МИНИСТЕРСТВО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

**Реферат**

**Квантовые вычисления**

2009

**Содержание**

Введение

Глава I. Основные понятия квантовой механики

Глава II. Основные понятия и принципы квантовых вычислений

Глава III. Алгоритм Гровера

Заключение

Список литературы

**Введение**

*Представьте себе компьютер, память которого экспоненциально больше, чем можно было бы ожидать, оценивая его явный физический размер; компьютер, который может оперировать одновременно с экспоненциально большим набором входных данных; компьютер, который проводит вычисления в туманном для большинства из нас гильбертовом пространстве.*

*Тогда вы думаете о квантовом компьютере.*

Идея вычислительного устройства, основанного на квантовой механике, впервые рассматривалась еще в ранних 1970-х годах и ранних 1980-х физиками и компьютерными учеными, такими, например, как Чарльз Х. Беннет из IBM Thomas J. Watson Research Center, Пол А. Бениофф из Аргоннской национальной лаборатории в Иллинойсе, Дэвидом Дойчем из Оксфордского университета, и позднее Ричардом П. Фейнманом из из Калифрнийского технологического института (Калтех). Идея возникла тогда, когда ученые заинтересовались фундаментальными ограничениями вычислений. Они поняли, что если технология будет продолжать следовать постепенному уменьшению размеров вычислительных сетей упакованных в кремниевые ЧИПы, то это приведет к тому, что индивидуальные элементы станут не больше чем несколько атомов. Тогда возникла проблема, так как на атомном уровне действуют законы квантовой физики, а не классической. А это подняло вопрос, можно ли сконструировать компьютер, основанный на принципах квантовой физики.

Фейнман одним из первых попытался дать ответ на этот вопрос. В 1982г. он предложил модель абстрактной квантовой системы, пригодной для вычислений. Он также объяснил, как такая система может быть симулятором в квантовой физике. Другими словами, физики могли бы проводить вычислительные эксперименты на таком квантовом компьютере.

Позже, в 1985 году, Дойч осознал, что утверждение Фейнмана могло бы, в конце концов, привести к квантовому компьютеру общего назначения, и опубликовал важнейшую теоретическую работу, показывающую, что любой физический процесс может в принципе быть промоделирован на квантовом компьютере.

К сожалению, все, что тогда смогли придумать, было несколько довольно надуманных математических задач, до тех пор, пока Шор выпустил в 1994 году свою работу, в которой представил алгоритм решения на квантовом компьютере одной важной задачи из теории чисел, а именно, разложения на простые множители. Он показал, как набор математических операций, сконструированных специально для квантового компьютера, может *факторизовать* (разложить на простые множители) огромные числа фантастически быстро, значительно быстрее, чем на обычных компьютерах. Это был прорыв, который перевел квантовые вычисления из разряда академического интереса в разряд задачи, интересной для всего мира.

**Глава I. Основные понятия квантовой механики**

В конце 19 века среди ученых было широко распространено мнение, что физика – наука «практически завершенная» и для полной её «завершенности» осталось совсем немного: объяснить структуру *оптических спектров атомов* и спектральное распределение *теплового излучения*. *Оптические спектры атома* получаются при испускании или поглощении света (электромагнитных волн) свободными или слабо связанными атомами; такими спектрами обладают, в частности, одноатомные газы и пары.

*Тепловое излучение* – это механизм переноса тепла между пространственно разделёнными частями тела за счет электромагнитного излучения.

Однако начало 20 века привело к пониманию того, что ни о какой «завершенности» не может быть и речи. Становилось ясным, что для объяснения этих и многих других явлений требуется кардинальным образом пересмотреть представления, лежащие в основе физической науки.

Например, исходя из волновой теории света, оказалось невозможным дать исчерпывающее объяснение всей совокупности оптических явлений.

При решении проблемы спектрального состава излучения немецким физиком Максом Планком в 1900 году было высказано предположение о том, что излучение и поглощение света веществом происходит конечными порциями, или *квантами.* При этом энергия *фотона* - *кванта электромагнитного излучения* (в узком смысле — света) определяется выражением

,

Где  - частота излучаемого (или поглощаемого) света, а  – универсальная постоянная, называемая теперь постоянной Планка.



Часто используется постоянная Дирака 

Тогда энергия кванта выражается как , где

 - круговая частота излучения.

Противоречия между рассмотрением света как потока заряженных частиц и как волны привело к понятию *корпускулярно-волнового дуализма.*

С одной стороны, фотон демонстрирует свойства электромагнитной волны в явлениях *дифракции* (огибание волнами препятствий, сравнимых с длинной волны) и *интерференции* (наложение волн с одинаковой частотой и с одинаковой начальной фазой) в масштабах, сравнимых с длиной волны фотона. Например, одиночные фотоны, проходящие через двойную щель, создают на экране интерференционную картину, которую можно описать *уравнениями Максвелла*. Тем не менее, эксперимент показывает, что фотоны излучаются и поглощаются целиком объектами, размеры которых много меньше длины волны фотона (например, атомами), или, вообще, в некотором приближении могут считаться точечными (например, электрон), то есть ведут себя как частицы - *корпускулы*. В окружающем нас макромире существует два фундаментальных способа передачи энергии и импульса между двумя точками пространства: непосредственное перемещение материи в одной точки в другую и волновой процесс передачи энергии без переноса вещества. Все носители энергии здесь строго разделены на корпускулярные и волновые. Напротив, в микромире такого разделения не существует. Всем частицам, а в частности и фотонам, приписываются одновременно и корпускулярные, и волновые свойства. Ситуация ненаглядна. Это объективное свойство квантовых моделей.

