E. RIEFFEL
FX Palo Alto Laboratory, 3400 Hillview Avenue, Palo Alto, CA 94304, USA

W. POLAK
1021 Yorktown Drive, Sunnyvale, CA 94087, USA

ОСНОВЫ КВАНТОВЫХ ВЫЧИСЛЕНИЙ*†

Ричард Фейнман заметил, что определённые квантово-механические процессы нельзя эффективно моделировать на классическом компьютере. Это наблюдение привело к более общему утверждению, что для проведения вычислений квантовые процессы являются более эффективными, чем классические. Данное предположение было подтверждено Питером Шором, который разработал квантовый алгоритм разложения целых чисел на простые множители за полиномиальное время.

В квантовых системах пространство вычислений экспоненциально возрастает с размером системы, что и делает возможным экспоненциальный параллелизм. Данный параллелизм может привести к квантовым алгоритмам, которые экспоненциально быстрее классических. Доступ к результатам квантовых вычислений требует проведения процесса измерения и является непростым. Для всего этого требуются новые нетрадиционные методы программирования.

Цель настоящей работы заключается в том, чтобы помочь тем, кто занимается теорией вычислений, преодолеть барьер, который разделяет квантовые и традиционные классические вычисления. Представляются основные принципы квантовой механики, объясняющие, откуда берётся мощь квантового компьютера и почему её трудно использовать. Описывается квантовая криптография, телепортация и плотное кодирование. Приводятся различные приёмы эффективного использования квантового параллелизма. В завершение рассматривается исправление квантовых ошибок.

1. Введение

В начале восьмидесятых годов нашего столетия Ричард Фейнман [Feynman 1982] заметил, что определённые квантово-механические операции нельзя в точности переносить на классический компьютер[1]. Это наблюдение натолкнуло на мысль о том, что, возможно, в целом, вычисления могут быть более продуктивными, если они осуществляются при помощи квантовых операций. Однако создание квантовых компьютеров и вычислительных машин, в которых используются подобные квантовые операции, оказалось очень сложным. К тому же многие были не уверены в том, что квантовые эффекты позволят ускорить вычисления. Поэтому данное направление развивалось крайне медленно. Так продолжалось

[1] В 1980 году подобные соображения в более сжатой форме выразил Ю. И. Манин. См. Манин Ю. И., «Вычислимое и невычислимое», М.: Сов. радио, 1980, стр. 15. — *Прим. перев.*

вплоть до 1994 года, когда Питер Шор удивил мир, описав квантовый алгоритм разложения целых чисел на множители за полиномиальное время [Shor 1994; Shor 1997]. Тогда область квантовых вычислений удостоилась должного внимания. Это открытие побудило к действию как экспериментаторов, пытающихся создать квантовые компьютеры, так и теоретиков, пытающихся найти новые квантовые алгоритмы. Дополнительный интерес к этому предмету был вызван изобретением квантового протокола передачи ключа, а также освещением прессой успехов, достигнутых экспериментально в квантовой телепортации и демонстрации трёхкубитового квантового компьютера.

Цель настоящей работы заключается в том, чтобы помочь программистам и другим специалистам, не являющимся экспертами в области квантовых вычислений, преодолеть принципиальные и условные барьеры, отделяющие квантовые вычисления от традиционных, а также познакомить их с этим новым и интересным направлением. Для общества программистов важно понять эти новые веяния, т. к. они могут радикально изменить их мнение о вычислениях, программировании и сложности.

Вообще-то, время, которое необходимо для осуществления определённых вычислений, можно уменьшить, используя параллельные процессоры. Чтобы достичь экспоненциального уменьшения времени, требуется экспоненциально увеличить число процессоров, а, следовательно, и объём физического пространства. Тогда как в квантовой системе для экспоненциального уменьшения времени, требуется лишь линейное увеличение объёма необходимого физического пространства. Это явление связано непосредственно с квантовым параллелизмом [Deutsch and Jozsa 1992].

Существует ещё одна важная особенность. Пока квантовая система выполняет вычисления, доступ к результатам ограничен. Процесс доступа к результатам — есть процесс измерения, который возмущает квантовое состояние, искажая его. Может показаться, что здесь ситуация ещё хуже, чем с классическими вычислениями. Получается, что мы можем только считать результат выполнения одного из параллельных процессов, а поскольку измерение является вероятностным, то мы даже не можем выбирать, результат какого процесса мы получим.

Но за прошедшие несколько лет люди обнаружили нестандартные пути искусного решения задачи измерения, чтобы использовать преимущества квантового параллелизма. Манипуляции подобного рода не имеют аналогов в классической теории и требуют применения нетрадиционных приемов программирования. Один из таких приёмов заключается в управлении квантовым состоянием таким образом, чтобы могло быть считано общее свойство всех результирующих значений, такое как симметричность или период функции. Подобный техника используется в алгоритме разложения на множители Шора. При другом подходе квантовые состояния преобразуются так, чтобы увеличить вероятность считывания интересующего нас результата вычислений. Этот приём используется в поисковом алгоритме Гровера.

В работе в деталях описывается квантовый параллелизм, а также известные на сегодняшний день приёмы, позволяющие использовать его мощь.

В разделе 2, следующим за введением, описываются концепции квантовой механики, необходимые для квантовых вычислений. Этот раздел, конечно, не может содержать всесторонний обзор квантовой механики. Нашей целью является снабжение читателя инструментами в форме математических выкладок и обозначений для работы с квантовой механикой, используемой при квантовых вычислениях. Надеемся, настоящая работа достаточно подготовит читателей, чтобы они могли исследовать теоретические пласты квантовых вычислений.

В разделе 3 даётся определение квантовому биту или кубиту[1]. В отличие от классического бита квантовый бит может находиться в состоянии суперпозиции, содержа как 0, так и 1. Понятия суперпозиции в классической теории нет. Отдельные квантовые биты предполагают интересное применение. Мы опишем использование отдельного квантового бита при защищённом протоколе передачи ключа.

Настоящая сила квантовых вычислений проистекает из экспоненциальности пространства состояний множества квантовых битов: так, отдельный кубит может быть в суперпозиции 0 и 1, в то время как регистр из n кубитов может быть в суперпозиции 2^n значений. «Сверх» состояния, не имеющие аналога в классической теории и ведущие к экспоненциальной размерности пространства квантового состояния, являются запутанными состояния, подобно состоянию, приводящему к парадоксу ЭПР[2].

Мы рассмотрим два вида операций, происходящих в квантовой системе: измерение и преобразование квантового состояния. Большинство квантовых алгоритмов включает последовательные преобразования квантового состояния, за которыми следует измерение. Для стандартных компьютеров существует набор вентилей, которые являются универсальными в том смысле, что любое классическое вычисление может быть выполнено при использовании набора этих вентилей. Подобным же образом существуют наборы простейших преобразований квантового состояния, называемых квантовыми вентилями, которые универсальны для квантовых вычислений. Имея достаточное количество квантовых битов, можно сконструировать универсальную квантовую машину Тьюринга.

Квантовая физика накладывает ограничения на типы преобразований, которые можно выполнить. В частности, все преобразования квантового состояния, а, следовательно, все квантовые вентили и вычисления, должны быть обратимыми. Любой классический алгоритм можно сделать обратимым и выполнить на квантовом компьютере за приемлемое время. Некоторые общие квантовые вентили определены в разделе 4.

Два способа применения, объединяющих квантовые вентили и запутанные состояния, описываются в подразделе 4.2: телепортация и плотное кодирование. Телепортация — это передача квантового состояния из одного места в другое по классическим каналам. Такая телепортация весьма удивительна, т. к. из квантовой механики нам известно, что невозможно клонировать квантовые состояния или даже измерить их без их возмущения. Таким образом, совершенно не ясно, какую информацию надо послать по классическим каналам, чтобы она, воз-

[1] От англ. quantum bit — qubit. — *Прим. перев.*

[2] ЭПР (EPR) — Эйнштейн, Подольский, Розен.

можно, смогла бы реконструировать неизвестное квантовое состояние на другом конце. При плотном кодировании, в отличие от телепортации, для переноса двух битов классической информации используется один квантовый бит. Как телепортация, так и плотное кодирование, зависят в некоторой степени от запутанных состояний, описываемых в эксперименте ЭПР.

И только в 5 разделе мы увидим, откуда берётся то экспоненциальное ускорение квантовых компьютеров в сравнении с классическими. На вход квантового вычислителя может быть подана суперпозиция, которая включает все возможные входные значения. Выполнение вычислений в этом начальном положении будет иметь результатом суперпозицию соответствующих выходных значений. Таким образом, за одно и то же время на классическом компьютере ведется вычисление выходных значений для единичного входного значения, а на квантовом одновременно вычисляются выходные значения для всех входных значений. Такой процесс известен как квантовый параллелизм. Измерением выходных состояний можно случайно определить только одно из значений в суперпозиции, и в то же время стереть все остальные результаты вычислений. В разделе 5 такая ситуация описывается подробно. В разделах 6 и 7 описываются методы извлечения преимуществ из квантового параллелизма при строгих ограничениях, которые накладывает квантовая механика на то, что может быть измерено.

В разделе 6 описывается подробно алгоритм Шора — алгоритм разложения натурального числа на простые множители за полиномиальное время. Самый быстрый из известных классический алгоритм разложения требует экспоненциального времени. В общем, считается (хотя это строго не доказано), что классического алгоритма разложения на множители за полиномиальное время не существует. В алгоритме Шора квантовый параллелизм используется благодаря применению квантового аналога преобразования Фурье.

Лов Гровер разработал алгоритм поиска в неупорядоченном списке из n элементов за $O\left(\sqrt{n}\right)$ элементарных операций на квантовом компьютере. Классические компьютеры работают заведомо не лучше $O(n)$, поэтому поиск в неупорядоченном списке на квантовом компьютере очевидно эффективней, чем тот же поиск на классическом компьютере. Но всё же ускорение здесь является полиномиальным, а не экспоненциальным, в отличие от алгоритма Шора. Было доказано, что алгоритм Гровера является самым быстрым алгоритмом поиска в неупорядоченном списке для квантовых компьютеров. Но если речь идет о хоть сколько нибудь упорядоченном списке, то алгоритмы, которые извлекают некоторую пользу из упорядоченности, могут работать быстрее. Тед Хогг, наряду с другими учёными, исследовал такую возможность. В разделе 7 мы опишем различные квантовые приёмы поиска.

До сих пор пока неизвестно, можно ли использовать мощность квантового параллелизма для широкого круга задач. Один из основных вопросов — могут ли квантовые компьютеры решать NP-полные задачи за полиномиальное время — остаётся открытым.

Но, пожалуй, самым важным вопросом остаётся создание квантового компьютера. Существует большое множество предложений по созданию такого ком-

пьютера с использованием ионных ловушек, ядерного магнитного резонанса (ЯМР), оптики и твёрдого тела. Все текущие предложения сводятся к решению проблемы увеличения числа кубитов. Необходим качественно новый уровень вычислений, чтобы обрабатывать не десятки, а сотни кубитов информации.

На сегодняшний день технологии с использованием ЯМР и ионных ловушек являются наиболее разрабатываемыми, однако использование оптики и твёрдого тела также подаёт надежды.

