [кубитов](#)) имеет 2^L линейно независимых состояний, а значит, вследствие принципа квантовой суперпозиции, пространством состояний такого квантового регистра является 2^L -мерное [гильбертово пространство](#). Операция в квантовых вычислениях соответствует повороту вектора состояния регистра в этом пространстве. Таким образом, квантовое вычислительное устройство размером L кубит может выполнять параллельно 2^L операций.

Предположим, что имеется один кубит. В таком случае после измерения, в так называемой классической форме, результат будет 0 или 1. В действительности кубит — квантовый объект и поэтому, вследствие принципа неопределённости, в результате измерения может быть и 0, и 1 с определенной вероятностью. Если кубит равен 0 (или 1) со стопроцентной вероятностью, его состояние обозначается с помощью символа $|0\rangle$ (или $|1\rangle$) — в [обозначениях Дирака](#). $|0\rangle$ и $|1\rangle$ — это базовые состояния. В общем случае квантовое состояние кубита находится "между" базовыми и записывается, в виде $a|0\rangle + b|1\rangle$, где $|a|^2$ и $|b|^2$ — вероятности измерить 0 или 1 соответственно; $a, b \in \mathbb{C}$; $|a|^2 + |b|^2 = 1$. Более того, сразу после измерения кубит переходит в базовое квантовое состояние, аналогичное классическому результату.

Пример:

Имеется кубит в квантовом состоянии $\frac{4}{5}|0\rangle - \frac{3}{5}|1\rangle$

В этом случае, вероятность получить при измерении

0 составляет $(4/5)^2 = 16/25 = 64\%$,

1 $(-3/5)^2 = 9/25 = 36\%$.

В данном случае, при измерении мы получили 0 с 64 % вероятностью.

Тогда кубит перескакивает в новое квантовое состояние $1*|0\rangle + 0*|1\rangle = |0\rangle$, то есть, при следующем измерении этого кубита мы получим 0 со стопроцентной вероятностью. Это обусловлено тем, что дираковский вектор состояния не зависит от времени, то есть раскладывается в сумму векторов базисных состояний с независимыми от времени коэффициентами.

Приведем для объяснения два примера из квантовой механики: 1) фотон находится в состоянии суперпозиции двух поляризаций; измерение раз и навсегда коллапсирует состояние фотона в таковое с определенной поляризацией; 2) радиоактивный атом имеет определенный период полураспада; измерение может выявить то, что он еще не распался, но это не значит, что он никогда не распадется.

Перейдем к системе из двух кубитов. Измерение каждого из них может дать 0 или 1. Поэтому у системы 4 классических состояния: 00, 01, 10 и 11. Аналогичные им базовые квантовые состояния: $|00\rangle$, $|01\rangle$, $|10\rangle$ и $|11\rangle$. И наконец, общее квантовое состояние системы имеет вид $a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$. Теперь $|a|^2$ — вероятность измерить 00 и т. д. Отметим, что $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$ как полная вероятность.

В общем случае, системы из L кубитов у неё 2^L классических состояний (0000...(L -нулей), ...00001(L -цифр), ... , 1111...(L -единиц)), каждое из которых может быть измерено с вероятностями 0—100 %.

Таким образом, одна операция над группой кубитов затрагивает все значения, которые она может принимать, в отличие от классического бита. Это и обеспечивает беспрецедентный параллелизм вычислений.

Вычисление

Упрощённая схема вычисления на квантовом компьютере выглядит так: берется система кубитов, на которой записывается начальное состояние. Затем состояние системы или её подсистем изменяется посредством базовых квантовых операций. В конце измеряется значение, и это результат работы компьютера.

Оказывается, что для построения любого вычисления достаточно двух базовых операций. Квантовая система дает результат, только с некоторой вероятностью являющийся правильным. Но за счет небольшого увеличения операций в алгоритме можно сколь угодно приблизить вероятность получения правильного результата к единице.

С помощью базовых квантовых операций можно симулировать работу обычных логических элементов, из которых сделаны обычные компьютеры. Поэтому любую задачу, которая решена сейчас, квантовый компьютер решит, и почти за такое же время. Следовательно, новая схема вычислений будет не слабее нынешней.

