МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ РАДИОФИЗИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ
Кафедра физики и аэрокосмических технологий

КВАНТОВЫЕ КОМПЬЮТЕРЫ

Реферат

Дуньчик Алёны Игоревны

Студентка 2 курса 4 группы

Минск 2021

Оглавление

Введение

Цифровые электронные компьютеры, широко используемые в настоящее время, созданы с помощью полупроводниковых технологий. Такие компьютеры обычно представляют собой совокупность элементов только с двумя возможными логическими состояниями «0» и «1» — так называемыми «битами». Такие компьютеры, в которых логические операции производятся с этими классическими, с точки зрения физики, состояниями в настоящее время принято называть классическими.

Однако уже достаточно давно было обнаружено, что эти классические компьютеры не могут справиться с некоторыми очень важными задачами. Примерами таких задач являются поиск в неструктурированной базе данных, моделирование эволюции квантовых систем (например, ядерные реакции) и, наконец, факторизация больших чисел.

Интерес к последней задаче связан с тем, что практически все современные шифры для секретной переписки основаны на этой математической процедуре. Для взлома уже существующего кода необходима работа классического компьютера в течение нескольких лет.

Идея квантовых вычислений впервые была высказана Ю.И. Маниным [1] в 1980 году, но активно эта проблема стала обсуждаться после появления в 1982 году статьи американского физика-теоретика Р. Фейнмана [2]. В этих работах было предложено использовать для вычислений операции с состояниями квантовой системы. Авторы обратили внимание на то, что каждое состояние квантовой системы в отличие от классической может находиться в состоянии суперпозиции. В терминах классического компьютера квантовый бит, или кубит, в соответствии с законами квантовой механики может находиться одновременно в состоянии «0» и «1».

Наиболее популярная попытка объяснения этой «странности» квантового мира производится на примере свойства спина электрона, ярко проявляющегося в экспериментах ядерного магнитного резонанса (ЯМР). Это свойство электрона часто изображают в виде вращения волчка с осью вращения, направленной вверх или вниз. Спин вверх можно принять за единицу, спин вниз за ноль. Но оказывается можно показать математически, что электрон может также находиться в «призрачном» двойном состоянии,

состоянии суперпозиции, в котором спин как бы смотрит одновременно вверх и вниз. Это означает, что такое состояние есть одновременно ноль и единица. Если теперь выполнять вычисление с помощью этого электрона, то они будут выполняться с одновременным использованием нуля и единицы!

Поскольку данная работа имеет реферативный характер, то основной её целью является знакомство с основными знаниями и понятиями на таком уровне, что человек, не имеющий никакого понятия о квантовых вычислениях и квантовых компьютерах, но имеющий определённую математическую подготовку, после ознакомления с ней мог свободно читать научную литературу, посвящённую этому вопросу.

В первом разделе рассмотрена сама идея квантовых вычислений и её история, а также алгоритмы факторизации чисел и поиска в неупорядоченной базе данных. Второй раздел посвящён реализации квантовых компьютеров и основным направлениям развития их элементной базы.

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 уже существует новый класс квантовых устройств - квантовых компьютеров, которые с каждым годом увеличивают свою мощность. Идея квантового компьютера возникла так.

Все началось в 1982 году, когда Фейнман [2] написал очень интересную статью, 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.

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

Следующий этап - статья Шора (P.W. Shor) [7] 1994 года, 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. 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.

Благодаря этом открытиям началось стремительно развитие квантовых вычислений. В 2000 году продемонстрирован первый работающий пяти кубитный квантовый компьютер в Мюнхенском техническом университете. 2007 канадская компания D-WAVE продемонстрировала первый 16-кубитный и 28-кубитный квантовый компьютер. В 2011 году они выпустили квантовый компьютер с 128-битным чипом. В 2013 с 512-битным чипом. На самом деле эти компьютеры способны справится только с одной определенной задачей. Из-за этого на данный момент самым мощным квантовым компьютером считается 51-кубитный квантовый компьютер, который разработали русские ученые в 2017 году.

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. 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.
Базовым элементом квантового компьютера (носителем квантовой информации) является квантовый бит – кубит. В системах квантовой связи информация передаётся путём физического переноса кубита – носителя информации – или методом телепортации квантового состояния кубита.
В качестве кубита может быть выбрана любая квантовая система с двумя состояниями, характеризуемыми ортонормированными волновыми функциями $¿\varphi_0\rangle$ и $¿\varphi_1\rangle$. Удобным примеров кубита являются ядерные (или электронные) спины $I=1/2$, которые в постоянном внешнем магнитном поле B имеют два уровня энергии:

$E_0=\frac{-1}{2}\hbar\gamma B$, $E_1=\frac{1}{2}\hbar\gamma B$, соответствующих направлениям спина вдоль поля или против поля (рис. 1).