В квантовых компьютерах с ионной ловушкой [Cirak and Zoller 1995; Stean 1996] линейная последовательность ионов, представляющих кубиты, ограничена электрическим полем. Для того, чтобы произвести однокубитовые квантовые операции, лазеры направляются на отдельные ионы. Двухкубитовые операции осуществляются при использовании лазера, направленного на отдельный кубит для создания колебания, которое распространяется по цепи ионов до второго кубита, где другой лазер останавливает движение и завершает двухкубитовую операцию. При данном методе требуется, чтобы ионы находились в предельно чистом вакууме при максимально низких температурах.

Преимущество метода использования ЯМР заключается в том, что его можно применять при комнатной температуре. Тем более, что технология ЯМР в целом уже добилась некоторого успеха. Суть метода в том, чтобы использовать макроскопическое количество материи и закодировать квантовый бит в среднем состоянии спина большего количества ядер. Состояниями спина можно управлять посредством магнитных полей, а среднее состояние спина можно измерить при помощи техники ЯМР. Основная проблема при использовании этого метода заключается в трудностях при увеличении квантового регистра. Мощность измеряемого сигнала падает как $\frac{1}{2^n}$, где n — число кубитов. Однако, недавнее предложение [Schulman and Vazirani (1998)] вероятно сможет разрешить эту проблему. Не так давно было успешно завершено создание трёхкубитового ЯМР компьютера [Cory et al. 1998; Vandersypen et al. 1999; Gershenfeld and Chuang 1997; Laflamme et al. 1997]. В данной работе вопросы, связанные с физическими и инженерными задачами создания квантового компьютера, рассматриваться не будут.

Основной проблемой при создании квантового компьютера является отсутствие когерентности и разрушение квантового состояния из-за взаимодействия с окружающей средой. Некоторое время существовали опасения, что квантовый компьютер нельзя будет создать, т. к. изолировать его от внешней среды не представляется возможным. Решение этой проблемы пришло скорее с алгоритмической, чем с физической стороны: были придуманы приёмы квантовой коррекции ошибок. Сначала учёные думали, что квантовая коррекция ошибок будет неосуществима из-за невозможности надёжного копирования неизвестных квантовых состояний. Но, оказывается, вполне возможно разработать коды, которые обнаруживают определённые виды ошибок и в состоянии восстановить когерентное квантовое состояние. Квантовая коррекция ошибок будет рассмотрена в разделе 8.

В приложении даются основные определения тензорных произведений и непрерывных дробей.

2. Квантовая механика

Явления квантовой механики достаточно трудно понять, поскольку они абсолютно не соответствуют законам и представлениям макроскопического мира. И данная работа, к сожалению, не может дать глубокого понимания квантовой механики (за дополнительной информацией по квантовой механике обращайтесь: [Feynman et al. 1965; Liboff 1997; Greenstein and Zajonc]). Вместо этого мы будем излагать материал, используя квантовую механику и математический формализм лишь в объёме, необходимом для работы с квантовыми вычислениями.

С математической точки зрения, квантовая механика — это теория, определяемая некоторым набором аксиом. Следствия этих аксиом описывают поведение квантовых систем. Квантовая механика приводит к некоторым парадоксам: может показаться, что в эффекте Комптона последствие предшествует причине, а в эксперименте ЭПР взаимодействие распространяется быстрее, чем скорость света (эксперимент ЭПР будет детально рассмотрен в 3.4).

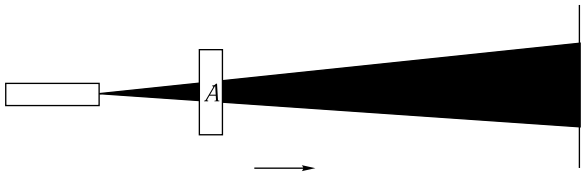
Начнём с простого эксперимента, который может быть осуществлён при помощи легко доступного оборудования и который продемонстрирует некоторые ключевые аспекты квантовой механики, необходимые для квантовых вычислений.

2.1. Поляризация фотона

Фотоны — единственные частицы, которые мы можем видеть непосредственно. Для нашего эксперимента потребуется минимальный набор оборудования: источник яркого света, например, лазерная указка, и три поляроида (поляризационных фильтра), которые можно купить в любом оптическом магазине. Наблюдая в эксперименте фотоны и их поляризацию мы продемонстрируем важные явления квантовой механики.

2.1.1. Эксперимент. Луч света направлен на отражающий экран. Фильтр A поляризован горизонтально, B — под углом 45°, C — вертикально. (Фильтры располагаются таким образом, что луч света их пересекает).

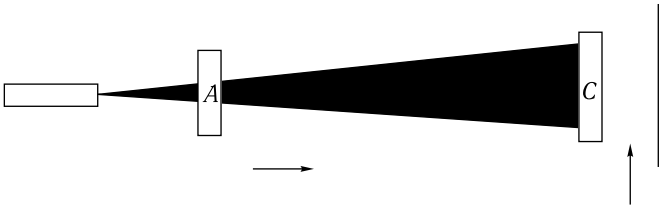
Сначала установим фильтр A. Будем считать, что входящий свет поляризован случайным образом. Интенсивность выходящего света будет равна половине интенсивности входящего. Все выходящие фотоны поляризованы горизонтально.



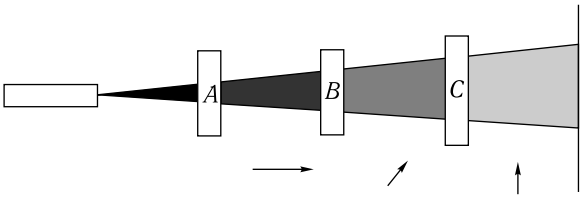
Функцию фильтра A нельзя рассматривать как «сито», которое пропускает только горизонтально поляризованные фотоны. Если бы это было так, то лишь

малая часть случайно поляризованных входящих фотонов была бы горизонтально поляризована, и свет ослаблялся бы гораздо сильнее при прохождении через фильтр.

Далее установив фильтр C, мы видим, что интенсивность выходящих фотонов снижается до нуля, т.е. ни один из горизонтально поляризованных фотонов не может пройти через вертикальный фильтр. (Модель «сита» такое поведение фотонов объяснить ещё может).



Установим теперь фильтр B между A и C. При этом мы столкнемся с удивительным фактом: интенсивность света на экране перестанет быть нулевой. (Она будет равна одной восьмой от первоначальной интенсивности).



Мы наблюдаем непредсказуемое явление. Исходя из классической точки зрения, добавление фильтра должно снизить количество проходящих фотонов. Как же это количество увеличилось?

2.1.2. Разъяснение. Состояние поляризованного фотона может быть задано единичным вектором, имеющим определённое направление. Любая произвольная поляризация может быть выражена как линейная комбинация $a|\uparrow\rangle + b|\rightarrow\rangle$ двух базисных векторов[1] $|\rightarrow\rangle$ (горизонтальная поляризация) и $|\uparrow\rangle$ (вертикальная поляризация).

Поскольку нас интересует только направление поляризации (величина вектора не важна), то вектор состояния будем считать единичным вектором, т.е. $|a|^2 + |b|^2 = 1$. В общем случае поляризация фотона может быть выражена как $a|\uparrow\rangle + b|\rightarrow\rangle$, где a и b — комплексные числа[2], такие что $|a|^2 + |b|^2 = 1$. Замечание: выбор базиса для данного случая абсолютно произвольный — можно использовать любые два ортогональных единичных вектора (напр., $\{|\nwarrow\rangle|\nearrow\rangle\}$).

[1] Обозначение $|\rightarrow\rangle$ будет разъяснено в разделе 2.2.

[2] Мнимые коэффициенты соответствуют круговой поляризации. (Точнее, при круговой поляризации отношение данных коэффициентов мнимое. — *Прим. перев.*)

Постулат измерения в квантовой механике утверждает, что любое устройство, измеряющее двумерную систему, обладает связанным ортогональным базисом, по отношению к которому производится квантовое измерение. Измерение состояния преобразует его в один из связанных базисных векторов измеряющего устройства. Вероятность того, что состояние измерено как базисный вектор $|u\rangle$, равна квадрату нормы проекции первоначального состояния на базисный вектор $|u\rangle$. Например, пусть нам дано устройство для измерения поляризации фотонов со связанным базисом $\{|\uparrow\rangle, |\rightarrow\rangle\}$, тогда состояние $\Psi = a|\uparrow\rangle + b|\rightarrow\rangle$ измеряется как $|\uparrow\rangle$ с вероятностью $|a|^2$, и как $|\rightarrow\rangle$ с вероятностью $|b|^2$ (см. рис. 1). Различные измеряющие устройства имеют различные связанные базисы, поэтому результаты измерений, проведенных разными устройствами, в общем случае не совпадают. Поскольку измерения всегда проводятся по отношению к ортонормированному базису, в оставшейся части статьи все базисы будут считаться ортонормированными.

Важно отметить, что измерение переводит квантовое состояние в то состояние, которое получилось в результате измерения, то есть, если измерение $\Psi = a|\uparrow\rangle + b|\rightarrow\rangle$ имеет результатом $|\uparrow\rangle$, то состояние Ψ переходит в $|\uparrow\rangle$, и второе измерение, по отношению к тому же базису, будет иметь результатом $|\uparrow\rangle$ с вероятностью 1. Таким образом, до тех пор, пока первоначальное состояние не стало одним из базисных векторов измеряющего устройства, процесс измерения будет изменять состояние. После измерения уже невозможно определить, каким было первоначальное состояние.

С точки зрения квантовой механики эксперимент с поляризацией можно объяснить следующим образом. Поляроид измеряет квантовое состояние фотонов по отношению к базису, содержащему вектор поляризации самого поляроида, и вектор, перпендикулярный вектору поляризации поляроида. Фотоны, прошедшие сквозь фильтр имеют ту же поляризацию, что и сам фильтр, тогда как отражённые фотоны обладают поляризацией, перпендикулярной поляризации фильтра. Например, фильтр A измеряет поляризацию фотона по отношению к базисному вектору $|\rightarrow\rangle$. Все фотоны прошедшие через фильтр A обладают $|\rightarrow\rangle$ поляризацией. Те фотоны, которые отражаются, имеют $|\uparrow\rangle$ поляризацию.

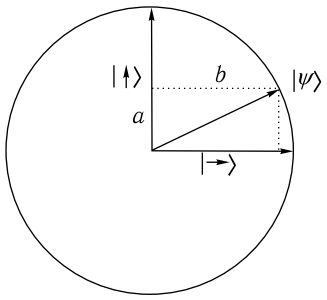


Рис. 1. Измерение является проекцией на базисные векторы

Если учесть то, что источник света испускает фотоны с произвольной поляризацией, фильтр A будет пропускать 50% фотонов. Состояние прошедших фотонов будет $|\rightarrow\rangle$. Фильтр C будет измерять фотоны в по отношению к $|\uparrow\rangle$. Но состояние $|\rightarrow\rangle = 0|\uparrow\rangle + 1|\rightarrow\rangle$ будет проектироваться на $|\uparrow\rangle$ с вероятностью 0, и поэтому ни один фотон не пройдёт фильтр C.

