Квантовые компьютеры.

Немного истории.

- Хью Эверетт III (англ. Hugh Everett III , 11 ноября 1930 — 19 июля 1982)

В 1957 году предложил оригинальное объяснение квантовым эффектам. Он заявил, что подобные эффекты вызывают теневые фотоны, то есть фотоны, которые принадлежат другим вселенным.

-

- Ричард Филлипс Фейнман (Фа́йнман) (англ. Richard Phillips Feynman; 11 мая 1918 — 15 февраля 1988)

В 1982 году предложил использовать многомировую интерпретацию Эверетта для создания вычислительных машин.

-

- Питер Шор(англ. Peter Shor)

В 1994 году предложил эффективный квантовый алгоритм для сложных вычислений, которые могут использоваться, к примеру, для взламывания систем шифрования информации. Алгоритм Шора позволяет за короткий промежуток времени решать на квантовом компьютере задачи, с которыми не могут справиться современные компьютеры.

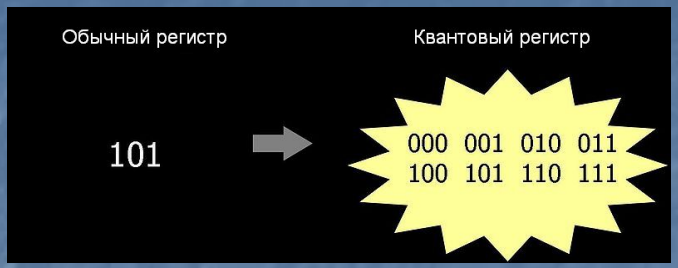
-

- Лов Гровер (англ. Lov Kumar Grover)

В 1996 году предложил квантовый алгоритм быстрого поиска в неупорядоченной базе данных.

Кубит.

Кубит (q-бит, кьюбит; от quantum bit) — квантовый разряд или наименьший элемент для хранения информации в квантовом компьютере .



Как и бит, кубит допускает два собственных состояния, обозначаемых |0) и |1), но при этом может находиться и в их суперпозиции, т.е. в состоянии A*|0)+B*|1), где A и B любые комплексные числа, удовлетворяющие условию $|A|^2+|B|^2=1$.
При любом измерении состояния кубита он случайно переходит в одно из своих собственных состояний. Вероятности перехода в эти состояния равны, соответственно $|A|^2$ и $|B|^2$, то есть косвенно, по наблюдениям за множеством кубитов, всё-таки можно судить об исходном состоянии.
Кубиты могут быть «запутаны» друг с другом, то есть, на них может быть наложена ненаблюдаемая связь, выражающаяся в том, что при всяком измерении над одним из нескольких кубитов, остальные меняются согласованно с ним. То есть, совокупность запутанных между собой кубитов может интерпретироваться как заполненный квантовый регистр. Как и отдельный кубит, квантовый регистр гораздо более информативен. Он может находиться не только во всевозможных комбинациях составляющих его битов, но и реализовывать всевозможные тонкие зависимости между ними.

Квантовые вычисления.

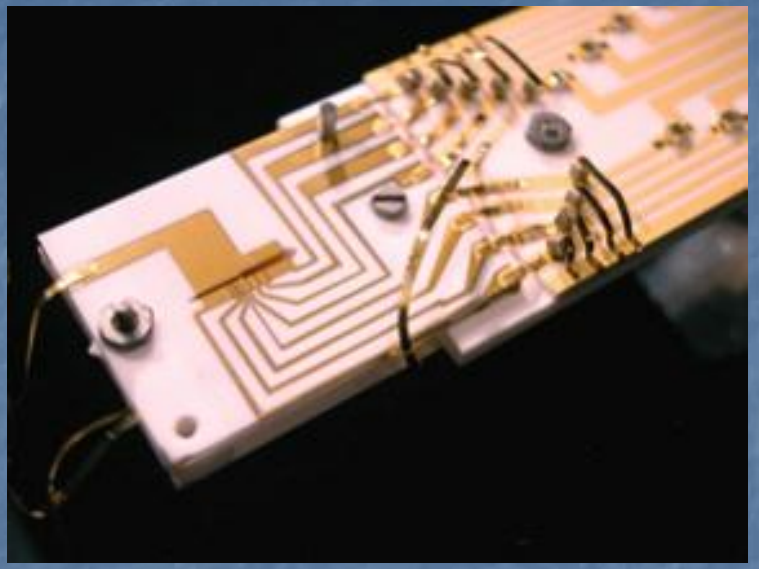
Идея квантовых вычислений состоит в том, что квантовая система из L двухуровневых квантовых элементов (квантовых битов, кубитов) имеет 2^L линейно независимых состояний, а значит, вследствие принципа квантовой суперпозиции, пространством состояний такого квантового регистра является 2^L-мерное гильбертово 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.

