**МИНИСТЕРСТВО ОБЩЕГО И ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ РФ**

**АСТРАХАНСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ**

***кафедра теоретической физики***

РЕФЕРАТ

на тему:

***«Квантовые компьютеры»***

Выполнил:

студент 154 группы ФМФ

***Безниско Евгений.***

Руководитель:

к.ф.-м.н., доцент

***Джалмухамбетов А.У.***

*Астрахань – 2000 г.*

***Предпосылки создания квантовых компьютеров.***

Уже сейчас существует множество систем, в работе которых кванто­вые эффекты играют существен­ную роль. Одним из наиболее из­вестных примеров может служить лазер: поле его излучения поро­ждается квантово-механическими событиями - спонтанным и ин­дуцированным излучением света. Другим важным примером таких систем являются современные микросхемы - непрерывное ужесточение проектных норм приводит к тому, что квантовые эффекты начинают играть в их поведении существенную роль. В диодах Ганна возникают осцил­ляции электронных токов, в полу­проводниках образуются слои­стые структуры: электроны или дырки в различных запертых состояниях могут хранить информа­цию, а один или несколько элек­тронов могут быть заперты в так называемых квантовых ямах.

Сейчас ведутся разработки нового класса квантовых устройств - кванто­вых компьютеров. Идея кванто­вого компьютера возникла так.

Все началось в 1982 году, когда Фейнман написал очень интерес­ную статью [1], в которой рас­смотрел два вопроса. Он подошел к процессу вычисления как фи­зик: есть чисто логические огра­ничения на то, что можно вычис­лить (можно придумать задачу, для которой вообще нет алгорит­ма, можно придумать задачу, для которой любой алгоритм будет долго работать). А есть ли ограни­чения физические? Вот есть закон сохранения энергии - вечный двигатель невозможен; а есть ли какое-нибудь физическое огра­ничение на функционирование компьютера, которое накладыва­ет некие запреты на реализуемость алгоритмов? И Фейнман показал, что термодинамических ограни­чений, типа второго начала тер­модинамики, нет. Если мы будем уменьшать потери энергии, шумы, то мы можем сделать сколь угод­но длинные вычисления со сколь угодно малыми затратами энер­гии. Это означает, что вычисления можно сделать обратимым образом *-* потому что в необратимых про­цессах энтропия возрастает. Соб­ственно, Фейнмана это и заинте­ресовало: ведь реальное вычис­ление на реальном компьютере необратимо. И полученный им результат состоит в том, что мож­но так переделать любое вычис­ление - без особой потери эф­фективности, - чтобы оно стало обратимым. Те вычисления, кото­рые делаются «просто так», ко­нечно, необратимы, но «рост нео­братимости» пренебрежимо мал по сравнению, скажем, с шумами в современном компьютере. То есть необратимость - это тонкий эффект; тут вопрос не практичес­кий а принципиальный: если представить себе, что технология дойдет до такого уровня, что этот эффект станет существенным, то можно так перестроить вычисле­ния, чтобы добиться обратимости.

И в этой же работе Фейнман об­ратил внимание на то, что если у нас имеется устройство *квантовое*, то есть подчиняющееся законам кван­товой механики, то его вычисли­тельные возможности совершенно не обязательно должны совпадать с возможностями обычного устрой­ства. Возникают некоторые допол­нительные возможности. Но пока непонятно, позволяют они полу­чить какой-то выигрыш или нет. Фактически, он и поставил своей статьей такой вопрос.

Кстати, Ю.И. Манин в конце семидесятых годов написал две популярные книжки по логике - «Вычислимое и невычислимое» и «Доказуемое и недоказуемое», и в одной из них есть сюжет про кван­товые автоматы, где он говорит о некоторых кардинальных отличи­ях этих автоматов от классических [2].

В середине восьмидесятых годов появились работы Дойча (D. Deutsch), Бернстайна и Вазирани (Е. Bernstein, U. Vazirani), Яo (A. Уао). В них были построены формальные модели квантового компьютера - напри­мер, квантовая машина Тьюринга [3-6].

Следующий этап - статья Шора (Р.W. Shor) 1994 года [7], вызвавшая лавинообразный рост числа публикаций о квантовых вы­числениях. Шор построил кван­товый (то есть реализуемый на квантовом компьютере) алгоритм факторизации (разложения це­лых чисел на множители - ис­пользуется в том числе для вскры­тия зашифрованных сообщений). Все известные алгоритмы для обычного компьютера - экспо­ненциальные (время их работы растет как экспонента от числа зна­ков в записи факторизуемого чис­ла). Факторизация 129-разряд­ного числа потребовала 500 MIPS-лет, или восемь месяцев непре­рывной работы системы из 1600 рабочих станций, объединенных через Интернет. А при числе раз­рядов порядка 300 это время су­щественно превзойдет возраст Вселенной - даже если работать одновременно на всех существующих в мире машинах. Считается (хотя это и не доказано!), что бы­строго алгоритма решения этой задачи не существует. Более того, гарантией надежности большин­ства существующих шифров яв­ляется именно сложность реше­ния задачи факторизации или од­ной из родственных ей теорети­ко-числовых задач, например - дискретного логарифма. И вдруг выясняется, что на квантовом ком­пьютере эта задача имеет всего лишь кубическую сложность! Пе­ред квантовым компьютером клас­сические банковские, военные и другие шифры мгновенно теряют всякую ценность. Короче говоря, работа Шора показала, что вся эта изысканная академическая дея­тельность непосредственно каса­ется такой первобытной стихии, как деньги. После этого и началась настоящая популярность...