Наконец, фильтр B измеряет квантовое состояние по отношению к базису

$$\left\{\frac{1}{\sqrt{2}}(|\uparrow\rangle + |\rightarrow\rangle), \frac{1}{\sqrt{2}}(|\uparrow\rangle - |\rightarrow\rangle)\right\},$$

который мы запишем как $\{|\nearrow\rangle, |\nwarrow\rangle\}$. Отметим, что $|\rightarrow\rangle = \frac{1}{\sqrt{2}}(|\nearrow\rangle - |\nwarrow\rangle)$ и $|\uparrow\rangle = \frac{1}{\sqrt{2}}(|\nearrow\rangle + |\nwarrow\rangle)$. Фотоны, которые измеряются как $|\nearrow\rangle$, проходят через этот фильтр. Фотоны, проходящие A с состоянием $|\rightarrow\rangle$, будут измерены фильтром B как $|\nearrow\rangle$ с вероятностью $\frac{1}{2}$ и, следовательно, 50% фотонов, проходящих через A, пройдут через B и будут находиться в состоянии $|\nearrow\rangle$. Соответственно, эти фотоны будут измерены фильтром C как $|\uparrow\rangle$ с вероятностью $\frac{1}{2}$. Таким образом, только одна восьмая часть первоначальных фотонов способна пройти через последовательно расположенные фильтры A, B и C.

2.2. Пространство состояний и бра/кет обозначения

Пространство состояний квантовой системы, состоящее из координат, моментов, поляризаций, спинов и т. д. различных частиц, есть гильбертово пространство волновых функций. Вдаваться в подробности свойств этих волновых функций мы не будем. Для квантовых вычислений нам понадобятся только конечномерные квантовые системы, и для этого будет достаточно рассмотрения комплексных векторных пространств со скалярным произведением.

Состояния квантовой системы и их преобразования можно описать посредством векторов и матриц или используя более компактные бра/кет обозначения, введённые Дираком [Dirac 1958]. Кет-векторами $|x\rangle$ обозначают вектор-столбцы и обычно используют для описания квантовых состояний. Парными бра-векторами $\langle a|$ обозначают сопряжение и транспонирование кет-векторов $|x\rangle$. Ортонормированный базис $\{|0\rangle, |1\rangle\}$ обычно записывают как $\{(1, 0)^T, (0, 1)^T\}$. Любую комплексную линейную комбинацию $|0\rangle$ и $|1\rangle$: $a|0\rangle + b|1\rangle$ можно записать, как $(a, b)^T$. В принципе, выбрать порядок базисных векторов можно произвольно. Например, можно использовать запись $|0\rangle$ как $(0, 1)^T$ и $|1\rangle$ как $(1, 0)^T$, и всегда придерживаться её.

Комбинация $\langle x|y\rangle$ обозначает внутреннее (скалярное) произведение двух векторов. Например, $|0\rangle$ — единичный вектор, и $\langle 0|0\rangle = 1$. Векторы $|0\rangle$ и $|1\rangle$ ортогональны и $\langle 0|1\rangle = 0$.

Комбинация $|x\rangle\langle y|$ — внешнее произведение $|x\rangle$ и $\langle y|$.

Например, $|0\rangle\langle 1|$ есть преобразование, которое преобразует $|1\rangle$ в $|0\rangle$ и $|0\rangle$ в $(0, 0)^T$, т. к.

$$|0\rangle\langle 1||1\rangle = |0\rangle\langle 1|1\rangle = |0\rangle$$
$$|0\rangle\langle 1||0\rangle = |0\rangle\langle 1|0\rangle = 0|0\rangle = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Используя равенства $|0\rangle = (1, 0)^T, \langle 0| = (1, 0), |1\rangle = (0, 1)^T$ и $\langle 1| = (0, 1)$ $|0\rangle\langle 1|$ можно записать эквивалентно в виде матрицы

$$|0\rangle\langle 1| = \begin{pmatrix} 1 \\ 0 \end{pmatrix}(0, 1) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Эти обозначения предоставляют нам удобный способ классификации преобразований квантовых состояний по тому, что происходит с базисными векторами (см. раздел 4). Например, преобразование, меняющее местами $|0\rangle$ и $|1\rangle$, задаётся матрицей

$$X = |0\rangle\langle 1| + |1\rangle\langle 0|.$$

Однако в этой статье предпочтение отдается более интуитивной форме

$$\begin{aligned} X\colon |0\rangle &\to |1\rangle \\ |1\rangle &\to |0\rangle, \end{aligned}$$

которая явно задаёт результат преобразования базисных векторов.

3. Квантовые биты

Квантовый бит или кубит — это вектор единичной длины в 2-мерном комплексном векторном пространстве, в котором зафиксирован некоторый базис $\{|0\rangle, |1\rangle\}$. Ортонормированный базис $|0\rangle$ и $|1\rangle$ может соответствовать $|\uparrow\rangle$ и $|\rightarrow\rangle$ или $|\nearrow\rangle$ и $|\nwarrow\rangle$ поляризациям фотона или состояниям «спин вверх», «спин вниз» электрона. Когда речь идёт о кубитах и квантовых вычислениях вообще, базис $\{|0\rangle, |1\rangle\}$, для которого проводятся все рассуждения, выбирается заранее. Мы будем далее считать, если особо не оговорено обратное, что этот базис одновременно является базисом измерения.

В квантовых вычислениях базисные состояния обозначаются $|0\rangle$ и $|1\rangle$, чтобы «соответствовать» значениям классического бита 0 и 1. Но, в отличие от классического бита, кубиты могут находиться в суперпозиции $|0\rangle$ и $|1\rangle$, например, $a|0\rangle + b|1\rangle$, где a и b — комплексные числа, такие что $|a|^2 + |b|^2 = 1$. В случае с поляризацией фотона, если такая суперпозиция измеряется в базисе $\{|0\rangle, |1\rangle\}$, то вероятность того, что измерение даст $|0\rangle$ равна $|a|^2$, а вероятность того, что измерение даст $|1\rangle$ — $|b|^2$.

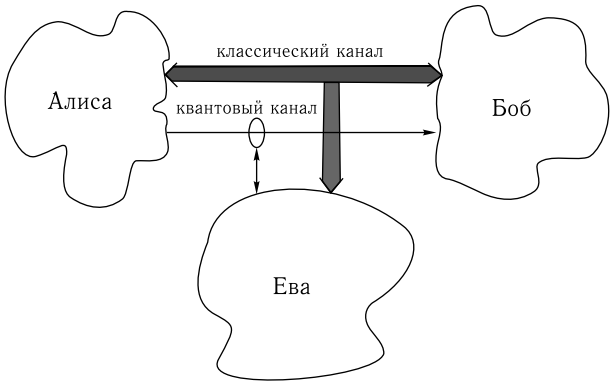
Хотя квантовый бит может находиться в бесчисленном множестве суперпозиций состояний, путём измерения из него можно извлечь только один бит классической информации. Измерение кубита заменяет его состояние на базисное, что мы и наблюдали в эксперименте с поляризацией фотонов. Так как каждое измерение приводит только к одному из двух состояний, т. е. к одному из базисных векторов измерительного устройства, то, как и в классической теории, есть только два возможных исхода. Измерение меняет состояние, поэтому очевидно, что состояние не может быть измерено по двум различным базисам. Более того, как мы увидим в подразделе 4.1.2, квантовые состояния нельзя клонировать, т.е. кубит невозможно измерить двумя способами даже косвенно, например, скопировав кубит и измеряя его копию по базисам, отличным от первоначального.

3.1. Квантовый протокол передачи ключа

Передачу последовательности отдельных кубитов можно использовать для передачи секретного ключа. В 1984 Беннетт и Брассард описали первую кванто-

вую схему протокола передачи ключа [Bennett and Brassard 1987; Bennett et al. 1992]. Обычно, для протокола передачи ключа используется процедура шифрования с открытым ключом, например, RSA.

Рассмотрим ситуацию, в которой Алиса и Боб хотят договориться использовать при переговорах секретный ключ. Связь осуществляется по обычному двустороннему каналу и одностороннему квантовому каналу. Эти оба канала прослушиваются Евой, которая хочет подслушать их разговор. Ситуация изображена на рисунке ниже.



Квантовый канал позволяет Алисе посылать Бобу отдельные частицы (например, фотоны) к Бобу, который может измерить их состояние. Ева также может попытаться измерить состояния этих частиц и переслать их Бобу.

Для того, чтобы начать процесс передачи секретного ключа Алиса посылает Бобу последовательность битов, кодируя каждый бит в квантовом состоянии фотона следующим образом: для кодировки каждого бита она произвольно использует один из базисов

$$0 \to |\uparrow\rangle$$
$$1 \to |\rightarrow\rangle$$

или

$$0 \to |\nwarrow\rangle$$
$$1 \to |\nearrow\rangle.$$

Боб измеряет состояния фотонов, выбрав также случайным образом один из этих базисов. После того как биты переданы, Боб и Алиса сообщают друг другу по открытому каналу, какие базисы они использовали для кодирования (раскодирования) битов при передаче (приёме) фотонов. Обладая такой информацией, они могут определять, какие из битов переданы правильно, т. е. биты, для которых согласованы базисы передачи и приёма. Эти биты они будут использовать в качестве ключа, все остальные будут отброшены. В среднем Алиса и Боб будут иметь примерно 50% совпадений базисов, т. е. для ключа будет использована примерно половина передаваемых битов.

Теперь предположим, что Ева измеряет состояния фотонов, передаваемых Алисой, и пересылает Бобу новые фотоны с этими же состояниями. Примерно в половине случаев она будет использовать ложные базисы. Поэтому, когда Боб измеряет переданный кубит в правильном базисе, вероятность того, что он получит неправильное значение, равна 25%. Таким образом, всякое подслушивание в квантовом канале увеличивает число ошибок передачи, что легко может быть обнаружено Алисой и Бобом, если они сравнят по открытому каналу некоторое количество контрольных битов ключа.

Итак, очевидно, не только то, что 25% ключа у Евы не верно, но и то, что Алисе и Бобу становится ясно, что кто-то их подслушивает.

Предлагались и другие приёмы использования квантовых операций для передачи ключа. Например, приёмы, предложенные Экертом [Ekert et al. 1992], Беннеттом [Bennett 1992], Лу и Чо [Lo and Chau 1999]. Но ни один из предложенных квантовых протоколов передачи ключа пока не может быть заменой шифрованию с открытым ключом. Кроме описанного выше метода прослушивания, возможны и другие аттаки. Вопросы защиты от всех подобных атак освещаются в работах Мейерса [Mayers 1998] и Лу и Чо [Lo and Chau 1999].

Квантовый протокол передачи ключа был апробирован на расстоянии 24 км с использованием стандартных оптоволоконных кабелей [Hughes et al. 1997] и на расстоянии 0.5 км при передаче по воздуху [Hughes et al. 1999].

3.2. Множества кубитов

Представим себе физический макроскопический объект, который разламывается на n частей, разлетающихся в разных направлениях. Состояние такой системы можно описать полностью, описав состояние каждой составляющей её части в отдельности. Для квантовой же системы из n частиц, имеет место удивительное и интуитивно неочевидное свойство, которое заключается в том, что для полного описания состояния такой системы, в общем случае недостаточно описать состояния составляющих её отдельных частиц. Исследование подобных систем, а именно систем с более чем одним кубитом даёт нам возможность понять, откуда берётся вычислительная мощность квантовых компьютеров.