Почти монохроматическое излучение с частотой **** испускаемое источником света, можно представить себе состоящим из «пакетов излучения», которые мы называем фотонами. Монохроматическое излучение – обладающее очень малым разбросом частот, в идеале — одной длиной волны.

Распространение фотонов в пространстве правильно описывается классическими уравнениями Максвелла. При этом каждый фотон считается классическим *цугом* *волн*, определенным двумя векторными полями - напряженностью электростатического поля  и индукцией магнитного поля . Цуг волн — это ряд возмущений с перерывами между ними. Излучение отдельного атома не может быть монохроматическим, потому что излучение длится конечный промежуток времени, имея периоды нарастания и угасания.

Неправильно интерпретировать сумму квадратов амплитуд  и  как плотность энергии в пространстве, в котором движется фотон; вместо этого каждую величину, квадратично зависящую от амплитуды волны следует интерпретировать как величину пропорциональную вероятности какого-либо процесса. Скажем,  не равен энергии, вносимой фотоном в эту область, а пропорционален вероятности обнаружить фотон в этой области.

Энергия, переданная в каком-либо месте пространства фотоном, всегда равна . Тем самым  где  - вероятность нахождения фотона в данной области, а - число фотонов.

В 1921 году опытом Штерна-Герлаха было подтверждено наличие у атомов *спина* и факт пространственного квантования направления их магнитных моментов (от англ. spin — вращаться, вертеться.). *Спин* -собственный момент количества движения элементарных частиц, имеющий квантовую природу и не связанный с перемещением частицы как целого. При введении понятия спина предполагалось, что электрон можно рассматривать как «вращающийся волчок», а его спин - как характеристику такого вращения. Спином называют также собственный момент импульса атомного ядра или атома; в этом случае спин определяется как векторная сумма (вычисленная по правилам сложения моментов в квантовой механике) спинов элементарных частиц, образующих систему, и орбитальных моментов этих частиц, обусловленных их движением внутри системы.

Спин измеряется в единицах (приведенных постоянных Планка, или постоянных Дирака) и равен , где *J* — характерное для каждого сорта частиц целое (в т. ч. нулевое) или полуцелое положительное число - *спиновое квантовое число*, которое обычно называют просто спином (одно из квантовых чисел). В связи с этим говорят о целом или полуцелом спине частицы. Однако не следует путать понятия спин и спиновое квантовое число. Спиновое квантовое число — это квантовое число, определяющее величину спина квантовой системы (атома, иона, атомного ядра, молекулы), т. е. её собственного (внутреннего) момента импульса. Проекция спина на любое фиксированное направление z в пространстве может принимать значения *J, J—1, ..., —J.* Т. о., частица со спином *J* может находиться в *2J + 1* спиновых состояниях (при *J* = 1/2 - в двух состояниях), что эквивалентно наличию у неё дополнительной внутренней степени свободы.

Ключевым элементом квантовой механики является *принцип неопределенности Гейзенберга*, который говорит о том, что нельзя одновременно точно определить положение частицы в пространстве и ее импульс. Этот принцип объясняет квантование света, а также пропорциональную зависимость энергии фотона от его частоты.

Движение фотона можно описать системой уравнений Максвелла, в то время как уравнение движения любой другой элементарной частицы типа электрона описывается уравнением Шрёдингера, которое более общее.

Система уравнений Максвелла инвариантна относительно преобразования Лоренца. *Преобразованиями Лоренца* в специальной теории относительности называются преобразования, которым подвергаются пространственно-временные координаты *(x,y,z,t)* каждого события при переходе от одной инерциальной системы отсчета к другой. По сути, эти преобразования представляют собой преобразования не только в пространстве, как преобразования Галилея, но и во времени.

**Глава II. Основные понятия и принципы квантовых вычислений**

Хотя компьютеры стали компактными и значительно быстрее, чем раньше, справляются со своей задачей, сама задача остается прежней: манипулировать последовательностью битов и интерпретировать эту последовательность как полезный вычислительный результат. Бит - это фундаментальная единица информации, обычно представляемая как 0 или 1 в вашем цифровом компьютере. Каждый классический бит физически реализуется макроскопической физической системой, такой как намагниченность на жестком диске или заряд конденсатора. Например, текст, составленный из *n* символов, и сохраненный на жестком диске типичного компьютера, описывается строкой из *8n* нулей и единиц. Здесь и лежит фундаментальное отличие между вашим классическим компьютером и квантовым компьютером. В то время как классический компьютер подчиняется хорошо понятным законам классической физики, квантовый компьютер это устройство, которое использует квантово-механические явления (в особенности *квантовую интерференцию*), чтобы осуществлять совершенно новый способ обработки информации.