Чем же квантовый компьютер лучше классического? Большая часть современных ЭВМ работают по такой же схеме: n бит памяти хранят состояние и каждый такт времени изменяются процессором. В квантовом случае система из n кубитов находится в состоянии, являющимся суперпозицией всех базовых состояний, поэтому изменение системы касается *всех* 2^n базовых состояний одновременно. Теоретически новая схема может работать намного (в экспоненциальное число раз) быстрее классической. Практически (квантовый) [алгоритм Гровера](#) поиска в базе данных показывает квадратичный прирост мощности против классических алгоритмов. Пока в природе их не существует.

Алгоритмы

Главная статья [Квантовый алгоритм](#)

- [Алгоритм Гровера](#) позволяет найти решение уравнения $f(x) = 1$, $0 \leq x < N$ за время $O(\sqrt{N})$.
- [Алгоритм Шора](#) позволяет разложить натуральное число n на простые множители за [полиномиальное](#) от $\log(n)$ время.

- [Алгоритм Дойча — Джоза](#) позволяет «за одно вычисление» определить, является ли функция двоичной переменной $f(n)$ постоянной ($f_1(n) = 0, f_2(n) = 1$ независимо от n) или «сбалансированной» ($f_3(0) = 0, f_3(1) = 1; f_4(0) = 1, f_4(1) = 0$).

Было показано, что не для всякого алгоритма возможно «квантовое ускорение».

Квантовая телепортация

Основная статья: [Квантовая телепортация](#)

Алгоритм телепортации реализует точный перенос состояния одного кубита (или системы) на другой. В простейшей схеме используются 4 кубита: источник, приёмник и два вспомогательных. Отметим, что в результате работы алгоритма первоначальное состояние источника разрушится — это пример действия общего **принципа невозможности клонирования** — невозможно создать точную копию квантового состояния, не разрушив оригинал. На самом деле, довольно легко создать одинаковые состояния на кубитах. К примеру, измерив 3 кубита, мы переведем каждый из них в базовые состояния (0 или 1) и хотя бы на двух из них они совпадут. Не получится скопировать *произвольное* состояние, и телепортация — замена этой операции.

Телепортация позволяет передавать квантовое состояние системы с помощью обычных классических каналов связи. Таким образом, можно, в частности, получить связанное состояние системы, состоящей из подсистем, удаленных на большое расстояние.

Применение квантовых компьютеров

Специфика применения

Может показаться, что квантовый компьютер — это разновидность аналоговой вычислительной машины. Но это не так: по своей сути это цифровое устройство, но с аналоговой природой.

Основные проблемы, связанные с созданием и применением квантовых компьютеров:

- необходимо обеспечить высокую точность измерений;
- внешние воздействия могут разрушить квантовую систему или внести в неё искажения.

Приложения к криптографии

Благодаря огромной скорости разложения на простые множители, квантовый компьютер позволит расшифровывать сообщения, зашифрованные при помощи популярного асимметричного криптографического алгоритма [RSA](#). До сих пор этот алгоритм считается сравнительно надёжным, так как эффективный способ разложения чисел на простые множители для классического компьютера в настоящее время неизвестен. Для того, например, чтобы получить доступ к кредитной карте, нужно разложить на два простых множителя число длиной в сотни цифр. Даже для самых быстрых современных компьютеров выполнение этой задачи заняло бы больше времени, чем возраст Вселенной, в сотни раз. При помощи алгоритма Шора эта задача делается вполне осуществимой, если квантовый компьютер будет построен.

Применение идей квантовой механики уже открыли новую эпоху в области криптографии, так как методы [квантовой криптографии](#) открывают новые возможности в области передачи сообщений^[5]. Прототипы систем подобного рода находятся на стадии разработки^[6].

Реализации

Первый квантовый компьютер

В ноябре 2009 года физикам из Национального института стандартов и технологий в США впервые удалось собрать программируемый квантовый компьютер, состоящий из двух кубит^[7].

D-Wave

Канадская компания D-Wave заявила в феврале 2007 года о создании образца квантового компьютера, состоящего из 16 кубит (устройство получило название Orion). Однако информация об этом устройстве не отвечала строгим требованиям точного научного сообщения; новость не получила научного признания. Более того, дальнейшие планы компании (создать уже в ближайшем будущем 1024-кубитный компьютер) вызвали скепсис у членов экспертного сообщества^[8].