Как мы уже убедились, состояния кубита можно представить вектором в двумерном комплексном векторном пространстве, порождённом $|0\rangle$ и $|1\rangle$. В классической физике возможные состояния системы из n частиц, в которой состояние каждой частицы задается вектором в 2-мерном пространстве, образуют $2n$-мерное векторное пространство. Однако, в квантовой системе общее пространство состояний[1] гораздо больше: система из n кубитов имеет пространство состояний размерности 2^n. Именно этот экспоненциальный рост пространства состояний в зависимости от числа частиц даёт экспоненциальное преимущество в скорости вычислений на квантовых компьютерах в сравнении с классическими.

[1] Далее будет показано, что пространство состояний n кубитов — это множество векторов в 2^n-мерном пространстве, нормированных так же, как и состояние одного кубита $a|0\rangle + b|1\rangle$, нормированное равенством $|a|^2 + |b|^2 = 1$.

В классической системе из n частиц, пространства состояний каждой частицы соединяются декартовым произведением. Квантовые же состояния соединяются тензорным произведением. Свойства тензорных произведений и их выражение через векторы и матрицы подробно даются в приложении A. Давайте коротко рассмотрим различия между декартовым и тензорным произведениями, которые являются ключевыми для понимания квантовых вычислений.

Пусть V и W — 2-мерные комплексные векторные пространства с базисами $\{v_1, v_2\}$ и $\{w_1, w_2\}$ соответственно. Их декартово произведение будет иметь базис $\{v_1, v_2, w_1, w_2\}$. Порядок выбора элементов этого базиса произволен[1]. В частности, размер пространства состояний множества классических частиц линейно возрастает с увеличением частиц, т. к. $\dim(X \times Y) = \dim(X) + \dim(Y)$. Тензорное же произведение V и W имеет базис $\{v_1 \otimes w_1, v_1 \otimes w_2, v_2 \otimes w_1, v_2 \otimes w_2\}$. Для тензорного произведения порядок выбора элементов базиса в общем случае не произволен. (Это станет очевидно, когда мы будем рассматривать тензорные произведения матриц).

Итак, пространство состояний двух кубитов, у каждого из которых базис $\{|0\rangle, |1\rangle\}$, имеет базис $\{|0\rangle\otimes|0\rangle, |0\rangle\otimes|1\rangle, |1\rangle\otimes|0\rangle, |1\rangle\otimes|1\rangle\}$, или в более краткой форме $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. В более общем случае мы будем писать $|x\rangle$, подразумевая $|b_n b_{n-1} \ldots b_0\rangle$, где b_i — двоичные цифры числа x. Базисом трёхкубитовой системы будет

$$\{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\},$$

В общем случае, система n кубитов имеет 2^n базисных векторов. Теперь мы видим экспоненциальный рост пространства квантовых состояний по мере увеличения числа частиц. Тензорное произведение $X \otimes Y$ имеет размерность $\dim(X) \times \dim(Y)$.

Состояние $|00\rangle+|11\rangle$ является примером квантового состояния, которое нельзя представить состояниями отдельных кубитов. Другими словами, мы не можем найти такие a_1, a_2, b_1, b_2, что $\big(a_1|0\rangle + b_1|1\rangle\big) \otimes \big(a_2|0\rangle + b_2|1\rangle\big) = |00\rangle + |11\rangle$, т. к.

$$\big(a_1|0\rangle + b_1|1\rangle\big) \otimes \big(a_2|0\rangle + b_2|1\rangle\big) = a_1a_2|00\rangle + a_1b_2|01\rangle + b_1a_2|10\rangle + b_1b_2|11\rangle$$

а из $a_1b_2 = 0$ следует, что либо $a_1a_2 = 0$, либо $b_1b_2 = 0$. Состояния, которые не могут разлагаться на составные части подобным образом, называют запутанными состояниями. Эти состояния не имеют классического аналога. Эти же состояния обеспечивают экспоненциальный рост пространства квантовых состояний по мере увеличения частиц.

Следует отметить, что потребуются огромные ресурсы, чтобы смоделировать даже небольшую квантовую систему на классических компьютерах. Эволюция квантовых систем протекает экспоненциально быстрее, чем эволюция их классических моделей. Потенциальная мощь квантовых компьютеров кроется в возможности использовать эволюцию квантового состояния в качестве вычислительного механизма.

[1] Порядок элементов базиса будет важен, когда мы будем использовать матричные обозначения для квантовых преобразований.

3.3. Измерение

Эксперимент в подразделе 2.1.2. демонстрирует, каким образом измерение одного кубита проектирует квантовое состояние на одно из базисных состояний, связанных с измеряющим устройством. Результат измерения является вероятностным, а сам процесс измерения заменяет состояние на измеренное.

Рассмотрим, например, процесс измерения в 2-кубитовой системе. Состояния любых двух кубитов можно представить как $a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$, где a, b, c и d комплексные числа, такие, что $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$. Предположим мы хотим измерить первый кубит в стандартным базисе $\{|0\rangle, |1\rangle\}$. Для удобства запишем состояние следующим образом:

$$a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle = |0\rangle \otimes \big(a|0\rangle + b|1\rangle\big) + |1\rangle \otimes \big(c|0\rangle + d|1\rangle\big) =$$
$$= u|0\rangle \oplus \big(a/u|0\rangle + b/u|1\rangle\big) + v|1\rangle \oplus \big(c/v|0\rangle + d/v|1\rangle\big).$$

Так как $u = \sqrt{|a|^2 + |b|^2}$ и $v = \sqrt{|c|^2 + |d|^2}$, то $c/v|0\rangle + d/v|1\rangle$ — векторы единичной длины. Записанное выше состояние есть тензорное произведение измеряемого бита и вектора единичной длины. Легко видеть, какие могут быть результаты после измерения. Измерение первого бита с вероятностью $u^2 = |a|^2 + |b|^2$ даст $|0\rangle$, проектируя состояние, в $|0\rangle \otimes \big(a/u|0\rangle + b/u|1\rangle\big)$, и с вероятностью $v = |c|^2 + |d|^2$ оно даст $|1\rangle$, проектируя состояние в $|1\rangle \otimes \big(c/v|0\rangle + d/v|1\rangle\big)$. Т. к. $|0\rangle \otimes \big(a/u|0\rangle + b/u|1\rangle\big)$ и $|1\rangle \otimes \big(c/v|0\rangle + d/v|1\rangle\big)$ являются единичными векторами, то перенормировка не требуется. Измерение второго кубита производится аналогично.

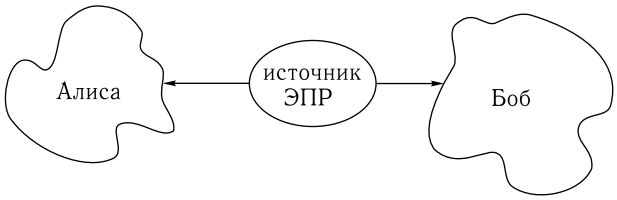
Для квантовых вычислений многобитовое измерение можно рассматривать как ряд однобитовых измерений в стандартном базисе. Возможны и другие виды измерений. Например, можно проверить, являются ли два кубита одинаковыми, не выясняя значений самих кубитов. Но подобные измерения эквивалентны унитарным преобразованиям, за которыми следует стандартное измерение отдельных кубитов, поэтому достаточно рассматривать только стандартные измерения.

В примере с двумя кубитами пространство состояний есть декартово произведение подпространства, состоящего из всех состояний, где первый кубит находится в состоянии $|0\rangle$, и ортогонального подпространства, где первый кубит находится в состоянии $|1\rangle$. Любое квантовое состояние можно представить в виде суммы двух векторов, по одному из каждого подпространства. Измерение k кубитов в стандартном базисе имеет 2^k возможных результатов m_i. Любое устройство, измеряющее k кубитов n-кубитной системы, делит 2^n-мерное пространство состояний $\mathscr{H}$ на декартово произведение ортогональных подпространств $S_1, \ldots, S_{2^k}$, где $\mathscr{H} = S_1 \times \ldots \times S_{2^k}$. В этом произведении значение измеряемых k кубитов есть m_i, а состояние после измерения находится в пространстве S_i для некоторого i. Устройство произвольно выбирает одно из S_i пространств с вероятностью квадрата амплитуды компоненты ψ в S_i. Далее оно проектирует состояние на эту компоненту, нормируя его затем до единичной длины. Другими словами, вероятность того, что результат является заданной величиной, равна сумме квадратов абсолютных величин амплитуд всех базисных векторов, совместимых с этой величиной измерения.

Измерения заставляют нас взглянуть на запутанные частицы с другой стороны. Частицы не являются запутанными, если измерение одной не влияет на другую. Например, состояние $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ запутанное, т. к. вероятность того, что после измерения первый бит станет $|0\rangle$ ровно $1/2$, при условии, что второй бит не измерялся. Однако если второй бит был измерен, то вероятность измерения первого бита как $|0\rangle$ равна 1 или 0, в зависимости от того, каким образом был измерен второй бит: как $|0\rangle$ или $|1\rangle$ соответственно. Следовательно, вероятный результат измерения первого бита изменяется под влиянием измерения второго бита. С другой стороны, состояние $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$ не является запутанным, т. к. $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) = |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. А любое измерение первого бита даст $|0\rangle$ независимо от того, был ли измерен второй бит или нет. Аналогичным образом, второй бит имеет равные шансы быть измеренным как $|0\rangle$, невзирая на то, был ли измерен первый бит или нет. Отметим, что определение запутанности, как влияния измерения одной частицы на результаты измерения другой, аналогично нашему предыдущему определению запутанных состояний, как состояний, которые нельзя записать в виде тензорного произведения состояний отдельных частиц.

3.4. Парадокс ЭПР

Эйнштейн, Подольский и Розен предложили провести теоретический «эксперимент», в котором запутанные частицы используются так, что создаётся впечатление, будто этот эксперимент противоречит фундаментальным основам теории относительности. Давайте представим себе, что существует источник, вырабатывающий две максимально запутанные частицы $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$, называемые ЭПР парой, и отсылает по одной из них Алисе и Бобу.



Алиса и Боб находятся на произвольном расстоянии друг от друга. Предположим, Алиса измеряет свою частицу и обнаруживает состояние $|0\rangle$. Это означает, что общее состояние теперь будет $|00\rangle$. А если Боб измерит свою частицу, то он также обнаружит $|0\rangle$. Аналогичным образом, если Алиса измерит $|1\rangle$, то и у Боба будет тот же результат. Заметим, что изменение общего квантового состояния происходит мгновенно, несмотря на то, что две частицы произвольно удалены друг от друга. Получается, что это позволяет Алисе и Бобу передавать друг другу сигналы, которые распространяются быстрее скорости света. Дальнейший

анализ покажет, что несмотря на то, что между двумя частицами существует связь, Алиса и Боб всё же не могут использовать этот механизм для передачи информации.

Существует два некорректных подхода, которые учёные всё ещё применяют для описания запутанных состояний и их измерения. У каждого есть свои плюсы, но оба они не верны и могут привести к недоразумениям. Давайте по очереди рассмотрим их.