В квантовом компьютере фундаментальная единица информации (называемая квантовый бит или *кубит*), не двоична, а скорее четверична по своей природе. Это свойство кубита проистекает как прямое следствие его подчиненности законам квантовой механики, которые радикально отличаются от законов классической физики. Кубит может существовать не только в состоянии, соответствующем логическим 0 или 1, как классический бит, но также в состояниях, соответствующих смесли или *суперпозиции* этих классических состояний. Другими словами, кубит может существовать как ноль, как единица, и как одновременно 0 и 1. При этом можно указать некоторый численный коэффициент, представляющий вероятность оказаться в каждом состоянии.

Идеи о возможности построения квантового компьютера восходят к работам Р. Фейнмана 1982- 1986 гг. Рассматривая вопрос о вычислении эволюции квантовых систем на цифровом компьютере, Фейнман обнаружил "нерешаемость" этой задачи: оказывается, что ресурсы памяти и быстродействия классических машин недостаточны для решения квантовых задач. Например, система из *n* квантовых частиц с двумя состояниями (спины *1/2*) имеет *2n* базисных состояний; для ее описания необходимо задать (и записать в память ЭВМ) *2n* амплитуд этих состояний. Отталкиваясь от этого негативного результата, Фейнман высказал предположение, что, вероятно, "квантовый компьютер" будет обладать свойствами, которые позволят решать на нем квантовые задачи.[3]

"Классические" компьютеры построены на транзисторных схемах, обладающих нелинейными зависимостями между входными и выходными напряжениями. По существу, это бистабильные элементы; например, при низком входном напряжении (логический "0") входное напряжение высокое (логическая "1"), и наоборот. Такой бистабильной транзисторной схеме в квантовом мире можно сопоставить двухуровневую квантовую частицу: состоянию  припишем значения логического , состоянию ,  *-* значение логической . Переходам  в бистабильной транзисторной схеме здесь будут соответствовать переходы с уровня на уровень: . Однако квантовый бистабильный элемент, получивший название кубит, обладает новым, по сравнению с классическим, свойством суперпозиции состояний: он может быть в любом суперпозиционном состоянии , где — комплексные числа, . Состояния квантовой системы из *п* двухуровневых частиц имеют в общем случае вид суперпозиции  *2n* базовых состоянии . В конечном счете квантовый принцип суперпозиции состояний позволяет придать квантовому компьютеру принципиально новые "способности".

Доказано, что квантовая ЭВМ может быть построена всего из двух элементов (вентилей): однокубитового элемента и двухкубитового элемента контролируемое НЕ (CNOT). Матрица *2x2* элемента имеет вид:



 (1)

Вентиль описывает поворот вектора состояния кубита от оси z к полярной оси, заданной углами *.* Если  — иррациональные числа, то многократным применением вектору состояния можно придать любую наперед заданную ориентацию. Именно в этом заключается "универсальность" однокубитового вентиля в форме (1). В частном случае получаем однокубитовый логический элемент НЕ (NOT): НЕ=, НЕ=. При физической реализации элемента НЕ необходимо воздействовать на квантовую частицу (кубит) импульсом извне, переводящим кубит из одного состояния в другое. Вентиль контролируемое НЕ исполняют, воздействуя на два взаимодействующих между собой кубита: при этом посредством взаимодействия один кубит контролирует эволюцию другого. Переходы под влиянием внешних импульсов хорошо известны в импульсной магниторезонансной спектроскопии. Вентиль НЕ соответствует перевороту спина под действием импульса  (вращение намагниченности вокруг оси на угол )*.* Вентиль CNOT выполняется на двух спинах *1/2* с гамильтонианом (спин контролирует ). CNOT выполняется в три шага: импульс + свободная прецессия в течение времени - импульс . Если  (контролирующий кубит в состоянии ), то при указанных воздействиях контролируемый кубит совершает переходы  (или ). Если же  (контролирующий кубит в состоянии ), то результат эволюции контролируемого кубита будет другим:  (). Таким образом, спин , эволюционирует по-разному при :  здесь в - состояние контролирующего кубита.[4]



При рассмотрении вопроса о реализации квантового компьютера на тех или иных квантовых системах в первую очередь исследуют реализуемость и свойства элементарных вентилей НЕ и контролируемое НЕ.