Впрочем, выясняется, что не толь­ко классическая, но и квантовая криптография (наука о шифрова­нии сообщений) часто не способна противостоять квантовой криптоаналитике (науке о расшифровке). Некоторые важные криптографи­ческие протоколы, такие как «под­брасывание монеты по телефону», рушатся при переходе к квантовым вычислениям. Точнее, гарантией их надежности является отныне не сложность тех или иных алгорит­мов, а сложность задачи создания квантового компьютера.

Таким образом возникает новая отрасль вычислений – квантовые вычисления. *Квантовые вычисления* (КВ) - это, как можно догадаться, вычисле­ния на квантовом компьютере. Квантовых компьютеров на свете пока нет. Более того, до сих пор неясно, когда появятся практиче­ски полезные конструкции и поя­вятся ли вообще. Тем не менее, квантовые вычисления - пред­мет, чрезвычайно модный сейчас в математике и физике, как теоре­тической, так и эксперименталь­ной, и занимается им довольно много людей. Судя по всему, именно инте­рес стимулировал первопроход­цев - Ричарда Фейнмана, напи­савшего пионерскую работу, в ко­торой ставился вопрос о вычис­лительных возможностях уст­ройств на квантовых элементах; Дэвида Дойча, формализовавше­го этот вопрос в рамках современ­ной теории вычислений; и Питера Шора, придумавшего первый не­тривиальный квантовый алгоритм.

***Типы квантовых компьютеров.***

Строго говоря, можно выделить два типа квантовых ком­пьютеров. И те, и другие основаны на квантовых явлениях, только разного порядка.

Представителями первого типа являются, например, компьютеры, в основе которых лежит квантова­ние магнитного потока на наруше­ниях сверхпроводимости - Джозефсоновских переходах. На эф­фекте Джозефсона уже сейчас де­лают линейные усилители, аналого-цифровые преобразователи, СКВИДы и корреляторы. Известен проект создания RISC-процессора на RSFQ-логике (Rapid Single Flux Quantum). Эта же элементная база используется в проекте создания петафлопного (1015 оп./с) компью­тера. Экспериментально достиг­нута тактовая частота 370 ГГц, ко­торая в перспективе может быть доведена до 700 ГГц. Однако время расфазировки волновых функций в этих устройствах сопоставимо со временем переключения отдель­ных вентилей, и фактически на но­вых, квантовых принципах реали­зуется уже привычная нам элемент­ная база - триггеры, регистры и другие логические элементы.

Другой тип квантовых компью­теров, называемых еще квантовы­ми когерентными компьютерами, требует поддержания когерентно­сти волновых функций исполь­зуемых кубитов в течение всего вре­мени вычислений - от начала и до конца (кубитом может быть лю­бая квантомеханическая система с двумя выделенными энергетиче­скими уровнями). В результате, для некоторых задач вычислительная мощность когерентных квантовых компьютеров пропорциональна *2N,* где *N* - число кубитов в компью­тере. Именно последний тип уст­ройств имеется в виду, когда го­ворят о квантовых компьютерах.

***Математические основы функционирования квантовых компьютеров.***

Классический компьютер состоит, грубо говоря, из некоторого числа битов, с которыми можно выпол­нять арифметические операции. Основным элементом кванто­вого компьютера (КК) являются квантовые биты, или кубиты (от Quantum Bit, qubit). Обычный бит - это классическая система, у которой есть только два возмож­ных состояния. Можно сказать, что пространство состояний бита - это множество из двух элемен­тов, например, из нуля и единицы. *Кубит* же - это квантовая система с двумя возможными состояниями. Имеется ряд примеров таких квантовых систем: электрон, у ко­торого спин может быть равен либо +1/2 либо –1/2, атомы в кристалли­ческой решетке при некоторых условиях. Но, поскольку система квантовая, ее пространство состо­яний будет несравненно богаче. Математически *кубит* - это двумерное комплек­сное пространство.

В такой системе можно вы­полнять унитарные преобразования про­странства состояний системы. С точки зрения геометрии такие пре­образования - прямой аналог вращении и симметрий обычного трехмерного пространства. Согласно принципу суперпозиции вы можете складывать состояния, вычитать их, ум­ножать на комплексные числа. Эти состояния образуют фазовые пространства. При объединении двух сис­тем полученное фазовое пространство будет их тензорным произведением. Эво­люция системы в фазовом про­странстве описывается унитарными преобразованиями фазового про­странства.