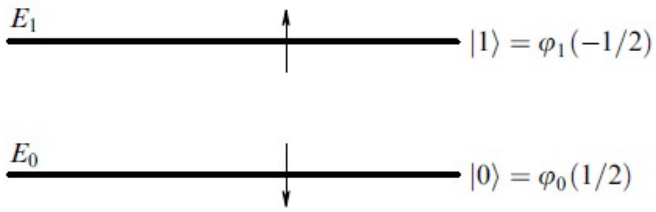

Рис. 1 Схема квантового бита - кубита

Волновые функции $¿\varphi_0\rangle=¿I_z=\frac{1}{2}\rangle, \vee\varphi_1\rangle=¿I_z=\frac{-1}{2}\rangle$ являются собственными функциями оператора полной энергии спина в магнитном поле B: $H=-I_z\hbar\gamma B$. [8]

Система является квантовой, поэтому ей пространство будет намного 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 квантовых компьютеров 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 квантовой механике? 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. Квантовая механика 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 квантовые вычисления, 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 КВ 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 [9]. 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:

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}.$$

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) [10]. Рассмотрим базу данных, содержащую 2^N 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 2^N 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 КВ находятся где-то между обычными вероятностными вычислениями и PSPACE. Если все же окажется, что КВ можно эффективно реализовать на классических вероятностных машинах, не будет смысла в физической реализации квантовых машин. Если же выяснится, что при помощи КВ 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 КВ 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 КВ, 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.

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 2^N (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 ($\sim 10^{23}$)

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 4p. 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 ориентированы 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 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.

Область применения

Основное применение квантовым вычислениям — это искусственный интеллект. ИИ основан на принципах обучения в процессе извлечения опыта, становится все точнее по мере работы обратной связи, пока, наконец, не обзаводится «интеллектом», пусть и компьютерным. То есть самостоятельно обучается решению задач определенного типа. Эта обратная связь зависит от расчета вероятности для множества возможных исходов, и квантовые вычисления идеально подходят для такого рода операций. Искусственный интеллект, подкрепленный квантовыми компьютерами, перевернет каждую отрасль, от автомобилей до медицины, и говорят, что ИИ станет для двадцать первого века тем, чем электричество стало для двадцатого.

Другой пример — это точное моделирование молекулярных взаимодействий, поиск оптимальных конфигураций для химических реакций. Такая «квантовая химия» настолько сложная, что с помощью современных цифровых компьютеров можно проанализировать только простейшие молекулы. Химические реакции квантовые по своей природе, поскольку образуют весьма запутанные квантовые состояния суперпозиции. Но полностью разработанные квантовые компьютеры смогут без проблем рассчитывать даже такие сложные процессы.

Квантовая криптография. Создание новых надежных алгоритмов шифрования. Например, чтобы взломать алгоритм классическим компьютером, нужно перебрать все возможные варианты. Это требует огромного количества времени, что делает эту операцию дорогостоящей и не практичной. А квантовые компьютеры могут выполнять такое разложение гораздо быстрее и эффективнее.

Как ни странно, глубокое изучение физики с применением квантовых компьютеров может привести… к изучению новой физики. Модели физики элементарных частиц зачастую чрезвычайно сложные, требуют пространных решений и задействуют много вычислительного времени для численного моделирования. Они идеально подойдут для квантовых компьютеров, и ученые уже положили на них глаз. Ученые Университета Инсбрука и Института квантовой оптики и квантовой информации (IQOQI) недавно использовали программируемую квантовую систему для подобных манипуляций с моделями. Для этого они взяли простую версию квантового компьютера, в котором ионы производят логические операции, базовые шаги

в любом компьютерном расчете. Моделирование показало прекрасное соглашение с реальными, описанными физикой, экспериментами.

И это не весь список, ведь по мере развития квантовых компьютеров будут расширяться возможности и сферы их применений.

Заключение

Вместе с квантовым компьютером наступит новая эра вычислений и научных открытий. Если создать квантовый компьютер из 200 кубитов, то мощность этого компьютера будет равна больше, чем число атомов во всей вселенной. Что позволит моделировать различные физические системы.

Пока квантовые компьютеры способны выполнять простые задачи. Но в дальнейшем, с развитием квантовых технологий и вычислений, они будут способны выполнять очень сложные задачи, которые не способен выполнить простой компьютер. В квантовом компьютере скрыт большой потенциал.

Не 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

1. Манин Ю.И. Вычислимое и невычислимое. - М.: Советское радио, 1980. – С. 17-101. – ил. (Кибернетика).

2. Feynman R.P. Simulating Physics with Computers. / R.P. Feynman // International Journal of Theoretical Physics. – 1982. – Vol. 21, №12. – P. 467-788.

3. Фейнман Р.Ф. Квантовомеханические ЭВМ. / Р.Ф. Фейнман; пер. с англ. Б. Ф. Полковникова под ред. И. И. Мазина. // Успехи физических наук. Т.149, Физика наших дней. – 1986. – №4. – С. 671–688.

4. Deutsch D. Quantum theory, the Church-Turing principle and the universal quantum computer. / D. Deutsch // Proceeding of the Royal Society of London. – 1985. – A400. – P. 97.

5. Deutsch D. Quantum computational networks / D. Deutsch // Proceeding of the Royal Society of London. – 1989. – A425. – P. 73.

6. Yao A.C. – C. Quantum circuit complexity. / A.C. Yao // 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. / P.W. Shor; edited by S. Goldwasser. // Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, IEEE Computer Society Press. – Los Alamitos, CA, 1994. – P. 124.

8. Валиев К.А. Квантовые компьютеры и квантовые вычисления. / К.А. Валиев // Успехи физических наук. Т. 175, Обзоры актуальных проблем. – 2005. – №1. – С. 3-39.

9. Китаев А.Ю. Квантовые вычисления: алгоритмы и исправление ошибок. / А.Ю. Китаев // Успехи математических наук. Т. 52. – 1997. – №6. – С. 53-112.

10. Grover L. Afast quantum mechanical algorithm for database search. / L. Grover // Proceedings of the 28th Annual ACM Symposium on Theory of Computing. – 1996. – P. 212-219.