Для дальнейшего полезно также ввести однокубитовое преобразование Адамара:

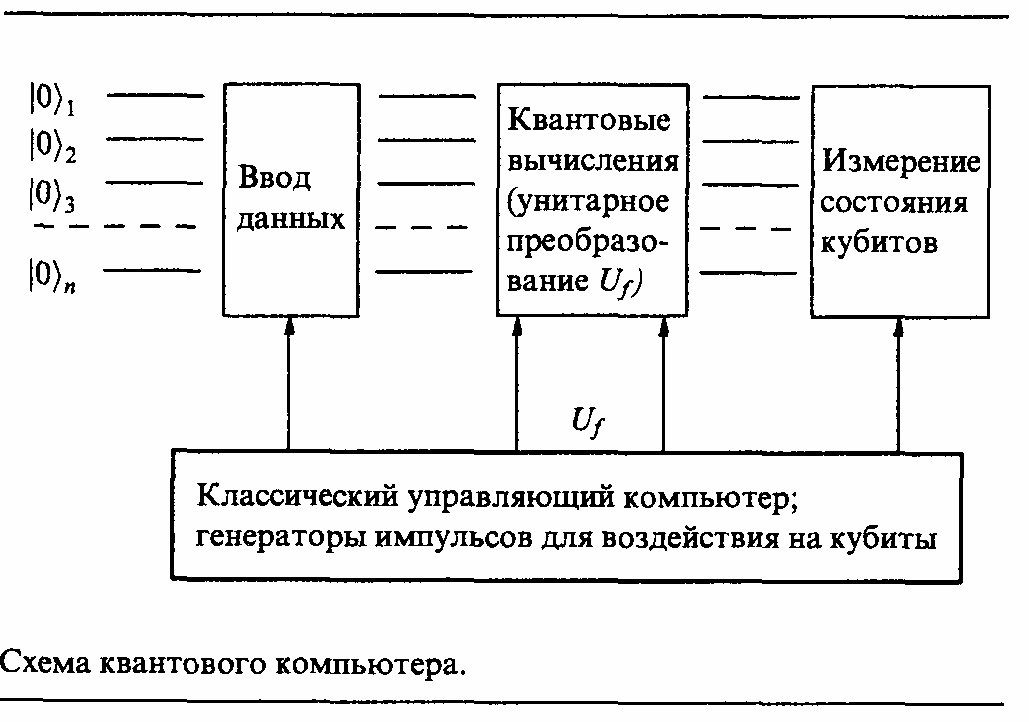


В технике магнитного резонанса эти вентили осуществляются импульсами :

Адамара:



Схема квантового компьютера представлена на рисунке. До начала работы компьютера все кубиты (квантовые частицы) должны быть приведены в состояние , т.е. в основное состояние. Это условие само по себе не тривиально.



Оно требует или глубокого охлаждения (до температур порядка милликельвина), или применения методов поляризации. Систему *п* кубитов в состоянии можно считать регистром памяти, приготовленным для записи входных данных и проведения вычислений. Кроме этого регистра обычно предполагают существование дополнительных (вспомогательных) регистров, необходимых для записи промежуточных результатов вычислений. Запись данных осуществляется путем того или иного воздействия на каждый кубит компьютера. Примем, например, что над каждым кубитом регистра совершается преобразование Адамара:



 (2)

В результате система перешла в состояние суперпозиции из *2п* базисных состояний с амплитудой *2-n/2.* Каждое базисное состояние представляет собой двоичное число от  до . Горизонтальные линии на рисунке обозначают оси времени.



Выполнение алгоритма совершается путем унитарного преобразования суперпозиции .представляет собой унитарную матрицу размерности *2п.* При физическом осуществлении посредством импульсных воздействий на кубиты извне матрица должна быть представлена как векторное произведение матриц размерности 2 и *.* Последние могут быть выполнены последовательным воздействием на единичные кубиты или пары кубитов *:*



 (3)

Количество сомножителей в этом разложении определяет длительность (и сложность) вычислений . Все в (3) выполняются с применением операций NOT, CNOT, Н (или их разновидностей).



Замечательно, что линейный унитарный оператор действует одновременно на все члены суперпозиции



 (4)

Результаты вычисления записываются в запасном регистре, который перед применением находился в состоянии . За один прогон вычислительного процесса мы получаем значения искомой функции f при всех значениях аргумента *х = 0,...,* *2п — 1*. Этот феномен получил название квантового параллелизма.



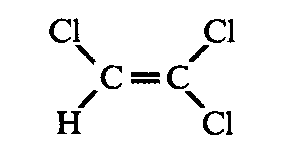
Измерение результата вычислений сводится к проецированию вектора суперпозиции в (4) на вектор одного из базисных состояний *:*

 (5)

Здесь проступает одно из слабых мест квантового компьютера: число в процессе измерения "выпадает" по закону случая. Чтобы найти при заданном *,* надо много раз провести вычисления и измерения, пока случайно не выпадет *.*

При анализе унитарной эволюции квантовой системы, совершающей вычислительный процесс, выявляется важность физических процессов типа интерференции. Унитарные преобразования совершаются в пространстве комплексных чисел, и сложение фаз этих чисел носит характер интерференции. Известна продуктивность преобразований Фурье в явлениях интерференции и спектроскопии. Оказалось, что и в квантовых алгоритмах неизменно присутствуют преобразования Фурье. Преобразование Адамара является простейшим дискретным фурье-преобразованием. Вентили типа NOT и СNOT могут быть осуществлены непосредственно на интерферометре Маха-Зендера с использованием явления интерференции фотона и вращения его вектора поляризации.