Так вот, в квантовом компьюте­ре аналогичная ситуация. Он тоже работает с нулями и единицами. Но его функциональные элемен­ты реализуют действия прямо в фазовом пространстве некоторой квантовой системы - при помо­щи унитарных преобразований этого пространства.

Конечно, унитарные пре­образования не могут быть произ­вольными - они должны удовлет­ворять некоторым естественным ог­раничениям. Например, в случае обычной логики достаточно иметь три операции: конъюнкция, дизъ­юнкция, отрицание. Все можно ре­ализовать, используя только эти три операции. Точно так же и в кванто­вом случае есть некоторый набор операторов, действующих только на три бита, с помощью которых мож­но все реализовать. Там есть даже более тонкие результаты: можно ограничиться классическими опера­торами на нескольких битах, а кван­товые операторы будут действовать только на один бит. То есть класси­ческий набор операций {конъюнк­ция, дизъюнкция, отрицание} мож­но заменить на такой: {конъюнкция, дизъюнкция, квантовое отрицание}, где квантовое отрицание - это про­извольное унитарное преобразо­вание одного кубита.

Фазовое пространство КК есть тензорное произведение кубитов. Если в каждом кубите фиксирован базис (он будет состоять из двух векторов), то фазовое простран­ство - это комплексное линейное пространство, базис которого ин­дексирован словами из нулей и единиц. Таким способом двоич­ное слово на входе определяет базисный вектор.

Итак, вход - двоичное слово, определяющее один из базисных векторов. Сам же алгоритм - предписанная последовательность элементарных операторов. При­меняем эту последовательность к вектору на входе, в результате по­лучаем некоторый вектор на выхо­де.

Так вот, согласно квантовой механике (КМ), пока система эволюционирует под дей­ствием наших унитарных операто­ров, мы не можем сказать, в каком именно классическом состоянии она находится. То есть она находится в каком-то квантовом состоянии, но измеряем-то мы, когда общаемся с системой, все равно какие-то классические значения. Как это понима­ется в КМ? В фазовом пространстве фиксируется некоторый базис, и век­тор состояния разлагается по этому базису. Это математическая форма­лизация процедуры измерения в КМ. То есть если мы имеем дело с сис­темой, у которой «то ли спин влево, то ли спин вправо», и если мы все-таки посмотрим, какой спин, то мы получим одно из двух в любом слу­чае. А вот вероятности того, что мы получим тот или другой резуль­тат, - это как раз квадраты модуля коэффициентов разложения. КМ ут­верждает, что точно предсказать ре­зультат измерения нельзя, но веро­ятности возможных результатов вы­числить можно.

Вероятность возни­кает в процессе измерения. А пока система живет, для нас существен­но, что там есть сам этот вектор.

Другими словами, существенно, что система «находится одновременно во всех возможных состояниях». Как пишут многие авторы популяр­ных введений в KB, возникает со­вершенно чудовищный параллелизм вычислении: к примеру, в случае нашей системы из двух кубитов мы как бы оперируем одновременно со всеми возможными ее состояниями: 00, 01, 11, 10.

Чтобы интерпретировать ответ, надо заранее условиться, что какой-то бит - допустим, первый - это бит ответа. Пусть алгоритм проработал, у нас получился ка­кой-то вектор, не обязательно ба­зисный. Тогда мы можем сказать, что первый бит с некоторой вероят­ностью равен 1. И требование к ал­горитму такое: если ответ «да», то вероятность того, что первый бит равен 1, должна быть больше двух третей. А если ответ «нет», вероят­ность того, что будет ноль, должна быть тоже больше двух третей.

***Задачи, реализуемые на КВ.***

Известно два примера нетри­виальных задач, в которых KB дают радикальный выигрыш.

Первый из них - задача разло­жения целых чисел на простые мно­жители и, как следствие, вычисле­ния дискретного логарифма (ДЛ). Дальше речь пойдет именно о ДЛ.

Пусть у нас есть поле вычетов по модулю простого числа. В нем есть первообразные корни - такие вы­четы, чьи степени порождают все ненулевые элементы. Если задан такой корень и задана степень, то возвести в степень можно быстро (например, сначала возводим в квадрат, потом получаем четвертую сте­пень, и т. д.) Дискретный лога­рифм - это обратная задача. Дан первообразный корень и какой-то элемент поля; найти, в какую степень нужно возвести этот корень, чтобы получить данный элемент. Вот эта задача уже считается сложной. На­столько сложной, что ряд совре­менных криптографических систем основан на том предположении, что вычислить ДЛ за приемлемое время невозможно, если модуль - доста­точно большое простое число.

Так вот, для дискретного лога­рифма есть эффективный кванто­вый алгоритм. Его придумал Шор в конце 1994 года. Пос­ле его статьи и начался взрыв публи­каций по КВ. Независимо от него, Алексей Китаев из ИТФ им. Ландау построил квантовый алгоритм для этой и некоторых более общих за­дач [8]. Идеи у них были разные.