Эйнштейн, Подольский и Розен предположили, что каждая частица обладает неким внутренним состоянием, которое полностью определяет, какой будет результат любого измерения. Это состояние временно от нас скрыто, и поэтому всё, что мы можем сделать в данный момент, это дать вероятностные прогнозы. Эта теория известна нам как теория скрытых переменных. Простейшая теория скрытых переменных для ЭПР пары заключается в том, что обе частицы находятся либо в состоянии $|0\rangle$, либо $|1\rangle$; мы просто не знаем, в каком из них. В такой теории для того, чтобы объяснять скореллированность измерений, связь между удалёнными частицами не нужна. С такой точки зрения, конечно, нельзя объяснить результаты измерений в различных базисах. Белл показал, что любая теория скрытых переменных предсказывает, что измерения будут удовлетворять некоторому неравенству, известному как неравенство Белла. Однако, результаты экспериментов показали, что неравенство Белла неверно. Таким образом, квантовую механику нельзя объяснить с помощью теории скрытых переменных. Более точные расчёты по теореме Белла и соответствующие эксперименты вы сможете найти в работе [Greenstein and Zajonc 1997].

Второй способ описания основывается на причине и следствии. Например, ранее было сказано, что измерение, осуществляемое Алисой, влияет на измерение, которое проводит Боб. Тем не менее, эта точка зрения также неверна, и, как считали Эйнштейн, Подольский и Розен, проявляется в глубоких противоречиях с теорией относительности. Можно предложить следующий сценарий ЭПР: один наблюдатель сначала наблюдает измерение Алисы, а затем Боба. В это время второй наблюдатель видит сначала измерение Боба, а потом Алисы. В соответствии с теорией относительности результаты измерений должны быть инвариантны относительно замены наблюдателей, т.е. наблюдения первого и второго наблюдателей должны совпадать. Экспериментальные результаты одинаково хорошо можно объяснить сперва с помощью измерений Боба и причиной изменения в состоянии частицы Алисы, и наоборот. Эта симметрия позволяет сделать вывод, что ни Боб, ни Алиса на самом деле не могут воспользоваться ЭПР парой для передачи сигналов быстрее скорости света. Таким образом разрешается существующий парадокс. Всё, что можно сказать, это то, что Алиса и Боб будут наблюдать одинаковый случайный результат.

В дальнейшем, в разделе, касающегося плотного кодирования и телепортации, мы увидим, что ЭПР пары можно будет использовать для получения некоторых преимуществ при передаче информации, но скорость её распространения всё равно будет меньше скорости света.

4. Квантовые вентили

До сих пор мы рассматривали лишь статические квантовые системы, состояние которых меняется только при измерении. Эволюция же динамических квантовых систем описывается уравнением Шрёдингера. При этом ортогональные состояния системы остаются ортогональными. Линейные преобразования комплексного векторного пространства, которые сохраняют ортогональность, называются унитарными. Любое линейное преобразование в комплексном векторном пространстве можно описать матрицей. Пусть матрица M^* получается из M транспонированием и последующим комплексным сопряжением. Матрица M является унитарной (т.е. описывает унитарное преобразование) тогда и только тогда, когда $MM^* = I$. Любое унитарное преобразование является допустимой эволюцией квантовой системы и наоборот. Унитарные преобразования можно рассматривать просто как повороты комплексного векторного пространства.

Важным следствием того, что квантовые преобразования унитарны, является их обратимость. Т.е. квантовые вентили должны быть обратимыми. Что же касается классических вычислений, то, как показали Беннетт, Фредкин и Тоффоли, они всегда могут быть выполнены обратимо. Более подробно обратимые вычисления и энергетический подход к ним рассмотрены в «Лекциях по вычислениям» Фейнмана [Feynman 1996].

4.1. Простейшие квантовые вентили

Рассмотрим несколько полезных примеров преобразований 1-кубитового квантового состояния. В силу линейности, преобразования полностью определяются их действием на базисные векторы. Соответствующие матрицы преобразований приведены рядом справа.

$$
\begin{array}{lll}
I\colon & |0\rangle \to |0\rangle & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \\
 & |1\rangle \to |1\rangle & \\
X\colon & |0\rangle \to |1\rangle & \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \\
 & |1\rangle \to |0\rangle & \\
Y\colon & |0\rangle \to -|1\rangle & \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \\
 & |1\rangle \to |0\rangle & \\
Z\colon & |0\rangle \to |0\rangle & \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \\
 & |1\rangle \to -|1\rangle &
\end{array}
$$

Обозначения этих преобразований являются общепринятыми. I — тождественное преобразование, X — отрицание, Z — операция сдвига по фазе, а $Y = ZX$ комбинация последних двух. Преобразование X уже рассматривалось в подразделе 2.2. Проверить, что эти вентили унитарны, не составит большого труда. Например,

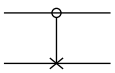
$$
YY^* = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = I.
$$

Вентиль CONTROLLED-NOT или $C_{\rm not}$, действует на два кубита следующим образом: второй кубит изменяет свое значение, если первый равен единице, и остаётся без изменений, если первый равен нулю. Векторы $|00\rangle$, $|01\rangle$, $|10\rangle$ и $|11\rangle$ образуют ортонормированный базис в пространстве состояний двухкубитовой системы – четырёхмерного комплексного векторного пространства. Для того, чтобы представить преобразование этого пространства в матричной форме нам необходимо выбрать изоморфизм между этим пространством и пространством четырёх комплексных орт. Единственная причина, по которой мы предпочитаем один изоморфизм другому, это условное соглашение. Так что наш изоморфизм связывает $|00\rangle$, $|01\rangle$, $|10\rangle$ и $|11\rangle$ со стандартным базисом такого же порядка $(1,\,0,\,0,\,0)^T$, $(0,\,1,\,0,\,0)^T$, $(0,\,0,\,1,\,0)^T$ и $(0,\,0,\,0,\,1)^T$. Тогда преобразование $C_{\rm not}$ имеет представление

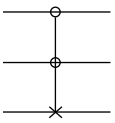
$$\begin{array}{l} |00\rangle \to |00\rangle \\ |01\rangle \to |01\rangle \\ |10\rangle \to |11\rangle \\ |11\rangle \to |10\rangle \end{array} \qquad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Преобразование $C_{\rm not}$ является унитарным, т. к. $C^*_{\rm not} = C_{\rm not}$ и $C_{\rm not}C_{\rm not} = I$. Заметим, что $C_{\rm not}$ нельзя представить, как тензорное произведение двух однобитовых преобразований.

Удобно представлять преобразования квантового состояния графически, особенно в случаях, когда проводится несколько преобразований. Вентиль $C_{\rm not}$ обычно представляют в виде следующей схемы



Незакрашенный кружок обозначает управляющий кубит, а знак $\times$ — условное отрицание подчинённого кубита. Некоторые авторы закрашенным кружком обозначают вентиль с управлением по сигналу 0, то есть переворот управляемого бита, когда управляющий бит находится в состоянии 0. В общем случае, управляющих кубитов может быть несколько. CONTROLLED-CONTROLLED-NOT отрицает последний кубит из трёх, но только в том случае, если оба первых кубита равны единице. Графически его можно представить как показано на рисунке.



Однокубитовые операции графически отображаются с помощью подписанных квадратов, как показано ниже.

4.1.1. Преобразование Уолша – Адамара. Другое важное однобитовое преобразование — это преобразование Адамара, определяемое как

$$H\colon |0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

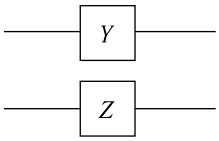
Преобразование H имеет большое число важных применений. Действуя на $|0\rangle$, H создает состояние суперпозиции $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Применяя H к n кубитам по от-

дельности, получим суперпозицию всех 2^n возможных состояний, обозначаемых двоичным представлением чисел от 0 до $2^n - 1$.

$$(H \otimes H \otimes \ldots \otimes H)|00\ldots0\rangle =$$
$$= \frac{1}{\sqrt{2^n}}\big((|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes \ldots \otimes (|0\rangle + |1\rangle)\big) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle.$$

Преобразование W, которое применяет H к всем n кубитам называется преобразованием Уолша – Адамара. Его можно определить рекурсивно

$$W_1 = H, \quad W_{n+1} = H \otimes W_n.$$



4.1.2. Невозможность клонирования. Оказывается, свойство унитарности не позволяет копировать или клонировать квантовые состояния. Представленное здесь доказательство невозможности клонирования впервые было получено Вуттерсом и Зуреком [Wootters and Zurek 1982]. Оно заключается в использовании линейности унитарных преобразований.

Предположим, что U — это клонирующее унитарное преобразование, такое что $U(|a0\rangle) = |aa\rangle$ для всех состояний $|a\rangle$. Пусть $|a\rangle$ и $|b\rangle$ — некоторые ортогональные состояния. $U(|a0\rangle) = |aa\rangle$ и $U(|b0\rangle) = |bb\rangle$. Возьмём состояние $|c\rangle = \frac{1}{\sqrt{2}}(|a\rangle + |b\rangle)$. Тогда, используя свойство линейности, получаем

$$U\big(|c0\rangle\big) = \frac{1}{\sqrt{2}}\big(U(|a0\rangle) + U(|b0\rangle)\big) = \frac{1}{\sqrt{2}}\big(|aa\rangle + |bb\rangle\big).$$

Но т. к. U клонирующее преобразование, то

$$U\big(|c0\rangle\big) = |cc\rangle = \frac{1}{2}\big(|aa\rangle + |ab\rangle + |ba\rangle + |bb\rangle\big),$$

что не равно $\left(\frac{1}{\sqrt{2}}(|aa\rangle + |bb\rangle\right)$. Таким образом, унитарной операции, которая может клонировать неизвестные квантовые состояния, не существует. Совершенно очевидно, что клонирование невозможно и при использовании измерения, т. к. оно является вероятностным и деструктивно для состояний, не являющихся базисными векторами измерительного устройства.

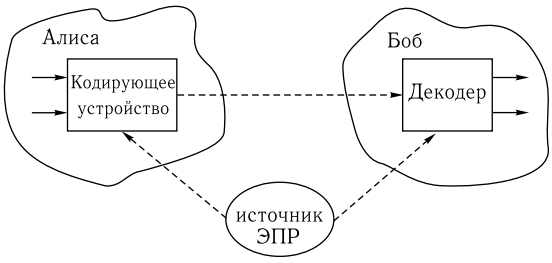
Крайне важно понять, какой вид клонирования допускается, а какой нет. Как мы показали выше, клонировать неизвестное квантовое состояние невозможно. Однако известное квантовое состояние в принципе можно клонировать. Привести n частиц в запутанное состояние $a|00\ldots0\rangle + b|11\ldots1\rangle$ из неизвестных состояний $a|0\rangle + b|1\rangle$ вполне возможно. Каждая из этих частиц будет вести себя одинаково при измерении в стандартном базисе $\{|00\ldots0\rangle, |00\ldots01\rangle, \ldots, |11\ldots1\rangle\}$, чего нельзя было бы сказать, если бы измерения проводились в каком-то другом базисе. Создать состояние n частиц $\big(a|0\rangle + b|1\rangle\big) \otimes \ldots \otimes \big(a|0\rangle + b|1\rangle\big)$ из неизвестных состояний $a|0\rangle + b|1\rangle$ невозможно.