Исследуются различные пути физической реализации квантовых компьютеров. Модельные эксперименты по квантовому компьютингу выполнены на импульсном ядерном магнитно-резонансном спектрометре. В этих моделях работало два или три спина (кубита), например два спина ядер 13С и один спин протона в молекуле трихлорэтилена



Однако в этих опытах квантовый компьютер был "ансамблевым": выходные сигналы компьютера сложены большим числом молекул в жидком растворе *(~ 1020).*

К настоящему времени высказаны предложения о реализации квантовых компьютеров на ионах и молекулах в ловушках в вакууме, на ядерных спинах в жидкостях (см. выше), на ядерных спинах атомов 31Р в кристаллическом кремнии, на спинах электронов в квантовых точках, созданных в двумерном электронном газе в гетероструктурах GaAs, на переходах Джозеф-сона. Как видим, в принципе, квантовый компьютер можно построить на атомных частицах в вакууме, жидкости, кристаллах. При этом в каждом случае предстоит преодолеть те или иные препятствия, однако среди них можно выделить несколько общих, обусловленных принципами действия кубитов в квантовом компьютере. Поставим задачу создать полномасштабный квантовый компьютер, содержащий, скажем, 103 кубитов (хотя и при *п = 100* квантовый компьютер может стать полезным инструментом).

1. Нужно найти способы "инициализации" кубитов компьютера в состояние . Для спиновых систем в кристаллах очевидно применение сверхнизких температур и сверхсильных магнитных полей. Применение поляризации спинов накачкой может оказаться полезным при одновременном применении охлаждения и больших магнитных полей.

Для ионов в вакуумных ловушках сверхнизкое охлаждение ионов (атомов) достигается лазерными методами. Очевидна также необходимость холодного и сверхвысокого вакуума.

2. Необходимо иметь технологию избирательного воздействия импульсами на любой выбранный кубит. В области радиочастот и спинового резонанса это означает, что каждый спин должен обладать своей резонансной частотой (в терминах спектроскопического разрешения). Различия резонансных частот для спинов в молекулах обусловлены химическими сдвигами для спинов одного изотопа и одного элемента; необходимые различия частот имеются для спинов ядер различных элементов. Однако здравый смысл подсказывает, что эти дарованные природой различия резонансных частот вряд ли достаточны, чтобы работать с *103* спинов.

Более перспективными представляются подходы, когда можно управлять извне резонансной частотой каждого кубита. В предложении о кремниевом квантовом компьютере кубитом служит ядерный спин примесного атома 31Р. Частота резонанса определяется константой *А* сверхтонкого взаимодействия ядерного и электронного спинов  атома 31Р. Электрическое поле на наноэлектроде, находящемся над атомом 31Р, поляризует атом и изменяет константу *А* (соответственно резонансную частоту ядерного спина). Таким образом, наличие электрода встраивает кубит в электронную схему и настраивает его резонансную частоту.

3. Для выполнения операции CNOT (контролируемое НЕ) необходимо взаимодействие между кубитами и вида *.* Такое взаимодействие возникает между спинами ядер в молекуле, если ядра и  разделены одной химической связью. В принципе, необходимо иметь возможность выполнять операцию  для любых пар кубитов *.* Иметь физическое взаимодействие кубитов одного масштаба величины и по принципу "все со всеми" в природной среде вряд ли возможно. Очевидна потребность в способе настройки среды между кубитами извне путем введения электродов с управляемым потенциалом. Таким путем можно создать, например, перекрытие волновых функций электронов в соседних квантовых точках и возникновение взаимодействия вида между спинами электронов [. Перекрытие волновых функций электронов соседних атомов 31Р обусловливает возникновение взаимодействия вида  между ядерными спинами.

Чтобы обеспечить операцию , где и  — отдаленные кубиты, между которыми взаимодействие вида отсутствует, необходимо применить в компьютере операцию обмена состояниями по цепочке так что обеспечивает операцию , поскольку состояние совпадает с состоянием .

4. В ходе выполнения унитарного преобразования, соответствующего избранному алгоритму, кубиты компьютера подвергаются воздействию со стороны среды; в результате амплитуды и фазы вектора состояния кубита испытывают случайные изменения — *декогеренизацию*. По существу, декогеренизация — это релаксация тех степеней свободы частицы, которые используются в кубите. Время декогеренизации  равно времени релаксации. В ядерном магнитном резонансе в жидкостях времена  и  релаксации составляют 1-10 с. Для ионов в ловушках с оптическими переходами между уровнями *Е0* и *Е1* временем декогеренизации выступают время спонтанного излучения и время столкновений с остаточными атомами. Очевидно, что декогеренизация — это серьезное препятствие квантовому вычислению: начатый вычислительный процесс приобретает черты случайности по истечении времени декогеренизации. Однако можно достичь устойчивого квантового вычислительного процесса в течение сколь угодно долгого времени т > та, если систематически использовать методы квантового кодирования и коррекции ошибок (фазовых и амплитудных). Доказано, что при относительно невысоких требованиях к безошибочному выполнению элементарных операций типа NОТ и СNОТ (вероятность ошибки не более 10-5) методы квантовой коррекции ошибок (QEC) обеспечивают устойчивую работу квантового компьютера.