Шор использовал примерно такую идею, она существенно квантовая: рассмот­рим базис в фазовом пространстве. Он состоит из классических состояний. Но в линейном пространстве много базисов. Мы можем найти некий оператор, который эффективно строит другой базис; мы можем к нему перейти, сделать там какие-то вычисления, вернуться обратно и получить нечто совершенно отлич­ное от того, что мы имели бы в классическом базисе. Одна из воз­можностей использовать квантовость состоит в том, что мы строим какой-то странный базис, в нем что-то делаем, возвращаемся обратно и интерпретируем результат. Шор именно эту идею и реализовал. При­чем преобразование оказалось та­кое, которое и в физике, и в матема­тике имеет принци­пиальное значение - дискретное преобразование Фурье.

Его можно представить в виде тензорного произведения опера­торов, которые действуют на каж­дый из кубитов такой матрицей:



Китаев придумал примерно следующее. Есть некото­рая ячейка - основной регистр, где мы записываем наши данные нулями и единицами. И еще есть один управляющий кубит. Мы ра­ботаем так: у нас реализована про­цедура умножения на первообраз­ный корень, на квадрат первооб­разного корня, и т. д. Управляю­щий кубит переводим в некоторое смешанное состояние, дальше строим такой оператор, который, в зависимости оттого, ноль или еди­ница в этом управляющем кубите, либо применяет умножение к на­шему основному регистру, либо не применяет. А потом кубит опять возвращаем в смешанное состоя­ние. Оказывается, что это эффек­тивный способ проделать некото­рое измерение. То есть Китаев за­метил, что одна из вещей, которые мы можем эффективно делать на квантовом компьютере, - это имитировать процесс квантового измерения. В данной задаче из результатов этих измерений эф­фективно извлекается ответ.

Сам процесс вычислений, происходит так: мы все время умножаем одну и ту же ячей­ку на некие константы, результаты измерений записываем, а потом производим своего рода обработ­ку результатов эксперимента - уже чисто классическими вычис­лениями. Вся квантовая часть зак­лючается в том, что где-то рядом с нашим регистром находится в некоем смешанном состоянии коррелированный с ним кубит, и мы его периодически наблюдаем.

Для вы­числения ДЛ числа, записанного *N* битами, нужно потратить *N 3* еди­ниц времени. Вполне реализуе­мо - на КК, естественно. Но здесь надо заметить, что никто пока не доказал, что не существует столь же быстрого алгоритма для вы­числения ДЛ на обычной машине.

Вторая задача предложена Гровером (L. Grover) [9]. Рассмотрим базу дан­ных, содержащую *2N* записей. Мы хотим найти ровно одну запись. Имеется некая процедура опреде­ления того, нужную запись мы взяли или нет. Записи не упоря­дочены. С какой скоростью мы можем решить эту задачу на обыч­ном компьютере? В худшем слу­чае нам придется перебрать все *2N* записей - это очевидно. Оказывается, что на КК достаточно числа запросов по­рядка корня из числа записей – *2*N*/2*.

Интересная задача - созда­ние оптимальных микросхем. Пусть есть функция, которую нужно ре­ализовать микросхемой, и эта функция задана программой, ис­пользующей полиномиально ог­раниченную память. Построение нужной микросхемы с минималь­ным числом функциональных эле­ментов - задача PSPACE. По­этому появление устройств, эф­фективно решающих PSPACE-задачи, позволило бы единообразно проектировать оптимальные по своим показателям вычислитель­ные устройства обычного типа. Кроме того, в PSPACE попадает большинство задач «искусственного интеллекта»: машинное обучение, распознавание образов и т.д.

Так вот, точно установлено, что KB находятся где-то между обыч­ными вероятностными вычисле­ниями и PSPACE. Если все же ока­жется, что KB можно эффективно реализовать на классических ве­роятностных машинах, не будет смысла в физической реализации квантовых машин. Если же выяс­нится, что при помощи KB можно эффективно решать те или иные PSPACE-задачи, то физическая реализация КК откроет принци­пиально новые возможности.

Есть еще одна область применения КК, где заведомо возможен радикальный выигрыш у существующих техно­логий. Это моделирование самих квантовых систем.

Давайте посмотрим на такой вопрос: как можно эволюцию квантовой системы изучать на обычном компьютере? Это посто­янно делается, так как это задача важна для химии, молеку­лярной биологии, физики и т.п. Но, за счет эк­споненциального роста размер­ности при тензорном произведе­нии, для моделирования десяти спинов вам нужно оперировать с тысячемерным пространством, сто спинов - это уже конец. А если вспомнить, что в молекуле белка десятки тысяч атомов, то... Там, правда, не всюду существенно именно квантовое моделирование, но в целом ясно, что есть очень серьезные препятствия для моде­лирования квантовых систем на классических компьютерах. Так что если создать вычислительное устройство, которое ведет себя квантовым образом, то по край­ней мере один важный класс за­дач на нем есть смысл решать - можно моделировать реальные квантовые системы, возникающие в физике, химии, биологии.

***Проблемы создания КК.***

Когда начался бум вокруг квантовых вычислений, физики высказывались об этом бо­лее чем скептически. Модель кван­товых вычислений не противоре­чит законам природы, но это еще не значит, что ее можно реализовать. К примеру, можно вспомнить создание атом­ного оружия и управляемый термояд.