Квантовые компьютеры.

- на основе ионных ловушек;
- ядерного магнитного резонанса;
- оптики;
- твёрдого тела;

КК на основе ионных ловушек.

В квантовых компьютерах с ионной ловушкой линейная последовательность ионов, представляющих кубиты, ограничена электрическим полем. Для того чтобы произвести однокубитовые квантовые операции, лазеры направляются на отдельные ионы. Двухкубитовые операции осуществляются при использовании лазера, направленного на отдельный кубит для создания колебания, которое распространяется по цепи ионов до второго кубита, где другой лазер останавливает движение и завершает двухкубитовую операцию. При данном методе требуется, чтобы ионы находились в предельно чистом вакууме при максимально низких температурах.



КК на основе ЯМР.

Преимущество метода использования ЯМР заключается в том, что его можно применять при комнатной температуре. Тем более что технология ЯМР в целом уже добилась некоторого успеха.

Суть метода в том, чтобы использовать макроскопическое количество материи и закодировать квантовый бит в среднем состоянии спина большего количества ядер. Состояниями спина можно управлять посредством магнитных полей, а среднее состояние спина можно измерить при помощи техники ЯМР. Основная проблема при использовании этого метода заключается в трудностях при увеличении квантового регистра. Мощность сигнала падает как 1/2n, где n - число кубитов.

Поиск по базе данных.

Основан на алгоритме Гровера.

Алгоритм Гровера — квантовый алгоритм быстрого поиска в неупорядоченной базе данных. Алгоритм был разработан Л. Гровером в 1996 году.

В классической модели вычислений среди алгоритмов поиска наибыстрейшим из возможных является линейный поиск, требующий N времени. Доказано, что он является наиболее быстрым квантовым алгоритмом для поиска в неупорядоченной базе данных. Также доказано, что не существует классических алгоритмов той же эффективности. Алгоритм Гровера обеспечивает квадратичный прирост скорости, в то время как некоторые другие квантовые алгоритмы, например, алгоритм факторизации Шора, дают экспоненциальный выигрыш по сравнению с соответствующими классическими алгоритмами. Но несмотря на это, квадратичный прирост значителен при достаточно больших значениях N.

Разложение натурального числа на множители.

Основан на алгоритме Шора.

Значимость алгоритма заключается в том, что при использовании достаточно мощного квантового компьютера, он сделает возможным взлом криптографических систем с открытым ключом. К примеру, RSA использует открытый ключ N, являющийся произведением двух больших простых чисел. Один из способов взломать шифр RSA — найти множители N. При достаточно большом N это практически невозможно сделать, используя известные классические алгоритмы. Так как алгоритм Шора работает только на квантовом компьютере, в настоящее время не существует технических средств, позволяющих за полиномиальное время от длины числа разложить достаточно большое число на множители. Алгоритм Шора в свою очередь, используя возможности квантовых компьютеров, способен произвести факторизацию числа за полиномиальное время. Это может поставить под угрозу надёжность большинства криптосистем с открытым ключом, основанных на сложности проблемы факторизации чисел.

Как и другие алгоритмы для квантовых компьютеров, алгоритм Шора вероятностный: он даёт верный ответ с высокой вероятностью. Вероятность ошибки может быть уменьшена при повторном использовании алгоритма. Тем не менее, так как возможна проверка предложенного результата (в частности простоту числа) в полиномиальное время, алгоритм может быть модифицирован так, что ответ, полученный в полиномиальное время, будет верным с единичной вероятностью.

Алгоритм Шора был разработан Питером Шором в 1994 году. Семь лет спустя, в 2001 году, его работоспособность была продемонстрирована группой специалистов IBM. Число 15 было разложено на множители 3 и 5 при помощи квантового компьютера с 7 кубитами..

КК в настоящее время.

- В феврале 2007 года канадская компания D-Wave Systems представила первый работающий прототип квантового компьютера Orion. Презентация работающего в Ванкувере компьютера производилась в Силиконовой долине. Компьютер представлял собой 16-кубитовый кремниевый чип, состоящий из кристалла ниобия, помещенного в катушку индуктивности. Работа квантового компьютера основана на измерении магнитных полей и переводу их изменений, вызванных ниобием, в результат счисления. Этот компьютер функционирует при температуре - 273,15 град Цельсия и охлаждается жидким гелием.
- Работают над квантовыми компьютерами и в России. Институт теоретической физики им. Ландау РАН и Физико-технологический институт РАН проводят опыты с разной архитектурой квантовых компьютеров, с разными материалами.