4.2. Примеры

Рассмотрим применение элементарных квантовых вентилей на двух примерах: плотное кодирование и телепортация.

При плотном кодировании для передачи двух классических битов используется ЭПР пара. Так как ЭПР пара может быть распределена заранее, то в дальнейшем для передачи двух битов информации потребуется передать физически всего лишь одну частицу. Это довольно неожиданный факт, поскольку, как отмечалось в разделе 3, из кубита путём измерения можно извлечь только один классический бит полезной информации.

Телепортация — это процесс, противоположный плотному кодированию. Здесь для передачи одного кубита, как вспомогательные, используются два классических бита. Телепортация неожиданна ввиду принципа невозможности клонирования, т. к. она позволяет производить перенос неизвестного квантового состояния.



Ключевым для плотного кодирования и телепортации является использование запутанных состояний. Первоначальная установка одинакова для обоих процессов. Пусть, например, Алиса и Боб хотят передавать друг другу информацию. Каждому посылается одна запутанная частица из ЭПР пары

$$\psi_0 = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big).$$

Предположим, Алисе послали первую частицу, а Бобу — вторую. Итак, пока частицы не пересылаются, только Алиса может совершать преобразование над своей частицей, и только Боб — над своей.

4.2.1. Плотное кодирование. Алиса принимает два классических бита, которые ей нужно передать Бобу, кодируя их числами от 0 до 3. В зависимости от этих чисел Алиса выполняет одно из преобразований $\{I, X, Y, Z\}$ над своим кубитом запутанной пары ψ_0. Преобразование над одним кубитом запутанной пары означает, что над другим кубитом происходит преобразование идентичности. Полученные состояния показаны в таблице:

Значение	Преобразование	Новое состояние
0	$\psi_0 = (I \otimes I)\psi_0$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$
1	$\psi_1 = (X \otimes I)\psi_0$	$\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$
2	$\psi_2 = (Y \otimes I)\psi_0$	$\frac{1}{\sqrt{2}}(-\|10\rangle + \|01\rangle)$
3	$\psi_3 = (Z \otimes I)\psi_0$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$

Затем Алиса отсылает свой кубит Бобу.
Боб применяет CONTROLLED-NOT к запутанной паре.

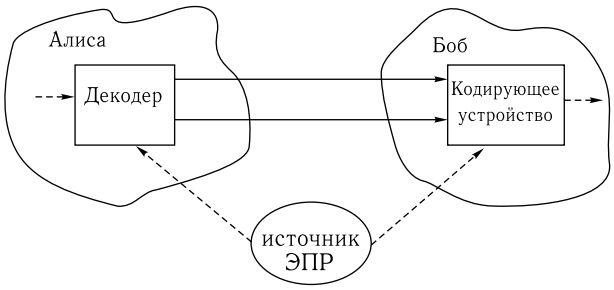
Первоначальное состояние	CONTROLLED-NOT	Первый кубит	Второй кубит
$\psi_0 = \frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|10\rangle)$	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\|0\rangle$
$\psi_1 = \frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$	$\frac{1}{\sqrt{2}}(\|11\rangle + \|01\rangle)$	$\frac{1}{\sqrt{2}}(\|1\rangle + \|0\rangle)$	$\|1\rangle$
$\psi_2 = \frac{1}{\sqrt{2}}(-\|10\rangle + \|01\rangle)$	$\frac{1}{\sqrt{2}}(-\|11\rangle + \|01\rangle)$	$\frac{1}{\sqrt{2}}(-\|1\rangle + \|0\rangle)$	$\|1\rangle$
$\psi_3 = \frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|10\rangle)$	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\|0\rangle$

Отметим, что сейчас Боб может измерить второй кубит, не возмущая квантовое состояние. Если результат измерения $|0\rangle$, то это означает, что закодированным значением было число 0 или 3, если результат $|1\rangle$, то — 1 или 2. Далее Боб применяет вентиль Адамара H к первому кубиту.

Первоначальное состояние	Первый кубит	H (первый кубит)
ψ_0	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\frac{1}{\sqrt{2}}(\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle) + \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)) = \|0\rangle$
ψ_1	$\frac{1}{\sqrt{2}}(\|1\rangle + \|0\rangle)$	$\frac{1}{\sqrt{2}}(\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle) + \frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)) = \|0\rangle$
ψ_2	$\frac{1}{\sqrt{2}}(-\|1\rangle + \|0\rangle)$	$\frac{1}{\sqrt{2}}(-\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle) + \frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)) = \|1\rangle$
ψ_3	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\frac{1}{\sqrt{2}}(\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle) - \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)) = \|1\rangle$

И наконец, измеряет первый кубит, что позволяет ему отличить 0 от 3 или 1 от 2.

4.2.2. Телепортация. Её целью является передача квантового состояния частицы, привлекая классические биты, и точное воссоздание квантового состояния у получателя. Поскольку квантовое состояние нельзя копировать, то у исходной частицы оно обязательно будет разрушено. Телепортацию одного кубита экспериментально осуществили [Bouwmeester et al. 1997; Nielsen et al. 1998; Boschi et al. 1998].



Алиса не знает состояния находящегося у неё кубита. Она хочет послать состояние этого кубита

$$\varphi = a|0\rangle + b|1\rangle$$

Бобу по классическим каналам. Как и при плотном кодировании, у Алисы и Боба есть по одному кубиту запутанной пары

$$\psi_0 = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Алиса применяет декодирующую процедуру плотного кодирования к кубиту, который нужно передать, и к своей частице запутанной пары. Следующим шагом Алиса расшифровывает плотный код передаваемого кубита φ, а также свою половину запутанной пары. Стартовым состоянием является

$$\begin{aligned}\varphi \otimes \psi_0 &= \frac{1}{\sqrt{2}}\big(a|0\rangle \otimes (|00\rangle + |11\rangle) + b|1\rangle \otimes (|00\rangle + |11\rangle)\big) = \\ &= \frac{1}{\sqrt{2}}\big(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle\big),\end{aligned}$$

в котором Алиса управляет первыми двумя кубитами, а Боб — последним. Далее Алиса прикладывает $C_{\text{not}} \otimes I$ и $H \otimes I \otimes I$ к этому состоянию:

$$\begin{aligned}&(H \otimes I \otimes I)(C_{\text{not}} \otimes I)(\varphi \otimes \psi_0) = \\ &= (H \otimes I \otimes I)(C_{\text{not}} \otimes I)\frac{1}{\sqrt{2}}\big(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle\big) = \\ &= (H \otimes I \otimes I)\frac{1}{\sqrt{2}}\big(a|000\rangle + |011\rangle + b|110\rangle + b|101\rangle\big) = \\ &= \frac{1}{2}\big(a(|000\rangle + |011\rangle + |100\rangle + |111\rangle) + b(|010\rangle + |001\rangle - |110\rangle - |101\rangle)\big) = \\ &= \frac{1}{2}\big(|00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(a|1\rangle + b|0\rangle) + |10\rangle(a|0\rangle - b|1\rangle) + |11\rangle(a|1\rangle - b|0\rangle)\big).\end{aligned}$$

Затем Алиса измеряет первые два кубита, получая с равной вероятностью $|00\rangle, |01\rangle, |10\rangle$ или $|11\rangle$. В зависимости от результата измерения квантовое состояние кубита Боба проектируется на $a|0\rangle + b|1\rangle$, $a|1\rangle + b|0\rangle$, $a|0\rangle - b|1\rangle$ или $a|1\rangle - b|0\rangle$

соответственно. Алиса посылает результат своего измерения Бобу в виде двух классических битов.

Отметим, что при измерении Алиса необратимо изменила состояние своего первоначального кубита φ. Именно эта потеря первоначального состояния и является причиной, по которой телепортация не противоречит принципу невозможности клонирования.

Боб, приняв два классических бита от Алисы, знает, как состояние его частицы запутанной пары связано с первоначальным состоянием кубита Алисы

Принятые кубиты	Состояния	Расшифровка
00	$a\|0\rangle + b\|1\rangle$	I
01	$a\|1\rangle + b\|0\rangle$	X
10	$a\|0\rangle - b\|1\rangle$	Z
11	$a\|1\rangle - b\|0\rangle$	Y

Применяя соответствующее преобразование к своей половине запутанной пары, Боб может восстановить изначальное состояние кубита Алисы φ. Заметим, что это есть кодирующий шаг плотного кодирования.

5. Квантовые компьютеры

В настоящем разделе обсуждается, каким квантовая механика может быть использована для проведения вычислений, и в чём состоит качественное отличие квантовых вычислений от вычислений, выполненных на классическом компьютере. Вспомним, что в разделе 4 говорилось о том, что все преобразования квантового состояния обратимы. Классический вентиль NOT (НЕ) тоже является обратимым, тогда как вентили AND (И), OR (ИЛИ) и NAND (2И-НЕ) таковыми не являются. Совсем не очевидно, что с помощью квантовых преобразований можно выполнять классические вычисления. В первом подразделе описываются полные наборы обратимых вентилей, которые могут осуществлять любые классические вычисления на квантовом компьютере. Более того, там же описываются и наборы вентилей, с помощью которых можно выполнять все квантовые вычисления. Во втором подразделе рассказывается о квантовом параллелизме.

5.1. Квантовые схемы

Комплексные унитарные операции удобно записывать с помощью бра- и кэт-обозначений. Для двух произвольных унитарных преобразований U_1 и U_2 «условное» преобразование $|0\rangle\langle 0| \otimes U_1 + |1\rangle\langle 1| \otimes U_2$ тоже является унитарным. Вентиль CONTROLLED-NOT (К-НЕ) может быть определён, как

$$C_{\text{not}} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X.$$

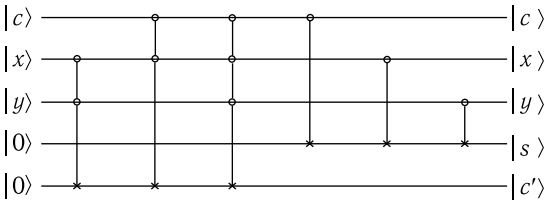
Трёхкубитный CONTROLLED-CONTROLLED-NOT или вентиль Тоффоли, рассмотренный в разделе 4, также является примером этого условного определения:

$$T = |0\rangle\langle 0| \otimes I \otimes I + |1\rangle\langle 1| \otimes C_{\text{not}}.$$

Оператор Тоффоли T может быть использован для построения полного набора булевых связок, так как с помощью него можно построить операторы AND и NOT:

$$T|1,\,1,\,x\rangle = |1,\,1,\,\neg x\rangle,$$
$$T|x,\,y,\,0\rangle = |x,\,y,\,x \wedge y\rangle.$$

Используя вентили Тоффоли можно построить любую классическую логическую схему. Например, следующая квантовая схема производит одноразрядное сложение, используя вентили Тоффоли и CONTROLLED-NOT



где x и y это биты данных, s — их сумма по модулю 2, c — входной разряд переноса, а c' — выходной разряд переноса. В работах Ведрала, Баренко и Экерта [Ekert et al. 1996] используются более сложные схемы.