В ноябре 2007 года та же компания D-Wave продемонстрировала работу образца 28-кубитного компьютера онлайн на конференции, посвященной суперкомпьютерам^[9]. Данная демонстрация также вызвала определенного рода скепсис.

В декабре 2008 года компания организовала проект [распределенных вычислений AQUA@home](#) (Adiabatic QUantum Algorithms)^[10], в котором тестируются алгоритмы, оптимизирующие вычисления на адиабатических сверхпроводящих квантовых компьютерах D-Wave.

Программные симуляторы квантовых компьютеров, см. [Квантовое программирование](#).

См. также

- [ДНК-компьютер](#)
- [Молекулярный компьютер](#)
- [Недетерминированная машина Тьюринга](#)
- [Квантовый алгоритм](#)
- [Квантовая информация](#)
- [Квантовая память](#)

Примечания

1. ↑ ^{1 2} [Холево, А. КВАНТОВАЯ ИНФОРМАТИКА: ПРОШЛОЕ, НАСТОЯЩЕЕ, БУДУЩЕЕ // В МИРЕ НАУКИ. — июль 2008. — № 7](#)
2. ↑ [Quantum entanglement](#)
3. ↑ <http://www.computerra.ru/offline/2001/379/6780/>
4. ↑ Килин С. Я. Квантовая информация. 5.2.1
5. ↑ [Валиев, К. А. Квантовая информатика: компьютеры, связь и криптография // Вестник российской академии наук. — 2000. — Том 70. — № 8. — С. 688—695](#)

6. [↑ Созданы прототипы квантовых компьютеров](#)
7. [↑ First universal programmable quantum computer unveiled](#)
8. [↑ D-Wave восхитила журналистов и возмутила ученых](#)
9. [↑ Сайт компании D-Wave](#)
10. [↑ Сайт AQUA@home](#)

Литература

- *Kilin S.Ya.* Quanta and information / Progress in optics. — 2001. — Vol. 42. — P. 1-90.
- *Килин С. Я.* Квантовая информация / Успехи Физических Наук. — 1999. — Т. 169. — С. 507—527. [1]
- [Квантовые вычисления за и против. Под ред. Садовниченко В. А.](#)
- [Квантовый компьютер и квантовые вычисления. Под ред. Садовниченко В. А.](#)
- [Валиев К. А., Кокин А. А. Квантовые компьютеры: надежды и реальность. Москва, Ижевск: Регулярная и хаотическая динамика, 2004. 320 с. ISBN 5-93972-024-2](#)

Ссылки

- [Квантовый ликбез](#)
- [Квантовый компьютер и его полупроводниковая элементарная база](#)
- [Первый квантовый компьютер](#)
- [Кафедра квантовой информатики факультета ВМК МГУ](#)
- [Лаборатория физики квантовых компьютеров Физикотехнологического института РАН](#)
- [Кутаев, А., Шень, А., Вялый, М. Классические и квантовые вычисления](#)
- [QWiki](#)^(англ.) и [Quantiki](#)^(англ.) — Wiki-ресурсы по квантовой информатике
- [Язык программирования QCL для квантовых компьютеров](#)^(англ.)
- Курс «[Современные задачи теоретической информатики](#)» (лекции по квантовым вычислениям: введение, суперплотное кодирование, квантовая телепортация, алгоритмы Саймона и Шора)
- [Gilles Brassard, Isaac Chuang, Seth Lloyd and Christopher Monroe. Quantum computing Beyond Bits: The Future of Quantum Information Processing Andrew M. Steane, Eleanor G. Rieffel](#)
- [InFuture.ru: Будущее квантовых компьютеров — в троичных вычислениях](#)
- [Валиев К. А. «Квантовые компьютеры и квантовые вычисления» УФН 175 3 \(2005\)](#)
- [Страничка проекта AQUA@home на сайте команды «Russia»](#)

Источник

«http://ru.wikipedia.org/wiki/%D0%9A%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D1%8B%D0%B9_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80»

Категории: [Компьютер](#) | [Квантовый компьютер](#)

Скрытые категории: [Википедия:Стилистически некорректные статьи](#) | [Статьи со ссылками на Викисклад](#)