Возможно и активное подавление процесса декогеренизации, если над системой кубитов проводить периодические измерения. Измерение с большой вероятностью обнаружит частицу в "правильном" состоянии, а малые случайные изменения вектора состояния при измерении коллапсируют (квантовый эффект Зенона). Однако трудно пока сказать, насколько полезным может быть такой прием, поскольку такие измерения сами по себе могут воздействовать на вычислительный процесс и нарушить его.

5. Состояния кубитов после завершения вычислительного процесса должны быть измерены, чтобы определить результат вычисления. Сегодня нет освоенной технологии таких измерений. Очевиден, однако, путь поисков такой технологии: надо использовать методы усиления в квантовом измерении. Например, состояние ядерного спина  передается электронному спину ; от последнего зависит орбитальная волновая функция; зная орбитальную волновую функцию, можно организовать передачу зарядов (ионизацию); присутствие или отсутствие заряда одиночного электрона можно обнаружить классическими электрометрическими методами. Большую роль в этих измерениях будут играть, вероятно, методы зондовой силовой микроскопии.

К настоящему времени открыты квантовые алгоритмы, приводящие к экспоненциальному ускорению вычислений по сравнению с вычислениями на классическом компьютере. К ним относится алгоритм Шора определения простых множителей больших (многоразрядных) чисел. Эта чисто математическая проблема тесно связана с жизнью общества, так как на "невычислимости" таких множителей построены современные шифровальные коды. Именно это обстоятельство вызвало сенсацию, когда был открыт алгоритм Шора. Для физиков важно, что и решение квантовых задач (решение уравнения Шрёдингера для многочастичных систем) экспоненциально ускоряется, если использовать квантовый компьютер.

Наконец, очень важно, что в ходе исследований задач квантового компьютинга подвергаются новому анализу и экспериментальной проверке основные проблемы квантовой физики: проблемы локальности, реальности, дополнительности, скрытых параметров, коллапса волновой функции.

Идеи квантового компьютинга и квантовой связи возникли спустя сто лет после рождения первоначальных идей квантовой физики. Возможность построения квантовых компьютеров и систем связи показана выполненными к настоящему времени теоретическими и экспериментальными исследованиями. Квантовая физика "достаточна" для проектирования квантовых компьютеров на различной "элементной базе". Квантовые компьютеры, если их удастся построить, будут техникой XXI века. Для их изготовления потребуется создание и развитие новых технологий на нанометровом и атомном уровне размеров. Эта работа может занять, по-видимому, несколько десятилетий. Построение квантовых компьютеров было бы еще одним подтверждением принципа неисчерпаемости природы: природа имеет средства для осуществления любой корректно сформулированной человеком задачи.

В обычном компьютере информация кодируется последовательностью битов, и эти биты последовательно обрабатываются булевскими логическими элементами, чтобы получить нужный результат. Аналогично квантовый компьютер обрабатывает кубиты, выполняя последовательность операций квантовыми логическими элементами, каждый из которых представляет собой унитарное преобразование, действующее на единичный кубит или пару кубитов. Последовательно выполняя эти преобразования, квантовый компьютер может выполнить сложное унитарное преобразование над всем набором кубитов приготовленных в некотором начальном состоянии. После этого можно произвести измерение над кубитами, которое и даст конечный результат вычислений. Это сходство вычислений между квантовым и классическим компьютером позволяет считать, что, по крайней мере, в теории, классический компьютер может в точности воспроизводить работу квантового компьютера. Другими словами, классический компьютер может делать все то же самое, что и квантовый компьютер. Тогда зачем вся эта возня с квантовым компьютером? Дело в том, что, хотя теоретически классический компьютер может симулировать квантовый компьютер, это очень неэффективно, настолько неэффективно, что практически классический компьютер не в состоянии решать многие задачи, которые по плечу квантовому компьютеру. Симуляция квантового компьютера на классическом компьютере вычислительно сложная проблема, потому что корреляции между квантовыми битами качественно отличается от корреляций между классическими битами, как было впервые показано Джоном Беллом. Для примера можно взять систему только из нескольких сотен кубитов. Она существует в пространстве Гильберта размерностью *~1090,* что потребует, при моделировании классическим компьютером, использования экспоненциально больших матриц (чтобы выполнить расчеты для каждого отдельного состояния, которое также описывается матрицей). Это означает, что классическому компьютеру понадобится экпоненциально больше времени по сравнению даже с примитивным квантовым компьютером.