Вентиль Фредкина выполняет так называемый «управляемый обмен», и определяется, как

$$F = |0\rangle\langle 0| \otimes I \otimes I + |1\rangle\langle 1| \otimes S,$$

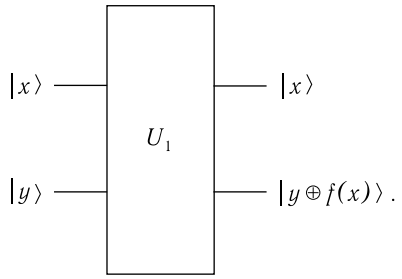
где S — операция, производящая обмен

$$S = |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|.$$

Читатель может проверить, что F и T, являются полными для построения произвольных классических логических схем.

Дойч показал [Deutsch 1985], что возможно построить обратимые квантовые схемы для вычисления любой классической функции. Фактически можно ввести понятие универсальной квантовой машины Тьюринга [Bernstein and Vazirani 1997]. При этом надо иметь в виду, что для «ленты» машины Тьюринга должно быть предоставлено необходимое количество кубитов.

Любая классическая функция f с m входными и k входными битами может быть вычислена на квантовом компьютере, то есть, существует такая квантовая схема, которая вычисляет f. Рассмотрим $(m+k)$-битовое преобразование $U_f\colon |x,\,y\rangle \to |x,\,y \oplus f(x)\rangle$, где $\oplus$ обозначает побитовое исключающее-ИЛИ (не путайте с векторной суммой). Квантовая схема U_f, определенная таким способом, является унитарной при любой функции f. Для того, чтобы вычислить $f(x)$ мы применяем U_f к $|x\rangle$, тензорно умноженному на с k нулей $|x,\,0\rangle$. Поскольку $f(x) \oplus f(x) = 0$, то мы имеем $U_f U_f = I$. Графически преобразование $U_f\colon |x,\,y\rangle \to |x,\,y \oplus f(x)\rangle$ изображается следующим образом:



Хотя вентили T и F являются универсальными для классических логических схем, из них нельзя построить произвольные квантовые преобразования. Для того, чтобы осуществить произвольные унитарные преобразования с точностью до постоянного фазового множителя (общий фазовый сдвиг состояния не имеет физического смысла), необходимо рассмотреть вращения одного бита. Баренко и др. [Barenco et al. 1995] показали, что C_{not} вместе с полным набором однобитовых квантовых вентилей является универсальным набором. Достаточно иметь возможность выполнять следующие однобитовые преобразования

$$\begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}, \begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{-i\alpha} \end{pmatrix}.$$

для всех $0 \leqslant \alpha \leqslant 2\pi$, а также C_{not}[1], чтобы получить универсальный набор квантовых вентилей. Как позднее будет видно, такие преобразования являются ключевыми для использования преимуществ квантовых вычислений.

5.2. Квантовый параллелизм

Что происходит, если U_f применяется к входному состоянию, которое является в суперпозицией? Ответ прост и удивителен: поскольку U_f — это линейное преобразование, то оно применяется ко всем базисным векторам в суперпозиции одновременно, и создает суперпозицию результатов. Таким способом возможно вычислить $f(x)$ для n значений аргумента x при однократном применении U_f. Такой эффект называется квантовым параллелизмом.

Достоинство квантовых алгоритмов заключается в преимуществе квантового параллеллизма и запутанности. Так, большинство квантовых алгоритмов начинается с вычисления интересующей нас функции на суперпозиции всех значений. Все начинается с состояния $|00\ldots0\rangle$ n-кубитов. Далее применяется преобразование Уолша–Адамара W из подраздела 4.1.1. для получения суперпозиции

$$\frac{1}{\sqrt{2^n}}\left(|00\ldots0\rangle + |00\ldots1\rangle + \ldots + |11\ldots1\rangle\right) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle.$$

[1] Имеется в виду возможность осуществления C_{not} для *каждой* пары кубитов. — *Прим. перев.*

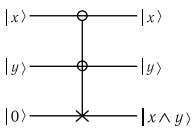
Добавляется k-битный регистр $|0\rangle$, и затем, по условию линейности, получаем

$$U_f\left(\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x,\,0\rangle\right)=\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}U_f\big(|x,\,0\rangle\big)=\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x,\,f(x)\rangle,$$

где $f(x)$ — интересующая нас функция. Следует отметить, что поскольку n кубитов позволяют работать одновременно с 2^n состояниями, то квантовый параллелизм обходит ограничение пространство-время классического параллелизма, так как он может обеспечить экспоненциальное возрастание вычислительного пространства при линейном возрастании объёма физического пространства.

Рассмотрим тривиальный пример использования CONTROLLED-CONTROLLED-NOT оператора Тоффоли T, для вычисления коньюнкции двух величин:

На вход подадим суперпозицию всех возможных бит-комбинаций x и y, кроме $x=1$, $y=1$:



$$H|0\rangle\otimes H|0\rangle\otimes|0\rangle=\frac{1}{\sqrt{2}}\big(|0\rangle+|1\rangle\big)\otimes\frac{1}{2}(|0\rangle+|1\rangle)\otimes|0\rangle=$$
$$=\frac{1}{2}\big(|000\rangle+|010\rangle+|100\rangle+|110\rangle\big).$$

Применяем T к суперпозиции входов, чтобы получить суперпозицию результатов:

$$T\big(H|0\rangle\otimes H|0\rangle\otimes|0\rangle\big)=\frac{1}{2}\big(|000\rangle+|010\rangle+|100\rangle+|111\rangle\big).$$

Результирующую суперпозицию можно рассматривать как таблицу истинности для конъюнкции или как граф функции. На выходе величины x, y и $x\wedge y$ запутаны таким образом, что измерение результата даст одну строку таблицы истинности, или, что эквивалентно, точку графа функции. После измерения, первые два кубита соответствуют входному значения, а третий кубит — соответствующему значению f.

На первый взгляд, здесь нет преимущества над классическим параллелизмом, поскольку при измерении можно получить только один результат, и к тому же мы не можем выбирать, какой результат мы получим. Суть любого квантового алгоритма — это способ, с помощью, которого он манипулирует квантовым параллелизмом таким образом, чтобы желаемые результаты измерялись с большой вероятностью. Управление такого типа не имеет классического аналога и требует нетрадиционных приемов программирования. Вот пара приемов, которые известны на сегодняшний день:

Усиление нужных нам выходных величин. Основная идея этого способа заключается в преобразовании состояния таким образом, чтобы интересующие нас величины имели большую амплитуду и, следовательно, более высокую вероятность быть измеренными. Примеры будут представлены в разделе 7.

Нахождение общих свойств всех значений $f(x)$. Этот способ применен в алгоритме Шора, где используется квантовое преобразование Фурье для получения периода f.

6. Алгоритм Шора

В 1994 году Питер Шор, вдохновленный работой Даниеля Саймона (опубликованной позже [Simon 1997]), открыл ограниченно–вероятностный алгоритм разложения на множители n-разрядных чисел за полиномиальное время на квантовом компьютере. Начиная с семидесятых, люди ищут эффективные алгоритмы для разложения целых чисел. Наиболее эффективным классическим алгоритмом, известным на сегодняшний день, является алгоритм Ленстра и Ленстра [Lenstra and Lenstra 1993], который экспоненциален по размеру входа. Вход — это набор цифр числа M, имеющий размер $n \sim \log M$. Люди были настолько уверены в том, что эффективного алгоритма разложения не существует, что были созданы криптографические системы, например RSA, которые опираются на сложность этой проблемы. Результат Шора был ошеломляющим для большинства учёных, побудив их к широкомасштабным исследованиям в области квантовых вычислений.

В большинстве алгоритмов, включая алгоритм Шора, используется стандартный способ сведения задачи разложения к задаче поиска периода функции. Шор использует квантовый параллелизм для получения суперпозиции всех значений функции за один шаг. Затем он производит квантовое преобразование Фурье, результатом которого, как для классического преобразовании Фурье, является функция, аргумент которой кратен величине, обратной периоду. С высокой вероятностью измерение состояния возвращает период, который в свою очередь, служит для разложения целого числа M.

Все что было сказано выше, раскрывает суть квантового алгоритма, но в очень упрощённом виде. Наибольшая трудность заключается в том, что квантовое преобразование Фурье основано на быстром преобразовании Фурье и, таким образом, дает только приблизительный результат в большинстве случаев.

Для начала мы опишем квантовое преобразование Фурье, а затем дадим подробное описание алгоритма Шора.

6.1. Квантовое преобразование Фурье

В общем случае преобразования Фурье переносят данные из временной в частотную область. Так, преобразования Фурье преобразуют функции с периодом r в функции, у которых значения, отличные от нуля, появляются только в значениях кратных частоте $\frac{2\pi}{r}$. Дискретное преобразование Фурье (DFT, ДПФ) действует на N равноудаленных выборок в полуинтервале $[0,\, 2\pi)$ для некоторого N, и выдает функцию, чья область определения — это целые числа от 0 до $N-1$. Дискретное преобразование Фурье функции периода r — это функция, сконцентрированная около значений, кратных $\frac{N}{r}$. Если период r делит N без остатка, то результатом будет функция, у которой значения, отличные от нуля, имеются только в точках, кратных $\frac{N}{r}$. В противном случае результат будет приближённым, и отличные от нуля члены появятся в числах, близких к кратным $\frac{N}{r}$.

Быстрое преобразование Фурье (FFT, БПФ) является разновидностью DFT,

где N — степень двойки. Квантовое преобразование Фурье (QFT, КПФ) является вариантом DFT, где, также, как и в FFT, используются степени двойки. Квантовое преобразование Фурье действует на амплитуды квантового состояния, как

$$\sum_x g(x)|x\rangle \to \sum_c G(c)|c\rangle,$$

где $G(c)$ — это дискретное преобразование Фурье $g(x)$, а x и c варьируются, как целые числа от 0 до $N-1$ (в двоичном представлении). Если бы состояние измерили после того, как преобразование Фурье выполнено, то вероятность того, что результат $|c\rangle$, была бы $|G(c)|^2$.

Применяя квантовое преобразование Фурье к периодической функции $g(x)$ с периодом r, мы предполагали закончить с $\sum_c G(c)|c\rangle$, где $G(c)$ равно нулю везде, кроме значений, кратных $\frac{N}{r}$. Таким образом, когда состояние измерено, результатом являются значения, кратные $\frac{N}{r}$, например $j\frac{N}{r}$. Но, как уже было замечено выше, квантовые преобразования Фурье дают лишь приблизительный результат для периодов, которые не являются степенью двух, т.е. периодов, которые не делят N. Однако чем больше степень двойки, использована в качестве базы преобразования, тем точнее аппроксимация. Квантовое преобразование Фурье U_{QFT} с базой $N = 2^m$ определяется как

$$U_{QFT} : |x\rangle \to \frac{1}{\sqrt{2^m}} \sum_{c=0}^{2^m-1} e^{\frac{2\pi icx}{2^m}} |c\rangle.$$

Для того, чтобы алгоритм Шора был полиномиальным, необходимо чтобы квантовое преобразование Фурье вычислялось эффективно. Шор показывает, что квантовое преобразование Фурье с базой 2^m можно построить с использованием только $\frac{m(m+1)}{2}$ преобразований. Это построение использует 2 типа вентилей. Один — для реализации уже знакомого преобразования Адамара H (через H_j обозначим преобразование Адамара, применяемое к j-му биту), другой — для реализации двубитного преобразования вида

$$S_{j,k} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\theta_{k-j}} \end{pmatrix},$$

где $\theta_{k-j} = \pi/2^{k-j}$. Это преобразование воздействует на k-ый и j-ный биты большого регистра. Квантовое преобразование Фурье задается выражением

$$H_0 S_{0,1} \ldots S_{0,m-1} H_1 \ldots H_{m-3} S_{m-3,m-2} S_{m-3,m-1} H_{m-2} S_{m-2,m-1} H_{m-1},$$

за которым следует обращение битов. Если за FFT следует измерение, как в алгоритме Шора, то обращение битов выполняется классическим способом. Все детали выполнения алгоритма можно найти в работе автора алгоритма [Shor 1997].