А если говорить о КК, надо отме­тить одну очень серьезную пробле­му. Дело в том, что любая физичес­кая реализация будет приближен­ной. Во-первых, мы не сможем сде­лать прибор, который будет давать нам произвольный вектор фазово­го пространства. Во-вторых, работа любого устройства подвержена вся­ческим случайным ошибкам. А уж в квантовой системе - пролетит ка­кой-нибудь фотон, провзаимодействует с одним из спинов, и все поменяется. Поэтому сразу возник вопрос, можно ли, хотя бы в прин­ципе, организовать вычисления на ненадежных квантовых элементах, чтобы результат получался со сколь угодно большой достоверностью. Такая задача для обычных компью­теров решается просто - напри­мер, за счет введения дополнитель­ных битов.

В случае КК эта проблема го­раздо глубже. То место, где воз­никает новое качество KB по срав­нению с обычными вычисления­ми, - это как раз сцепленные состояния - ли­нейные комбинации базисных век­торов фазового пространства. У вас есть биты, но они не сами по себе живут в каких-то состояниях - это был бы просто вероят­ностный компьютер (компьютер, дающий тот или иной ответ с определенной вероятностью), - а они на­ходятся в некоем смешанном со­стоянии, причем согласованно-смешанном. Из-за этого в КК нельзя, например, просто взять и скопировать один бит в другой! Обычная интуиция из теории алгоритмов здесь неприменима.

Так что проблема надежности довольно сложна, даже на уровне чистой теории. Те люди, которые активно занимаются KB, активно ее решали и добились успеха: доказано, что, как и в классике, можно делать вычисления на элементах с за­данной надежностью сколь угод­но точно. Это реализовано с по­мощью некоего аналога кодов, ис­правляющих ошибки.

Что касается технической сто­роны появляются сообщения, что созда­ются реальные квантовые систе­мы с небольшим числом битов - с двумя, скажем. Эксперименталь­ные, в железе, так сказать.

Так что эксперименты есть, но пока очень далекие от реальнос­ти. Два бита - это и для класси­ческого и для квантового компь­ютера слишком мало! Чтобы мо­делировать молекулу белка, нуж­но порядка ста тысяч кубитов. Для ДЛ, чтобы вскрывать шифры, достаточно примерно тысячи кубитов.

Задача эта возникла слишком недавно, и не исключено, что она потребует каких-то фундаменталь­ных исследований в самой физи­ке. Поэтому в обозримом будущем ожидать появления квантовых ком­пьютеров не приходится.

Но можно ожидать распрост­ранения через не очень долгое время квантовых криптографи­ческих систем. Квантовая крип­тография позволяет обмениваться сообщениями так, что враг, если попытается подслушать, сможет разве что разрушить ваше сооб­щение. То есть оно не дойдет до адресата, но перехватить его в принципе будет нельзя. Подобные системы, кото­рые уже реализованы, используют све­товод. Универсальный КК здесь не нужен. Нужно специа­лизированное квантовое устрой­ство, способное выполнять только небольшой набор операций, - сво­его рода квантовый кодек.

Физической системе, реализующей квантовый компьютер, можно предъявить пять требований:

1. Система должна состоять из точно известного числа частиц.
2. Должна быть возможность привести систему в точно известное начальное состояние.
3. Степень изоляции от внешней среды должна быть очень высока.
4. Надо уметь менять состояние системы согласно заданной последовательности унитарных преобразований ее фазового пространства.
5. Необходимо иметь возможность выполнять «сильные измерения» состояния системы (то есть такие, которые переводят ее в одно из чистых состояний).

Из этих пяти задач наиболее трудными считаются третья и четвертая. От того, насколько точно они решаются, зависит точность выполнения операций. Пятая задача тоже весьма неприятна, так как измерить состояние отдельной частицы нелегко.

*Физические основы организации КК.*

Итак, что же это за тайное оружие такое - КК? Остроумная идея за­ключается в использовании для хра­нения, передачи и обработки ин­формации существенно квантовых свойств вещества. В основном такие свойства проявляют объекты мик­ромира: элементарные частицы, атомы, молекулы и небольшие сгу­стки молекул, так называемые кла­стеры. (Хотя, конечно, и в жизни макромира квантовая механика иг­рает важную роль. В частности, только с ее помощью можно объяснить та­кое явление, как ферромагнетизм.) Одним из квантовых свойств веще­ства является то, что некоторые ве­личины при измерении (наблюде­нии) могут принимать значения лишь из заранее определенного дискрет­ного набора. Такой величиной, на­пример, является проекция собст­венного момента импульса, или, ина­че говоря, спина элементарной час­тицы, на любую заданную ось. На­пример, у электрона возможно только два значения проекции: +*1/2* или *–1/2*. Таким образом, количество информации, необходимое для со­общения о проекции, равно одному биту. Записав в классическую одно­битную ячейку памяти определен­ное значение, мы именно его оттуда и прочтем, если не произойдет ка­кой-нибудь ошибки.