Ричард Фейнман был среди первых, кто осознал потенциал, заложенный в явлении квантовой суперпозиции для решения таких задач гораздо быстрее. Например, система из 500 кубитов, которую практически невозможно промеделировать классически, представляет собой квантовую суперпозицию из *2500* состояний. Каждое значение такой суперпозиции классически эквивалентно списку из 500 единиц и нулей. Любая квантовая операция над такой системой, например, настроенный определенным образом импульс радиоволн, который может выполнить операцию управляемое НЕ над, скажем, 100-м и 101-м кубитом, будет одновременно воздействовать на *2500* состояний. Таким образом, за один тик компьютерных часов квантовая операция вычисляет не одно машинное состояние, как обычные компьютеры, а *2500* состояний сразу! Однако, в конце концов, над системой кубитов производится измерение, и система коллапсирует в единственное квантовое состояние, соответствующее единственному решению задачи, единственному набору из 500 единиц и нулей, как это диктуется измерительной аксиомой квантовой механики. Это поистине волнующий результат, поскольку это решение, найденное колективным процессом квантовых параллельных вычислений, берущим свои истоки в суперпозиции, эквивалентно выполнению той же самой операции на классическом суперкомпьютере с ~*10150* отдельных процессоров (что, конечно, невозможно)!! Первые исследователи в этой области были, конечно, вдохновлены такими гигантскими возможностями, и поэтому вскоре началась настоящая охота за подходящими задачами для такой вычислительной мощи. Питер Шор, исследователь и компьютерный ученый из компании AT&T's Bell Laboratories в Нью Джерси, предложил такую задачу, которую можно было бы решить именно на квантовом компьютере и при помощи квантового алгоритма. Алгоритм Шора использует мощь квантовой суперпозиции, чтобы раскладывать большие числа (порядка ~10200 двоичных разрядов и больше) на множители за несколько секунд. Эта задча имеет важное практическое применение для шифрования, где общепринятый (и лучший) алгоритм шифрования, известный как RSA, основан как раз на сложности разложения больших составных чисел на простые множители. Компьютер, который с легкостью решает такую задачу, конечно, представляет большой интерес для множества правительственных организаций, использующих RSA, который до сих пор считался "невзламываемым", и для любого кто заинтересован в безопсаности своих данных.

Шифрование, однако, только одно возможное применение квантового компьютера. Шор разработал целый набор математических операций, которые могут быть выполнены исключительно на квантовом компьютере. Некоторые из этих операций используются в его алгоритие факторизации. Далее, Фейнман утверждал, что квантовый компьютер может действовать как моделирующее устройство для квантовой физики, потенциально открывая двери ко многим открытиям в этой области. В настоящее время мощь и возможности квантового компьютера, в основном, предмет теоретических рассуждений; появление первого по-настоящему функционального квантового компьютера, несомненно, принесет много новых и волнующих практических применений.

**Глава III. Алгоритм Гровера**

Задача поиска состоит в следующем: имеется неупорядоченная база данных, состоящая из N-элементов, из которых лишь один удовлетворяет данным условиям — именно этот элемент нужно найти. Если элемент можно осмотреть, то определение того, удовлетворяет он требуемым условиям или нет, осуществляется за один шаг. Однако база данных такова, что в ней не существует какого-либо упорядочения, которое могло бы помочь выбору элемента. Наиболее эффективный классический алгоритм для этой задачи состоит в проверке элементов из базы данных одного за другим. Если элемент удовлетворяет требуемым условиям, поиск окончен, если нет, то данный элемент откладывается так, так чтобы он вновь не подвергался проверке. Очевидно, что в этом алгоритме требуется проверить в среднем элементов прежде, чем будет найден нужный. [1]



Реализуя данный алгоритм, можно используя то же самое оборудование, как в классическом случае, но задавая вход и выход в виде *суперпозиции* состояний, можно найти объект за *O*() *квантовомеханических шагов* вместо *О(N))* классических шагов. Каждый квантовомеханический шагсостоит из элементарной унитарной операции, которые рассмотрим далее.



Для осуществления данного алгоритма нам необходимы следующие три элементарные операции. Первая — это приготовление состояния, в котором система находится с равной вероятностью в любом из ее N базисных состояний; вторая — это преобразование Адамара и третья — выборочный поворот фаз состояний.

Как известно основной операцией для квантовых вычислений является операция *М*, действующая на один бит, которая представляется следующей матрицей:



т. е. бит в состоянии 0 превращается в суперпозицию двух состояний: (1/, 1/). Аналогично, бит в состоянии 1 трансформируется в (1/,, —1/,), т. е. величина амплитуды для каждого состояния равна 1/,, но фаза в состоянии 1 перевернута. Фаза не имеет аналога в классических вероятностных алгоритмах. Она возникает в квантовой механике, где амплитуда вероятности комплексна. В системе, в которой состояние описывается *п* битами (т. е. имеется *N = 2п* возможных состояний), мы можем осуществить преобразование *М* на каждом бите независимо, последовательно изменяя состояние системы. В случае, когда начальная конфигурация представляла собой конфигурацию с *п* битами в первом состоянии, полученная конфигурация будет иметь равные амплитуды для каждого из состояний. Это и есть способ создания суперпозиции с той же самой амплитудой для всех состояний.