Классической ячейкой может послужить и спин электрона. Од­нако квантовая механика позволя­ет записать в проекции спина боль­ше информации, чем в классике.

Для описания поведения кван­товых систем было введено понятие волновой функции. Существуют волновые функции, называемые собственными для какой-то кон­кретной измеряемой величины. В состоянии, описываемом собствен­ной функцией, значение этой вели­чины может быть точно предсказа­но до ее измерения. Именно с таки­ми состояниями работает обычная память. Квантовая же система может находиться и в состоянии с волно­вой функцией, равной линейной комбинации собственных функции, соответствующих каждому из воз­можных значений (назовем здесь такие состояния сложными). В сложном состоянии результат из­мерения величины не может быть предсказан заранее. Заранее из­вестно только, с какой вероятно­стью мы получим то или иное зна­чение. В отличие от обычного ком­пьютера, в квантовом для представ­ления данных используются такие ячейки памяти, которые могут на­ходиться в сложном состоянии. В нашем примере мы определили бы, что спин электрона с определенной вероятностью смотрит вверх и вниз, то есть можно сказать, что в кубит записаны сразу и 0, и 1. Количество информации, содержащееся в та­кой ячейке, и саму ячейку называют квантовым битом, или, сокращен­но, кубитом. Согласитесь, ячейки в сложных состояниях весьма не­обычны для классической теории информации. Каждому возможно­му значению величины, представ­ленной кубитом, соответствует ве­роятность, с которой это значение может быть получено при чтении. Эта вероятность равна квадрату мо­дуля коэффициента, с которым соб­ственная функция этого значения входит в линейную комбинацию. Именно вероятность и является ин­формацией, записанной в кубит.

Квантовую механику не случай­но называют иногда волновой ме­ханикой. Дело в том, что квантово-механические волновые функции ведут себя подобно световой или какой-либо другой волне. И для волновых функций, благодаря их способности интерферировать, также может быть введено понятие когерентности. Именно это свой­ство используется в когерентном квантовом компьютере. Набор кубитов представляется когерентны­ми волновыми функциями. Ока­зывается, что существует вполне определенный класс воздействий на квантовую систему, называе­мый унитарными преобразования­ми, при которых не теряется запи­санная в кубит информация и не нарушается когерентность волно­вых функций кубитов. Унитарные преобразования обратимы - по результату можно восстановить ис­ходные данные. После прохожде­ния через квантовый процессор, использующий унитарные преоб­разования, волновые функции ку­битов заставляют интерферировать друг с другом, наблюдая получаю­щуюся картину и судя по ней о результате вычисления.

Из-за того, что для представле­ния информации используются кубиты, в которых записано сразу оба значения - и *0*, и *1*, в процессе вычислений происходит парал­лельная обработка сразу всех воз­можных вариантов комбинаций би­тов в процессорном слове. Таким образом, в КК реализуется естест­венный параллелизм, недоступный классическим компьютерам. За счет возможности параллельной работы с большим числом вариантов, в идеале равным *2N* (где *N* - число кубитов), квантовому компьютеру необходимо гораздо меньше вре­мени для решения определенного класса задач. К ним относятся, на­пример, задача разложения числа на простые множители или поиск в большой базе данных. Для коге­рентного компьютера уже предло­жены алгоритмы, использующие его уникальные свойства. Кроме того, предполагается использовать КК для моделирования квантовых систем, что трудно или вообще невозможно сделать на обычных компьютерах из-за нехватки мощности или по принципиальным соображениям.

Все существующие на сегодняш­ний день обычные компьютеры, да­же с параллельной обработкой ин­формации на многих процессорах, могут быть смоделированы так на­зываемым клеточным автоматом Тьюринга. Это существенно детер­минированная и дискретная маши­на. С возникновением и обсуждени­ем идей квантовых вычислений ста­ла активно развиваться квантовая теория информации и, в частности, теория квантовых клеточных авто­матов - ККА. Квантовый клеточный автомат является обобщением авто­мата Тьюринга для КК. Сформули­рована гипотеза, гласящая, что каж­дая конечным образом реализуемая физическая система может быть дос­таточно хорошо смоделирована универсальной моделью квантовой вычислительной машины, исполь­зующей ограниченное количество ресурсов. Для одного из предложенных типов ККА теоретически уже доказано, что он подходит для тако­го моделирования и не противоре­чит квантовой теории.

Пытаясь осуществить свой за­мысел, ученые упираются в про­блему сохранения когерентности волновых функций кубитов, так как потеря когерентности хотя бы од­ним из кубитов разрушила бы ин­терференционную картину. В на­стоящее время основные усилия экспериментальных рабочих групп направлены на увеличение отно­шения времени сохранения коге­рентности ко времени, затрачивае­мому на одну операцию (это отно­шение определяет число операций, которые можно успеть провести над кубитами). Главной причиной по­тери когерентности является связь состояний, используемых для ку­битов, со степенями свободы, не участвующими в вычислениях. На­пример, при передаче энергии элек­трона в возбужденном атоме в по­ступательное движение всего ато­ма. Мешает и взаимодействие с ок­ружающей средой, например, с со­седними атомами материала ком­пьютера или магнитным полем Зем­ли, но это не такая важная проблема. Вообще, любое воздействие на ко­герентную квантовую систему, ко­торое принципиально позволяет получить информацию о каких-ли­бо кубитах системы, разрушает их когерентность. Потеря когерентно­сти может произойти и без обмена энергией с окружающей средой.

Воздействием, нарушающим когерентность, в частности, явля­ется и проверка когерентности. При коррекции ошибок возникает сво­его рода замкнутый круг: для того чтобы обнаружить потерю коге­рентности, нужно получить ин­формацию о кубитах, а это, в свою очередь, также нарушает когерент­ность. В качестве выхода предло­жено много специальных методов коррекции, представляющих так­же и большой теоретический инте­рес. Все они построе­ны на избыточном кодировании.

Если в области передачи инфор­мации уже созданы реально рабо­тающие системы и до коммерческих продуктов осталось лишь несколько шагов, то коммерческая реализация квантового когерентного процессо­ра - дело будущего. К настоящему времени КК научился вычислять сум­му *1+1*! Это большое достижение, если учесть, что в виде результата он выдает именно *2*, а не *3* и не *0*. Кроме того, не следует забывать, что и пер­вые обычные компьютеры были не особенно мощны.

Сейчас ведется работа над дву­мя различными архитектурами процессоров: типа клеточного ав­томата и в виде сети логических элементов. Пока не известно о ка­ких-либо принципиальных пре­имуществах одной архитектуры перед другой. Как функциональ­ная основа для логических эле­ментов квантового процессора бо­лее или менее успешно использу­ется целый ряд физических явле­ний. Среди них - взаимодействие одиночных поляризованных фо­тонов или лазерного излучения с веществом или отдельными ато­мами, квантовые точки, ядерный магнитный резонанс и - наибо­лее многообещающий - объем­ный спиновый резонанс. Процессор, постро­енный на последнем принципе, в шутку называют «компьютером в чашке кофе» - из-за того, что в нем работают молекулы жидкости при комнатной температуре и ат­мосферном давлении. Кроме этих эффектов есть довольно хорошо развитая технология логических элементов и ячеек памяти на джозефсоновских переходах, которую можно при соответствующих ус­ловиях приспособить под коге­рентный процессор.

Теорию, описывающую явле­ния, лежащие в основе первого типа логических ячеек, называют квантовой электродинамикой в по­лости или резонаторе. Кубиты хра­нятся в основных и возбужденных состояниях атомов, расположен­ных некоторым образом на равных расстояниях в оптическом резона­торе. Для каждого атома исполь­зуется отдельный лазер, приводя­щий его в определенное состояние с помощью короткого импульса. Взаимовлияние атомных состоя­ний происходит посредством об­мена фотонов в резонаторе. Ос­новными причинами разрушения когерентности здесь служат спон­танное излучение и выход фото­нов за пределы резонатора.

В элементах на основе ионов в линейных ловушках кубиты хра­нятся в виде внутренних состояний пойманных ионов. Для управле­ния логикой и для манипулирова­ния отдельными кубитами также используются лазеры. Унитарные преобразования осуществляются возбуждением коллективных кван­тованных движений ионов. Источ­никами некогерентности является спонтанный распад состояний ио­нов в другие внутренние состояния и релаксация в колебательные сте­пени свободы.

Сильно отличается от двух пре­дыдущих «компьютер в чашке ко­фе». Благодаря достоинствам данного метода этот ком­пьютер является наиболее реаль­ным претендентом на то, чтобы достигнуть разрядности 10 бит в бли­жайшее время. В компьютере на кол­лективном спиновом резонансе ра­ботают молекулы обычных жидко­стей (без всяких квантовых вывертов типа сверхтекучести). В качестве ку­битов используется ориентация ядерных спинов. Работа логических ячеек и запись кубитов осуществля­ется радиочастотными электромаг­нитными импульсами со специаль­но подобранными частотой и фор­мой. В принципе, прибор похож на обычные приборы ядерного маг­нитного резонанса (ЯМР) и исполь­зует аналогичную аппаратуру. Жиз­неспособность этого подхода обес­печивается, с одной стороны, очень слабой связью ядерных спинов с окружением и, потому, большим временем сохранения когерентно­сти (до тысяч секунд). Эта связь ос­лаблена из-за экранирования ядер­ных спинов спинами электронов из оболочек атомов. С другой стороны, можно получить сильный выход­ной сигнал, так как для вычислений параллельно используется большое количество молекул. «Не так уж сложно измерить спин четвертого ядра у какого-то типа молекул, если у вас имеется около числа Авогадро (~1023) таких молекул», - говорит Ди Винченцо (Di Vincenzo), один из исследователей. Для определения результата непрерывно контроли­руют излучение всего ансамбля. Та­кое измерение не приводит к потере когерентности в компьютере, как было бы в случае использования толь­ко одной молекулы.