Третье преобразование, которое нам понадобится, — это выборочное вращение фазы амплитуды в определенных состояниях. Преобразование, представленное здесь для системы из двух состояний, имеет форму:



где *j=* и *—* произвольные действительные числа. Заметим, что в отличие от преобразования Адамара и других матриц преобразования состояний, вероятность каждого состояния остается той же, т. к. квадрат абсолютной величины амплитуды в каждом состоянии остается прежним.



Рассмотрим задачу в абстрактной форме.

Пусть система имеет *N = 2п* состояний, которые обозначаются как ,..., . Эти *2п* состояния представляются как n-битные строки. Пусть существует единственное состояние, скажем , которое довлетворяет условию C() = 1, тогда как для всех других состояний S, *С(*,*) =* 0 (предполагается, что для любого состояния S условие оценивается за единицу времени). Задача состоит в распознании состояния ,



Перейдем собственно к алгоритму

Шаги (1) и (2) являются последовательностью элементарных унитарных операций описаных ранее. Шаг (3) есть завершающее измерение, осуществляемое внешней системой.

**(1)** Приводим систему в состояние суперпозиции:



с одинаковыми амплитудами для каждого из N состояний. Эта суперпозиция может быть получена за шагов.



**(2)** Повторим следующую унитарную операцию *О( )* раз:



**a**. Пусть система будет в каком-нибудь состоянии S:

В случае *С(S) =* 1, повернуть фазу на радиан;



В случае *С(S) =* 0, оставить систему неизмененной.

**b.** Применить преобразование диффузии *D* которое определяется матрицей *D* следующим образом:, если ;' и *. D* может быть реализована как последовательное выполнение унитарных преобразований: , где *W* – матрица преобразований Адамара, R – матрица фазового поворота.



**(3)** Произвести измерение полученного состоянии. Это состояние будет состоянием *С()„* (т. е. искомым состоянием, удовлетворяющим условию (C() = 1) с вероятностью, по крайней мере, не меньшей, чем 0.5. Заметим, что шаг (2а) — это фазовое вращение. В его реализацию должна быть включена процедура распознания состояния и последующего определения осуществлять или нет поворот фазы. Она должна проводиться таким образом, чтобы не оставлять следа на состоянии системы, так, чтобы была уверенность, что пути, приводящие к тому же самому конечному состоянию, неразличимы и могут интерферировать. Заметим, что эта процедура *не* включает классического измерения.



Данный квантовый алгоритм поиска, вероятно, будет проще реализовать по сравнению со многими другими известными квантово-механическими алгоритмами, так как необходимые операции — это только преобразование Уолша-Адамара и операция условного сдвига фазы, каждая из которых относительно проста по сравнению с операциями, используемыми другими квантово-механическими алгоритмами.

**Заключение**

Сейчас квантовые компьютеры и квантовые информационные технологии остаются в состоянии пионерских разработок. Решение трудностей, с которыми сейчас столкнулись эти технологии, обеспечит прорыв квантовых компьютеров к их законному месту самых быстрых вычислительных машин из всех физически возможных. К сегодняшнему дню исправление ошибок существенно продвинулось, приближая момент, когда мы сможем создавать достаточно надежные компьютеры, способные противостоять эффектам декогеренции. С другой стороны, создание квантового оборудования пока остается только возникающей отраслью; но работа, проделанная на сегодня, убеждает нас, что создание достаточно больших машин, способных выполнять серьезные алгоритмы, например, алгоритм Шора, всего лишь дело времени. Таким образом, квантовые компьютеры обязательно появятся. По меньшей мере, это будут самые совершенные вычислительные устройства, а современные нам компьютеры устареют. Квантовые вычисления берут свое начало в весьма специфических областях теоретической физики, но их будущее, несомненно, окажет огромное воздействие на жизнь всего человечества.

**Список литературы**

1. Квантовые вычисления: за и против. Под ред. В.А. Садовничего. – Ижевск: Издательский дом «Удмуртский университет», 1999. – 212 с.

2. Белонучкин В.E., Заикин Д.А., Ципенюк Ю.М., Основы физики. Курс общей физики: Учебн. В 2 т. Т. 2. Квантовая и статистическая физика. – М.: ФИЗМАТЛИТ, 2001. – 504 с.

3. Валиев К.А. «Квантовые компьютеры: можно ли их сделать «большими»?», Успехи физических наук, т. 169, № 6, 1999г.

4. Валиев К.А. «Квантовая информатика: компьютеры, связь и криптография», ВЕСТНИК РОССИЙСКОЙ АКАДЕМИИ НАУК, том 70, № 8, с. 688-695, 2000г.

5. Маслов. Д. «Квантовые вычисления и коммуникация: реальность и перспективы», Компьютерра, №46 , 2004г.

6. Халфин Л.А. «Квантовый эффект Зенона», Успехи физических наук, т. 160, № 10, 1990г.

### 7. Холево А. «Квантовая информатика: прошлое, настоящее, будущее»,

### В МИРЕ НАУКИ, №7, 2008г.

8. Centre for Quantum Technologies, National University of Singapore www.quantumlah.org