Ядерные спины в молекулах жидкости при комнатной темпера­туре хаотически разупорядочены, их направления равномерно рас­пределены от 0 до 4π. Проблема записи и считывания кажется не­преодолимой из-за этого хаоса. При воздействии магнитного поля спины начинают ориентироваться по полю. После снятия поля через небольшое время система снова приходит к термодинамическому равновесию, и в среднем лишь около миллионной доли всех спинов остается в состоянии с ориентацией по направлению поля. Однако бла­годаря тому, что среднее значение сигнала от хаотически направлен­ных спинов равно нулю, на этом фоне можно выделить довольно слабый сигнал от «правильных» спинов. Вот в этих-то молекулах с правильными ядерными спинами и размещают кубиты. Для коррек­ции ошибок при записи *N* кубитов используют *2N* или больше спинов. Например, для *N*=1 выбираются такие жидкости, где какие-то два спина ядер в одной молекуле после опре­деленного воздействия полем мо­гут быть ориентированны только одинаково. Тогда по направлению второго спина при снятии резуль­тата обработки можно отсеять нуж­ные молекулы, никак не влияя на первый спин.

Как уже было сказано, обработ­ка битов осуществляется радиоим­пульсами. Основным логическим элементом является управляемый инвертор. Из-за спин-спинового взаимодействия резонансная час­тота, при которой происходит оп­рокидывание одного спина, зави­сит от направления другого.

Что касается квантовой передачи данных, к настоящему времени экспериментально реализованы системы обмена секретной информацией по незащищенному от несанкционированного доступа каналу. Они основаны на фундаментальном постулате квантовой механики о невоз­можности измерения состояния без оказания влияния на него. Подслушивающий всегда изменяет состояние кубитов, кото­рые он подслушал, и это может быть зафиксировано связы­вающимися сторонами. Данная система защиты информации абсолютно надежна, так как способов обойти законы кванто­вой механики пока еще никто не выдумал.

***Вместо заключения…***

Пока квантовым компьютерам по плечу только наиболее простые за­дачи - например, они уже умеют складывать 1 и 1, получая в резуль­тате 2. Было также запланировано взятие дру­гого важного рубежа - фактори­зации числа 15, его предстоит раз­ложить на простые множители - 3 и 5. А там, глядишь, дойдет дело и до более серьезных задач.

Опытные образцы сейчас со­держат менее десяти квантовых би­тов. По мнению Нейла Гершенфельда (Nell Gershenfeld), участвовав­шего в создании одной из первых действующих моделей квантового компьютера, необходимо объеди­нить не менее 50-100 кубитов, что­бы решать полезные с практиче­ской точки зрения задачи. Интерес­но, что добавление каждого сле­дующего кубита в квантовый ком­пьютер на эффекте объемного спи­нового резонанса требует увеличе­ния чувствительности аппаратуры в два раза. Десять дополнительных кубитов, таким образом, потребуют увеличения чувствительности в 1000 раз, или на 60 дБ. Двадцать - в миллион раз, или на 120 дБ...

He исключе­но, что в информационном обще­стве появление квантового компь­ютера сыграет ту же роль, что в свое время, в индустриальном, - изоб­ретение атомной бомбы. Действи­тельно, если последняя является средством «уничтожения мате­рии», то первый может стать сред­ством «уничтожения информа­ции» - ведь очень часто то, что известно всем, не нужно никому.

**Литература, содержащая основную информацию о КК.**

1. Feynman R. Int. J. Theor. Phys. 21, 1982.
2. Манин Ю.И. Вычислимое и невычислимое. - М.: Советское ра­дио, 1980.
3. Feynman R. Quantum mechanical computers. // Optics News, February 1985, 11, p.11.
4. Deutsch D. Quantum theory, the Church-Turing principle and the universal quantum computer. - Proc. R. Soc. London A 400, 97, 1985.
5. Deutsch D. Quantum computational networks. - Proc. R. Soc. London A 425, 73, 1989.
6. Yao А. С.-С. Quantum circuit complexity. //Proceedings of the 34th Annual Symposium on the Foundations of Computer Science, IEEE Computer Society Press, Los Alamitos, CA, 1993, p. 352.
7. Shor P.W. Algorithms for Quantum Computation: Discrete log and Factoring. // Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, edited by S. Goldwasser, IEEE Computer Society Press, Los Alamitos, CA, 1994, p.124.
8. Китаев A.Ю. Квантовые вычисления: алгоритмы и исправление ошибок. //Успехи математических наук.
9. Grover L. Afast quantum mechanical algorithm for database search. //Proceedings of the 28th Annual ACM Symposium on Theory of Computing, 1996, pp. 212-219.
10. Kitaev A.Yu. Quantum measurements and the Abelian stabilizer problem. - LANL e-print quant-ph/9511026, http://xxx.lanl.gov.
11. Shor P.W. Fault-Tolerant Quantum Computation. - LANL e-print quant-ph/9005011, http://xxx.lanl.gov.
12. Bennett С.Н., Bernstein E., Brassard G., Vazirany U. Strengths and Weaknesses of Quantum Computing. - LANL e-print quant-ph/9701001, http://xxx.lanl.gov, to appear in SIAM J. On Computing.