6.2. Подробности алгоритма Шора

Последовательные шаги алгоритма Шора детально представлены в нижеследующем примере, где мы разлагаем на множители число $M = 21$.

Шаг 1. Квантовый параллелизм. Произвольно выбираем число a. Если a не является взаимно простым с M, то значит мы уже нашли делиттель M. В противном случае применяем оставшуюся часть алгоритма.

Пусть m будет таким, что $M^2 \leqslant 2^m < 2M^2$ [Этот выбор был сделан таким образом, чтобы аппроксимации, применяемой в шаге 3 для функций, чей период не является степенью двойки, будет вполне достаточно, чтобы оставшаяся часть алгоритма работала]. Используем квантовый параллелизм, как описано в подразделе 5.2. для вычисления $f(x) = a^x \mod M$ для всех целых чисел от 0 до $2^m - 1$. Получим, таким образом

$$\frac{1}{2^m} \sum_{x=0}^{2^m-1} |x,\, f(x)\rangle. \tag{1}$$

Пример. Предположим $a = 11$ было выбрано случайно. Т. к. $M^2 = 441 \leqslant 2^9 < 882 = 2M^2$, то мы находим $m = 9$. Таким образом, всего 14 кубитов, 9 для x и 5 для $f(x)$, требуются для вычисления суперпозиции (1).

Шаг 2. Состояние, чья амплитуда имеет тот же период, что и f. Квантовое преобразование Фурье воздействует на функцию амплитуды, связанной с входным состоянием. Чтобы использовать квантовое преобразование Фурье для получения периода функции f, необходимо составить состояние, чья функция амплитуды имеет тот же период, что и f.

Для составления такого состояния, измеряем последние $[\log_2 M]$ кубиты состояния (1), которые относятся к $f(x)$. Получаем случайное значение u. Само по себе значение u никакого интереса не представляет; нас интересует только воздействие измерения на наше множество суперпозиций. Это измерение проектирует пространство состояний на подпространство данной измеренной величины, поэтому состояние после измерения становится

$$C \sum_x g(x)|x,\, u\rangle,$$

с точностью до некоторого множителя C, где

$$g(x) = \begin{cases} 1, & \text{если } f(x) = u, \\ 0, & \text{в противном случае.} \end{cases}$$

Отметим, что иксы, которые появились в сумме, те, что с $g(x) \neq 0$, отличаются от друг от друга числом, кратным периоду, следовательно, $g(x)$ это и есть та функция, которую мы ищем. Если бы мы могли измерить два полученных икса в сумме, мы могли бы иметь период. Но к сожалению, законы квантовой физики позволяют нам провести только одно измерение.

Пример. Предположим, что случайное измерение суперпозиции уравнения (1) выдает 8. Состояние после этого измерения (На рис. 2 представлено только 9 битов; биты $f(x)$ известны из измерения) ясно демонстрирует нам периодичность f.

Шаг 3. Применение квантового преобразования Фурье. Часть состояния $|u\rangle$ больше использоваться не будет, поэтому мы ее не записываем. Применим квантовое преобразование Фурье к состоянию, полученному на шаге 2.

$$U_{QFT} : \sum_x g(x)|x\rangle \to \sum_c G(c)|c\rangle$$

Из стандартного анализа Фурье получаем, что, когда период r функции $g(x)$, определенной в шаге 2, есть степень двойки, то результат квантового преобразования Фурье есть

$$\sum_j c_j |j\frac{2^m}{r}\rangle,$$

где амплитуда равна нулю, кроме точек, кратных $2^m/r$. Когда период r не делит 2^m, преобразование выполняется точно, причём большая амплитуда сосредоточена в близи целых значений, кратных $\frac{2^m}{r}$.

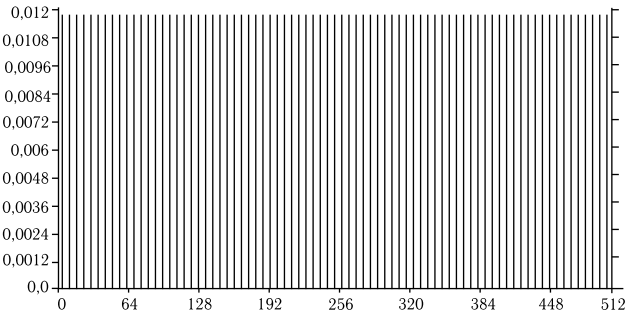


Рис. 2

Вероятности для различных x при измерении состояния $C \sum_{x \in X} |x, 8\rangle$ полученного в шаге 2, где $X = \{x|211^x \mod 21 = 8\}\}$.

Распределение вероятности квантового состояния после преобразования Фурье.

Пример. На рис. 3 отображён результат применения квантового преобразования Фурье к состоянию, полученному в шаге 2. Необходимо отметить, что рис. 3 — это график Быстрого Преобразования Фурье функции, показанной на рис. 2. В этом частном случае период функции f не делит 2^m.

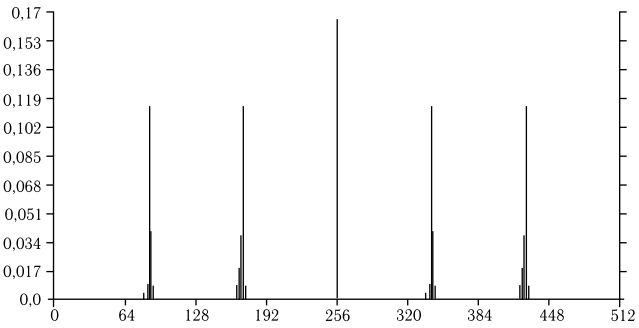


Рис. 3

Шаг 4. Извлечение периода. Измеряем состояния в стандартном базисе и получаем результат v. В случае, когда период является степенью двойки, квантовое преобразование дает точные значения, кратные $2m/r$, и извлечь период не сложно. В этом случае $v = j\frac{2^m}{r}$ для некоторого j. В большинстве случаев j и r будут взаимно просты, и в этом случае сокращение дроби $\frac{v}{2^m}(= \frac{j}{r})$ даст дробь, чей знаменатель q есть период r. Дело в том, что в общем случае квантовое преобразование Фурье даёт кратные значения основной частоты только приблизительно, что усложняет выяснение периода по результату измерения. Когда период не является степенью двойки, может быть получена хорошая оценка периода, если использовать так называемое разложение в бесконечную дробь $\frac{v}{2^m}$ Этот классический приём описывается в приложении B.

Пример. Допустим, что измерение состояния даёт величину $v = 427$. Поскольку v и 2^m взаимно просты, период r скорее всего не будет делить 2^m и поэтому можно применить разложение в бесконечную дробь, описанное в приложении B. Следующая таблица прослеживает алгоритм, описанный в приложении B,

i	a_i	p_i	q_i	ε_i
0	0	0	1	0.8339844
1	1	1	1	0.1990632
2	5	5	6	0.02352941
3	42	211	253	0.5

который заканчивается числом $6 = q_2 < M \leqslant q_3$. Таким образом, $q = 6$ наверняка является период функции f.

Шаг 5. Нахождение делителя M. Когда полученный период q чётный, используем алгоритм Евклида для эффективной проверки, имеют ли $a^{q/2} + 1$ или $a^{q/2} - 1$ отличный от единицы общий делитель с M.

Причина, по которой $a^{q/2} + 1$ или $a^{q/2} - 1$ могут иметь общий отличный от единицы делитель с M следующая. Если q действительно является периодом

функции $f(x) = a^x \mod M$, то $a^q = 1 \mod M$, поскольку $a^q a^x = a^x$ для всех x. Если q — чётно, мы можем записать

$$(a^{q/2} + 1)(a^{q/2} - 1) = 0 \mod M.$$

Следовательно, поскольку ни $a^{q/2} + 1$, ни $a^{q/2} - 1$ не являются кратными значениями M, $a^{q/2}+1$ или $a^{q/2}-1$ имеют отличный от единицы общий с M делитель.

Пример. Поскольку 6 чётное число, то либо $a^{6/2} - 1 = 11^3 - 1 = 1330$, либо $a^{6/2}+1 = 11^3+1 = 1332$ будут иметь общий с M делитель. В этом частном примере мы находим два делителя НОД(21,1330)=7 и НОД(21,1332)=3.

Шаг 6. При необходимости повторяем алгоритм. Некоторые действия могут выполняться неточно, поэтому процесс может не дать делитель M:

(1) Значение v не достаточно близко к кратному $\frac{2^m}{r}$.

(2) Период r и сомножитель j могут иметь общий множитель, а при этом знаменатель q является делителем периода, а не самим периодом.

(3) Шаг 5 выдаёт M, как делитель M.

(4) Период функции $f(x) = a^x \mod M$ является нечётным.

Шор показал, что небольшое число повторений алгоритма дает множитель M с высокой вероятностью.

6.2.1. Комментарий к шагу 2 алгоритма Шора. Оказывается, измерения на шаге 2 можно полностью опустить. Бернштейн и Вазирани [Bernstein and Vazirani 1997] показали, что измерений в середине алгоритма можно всегда избежать. Если исключить измерение на шаге 2, то состояние будет состоять из суперпозиций нескольких периодических функций. Каждая из них имеет один и тот же период. Вследствие линейности квантовых алгоритмов, применяемое квантовое преобразование Фурье приводит к суперпозиции преобразований Фурье этих функций. Каждое из этих преобразований запутано с соответствующим u и, следовательно, они не интерферируют друг с другом. Измерение дает значение одного из этих преобразований. Понимание того, как это утверждение можно обобщить, иллюстрирует некоторые тонкости работы с квантовыми суперпозициями. Применим тензорное произведение квантового преобразования Фурье и оператора идентичности $U_{QFT} \otimes I$ к $C \sum_{x=0}^{2^n-1} |x,\, f(x)\rangle$, получив

$$C' \sum_{x=0}^{2^n-1} \sum_{c=0}^{2^m-1} e^{\frac{2\pi i x c}{2^m}} |c,\, f(x)\rangle,$$

что равно

$$C' \sum_{u} \sum_{x|f(x)=u} \sum_{c} e^{\frac{2\pi i x c}{2^m}} |c,\, u\rangle$$

для u в диапазоне $f(x)$. То, что получилось, есть суперпозиция результатов, полученных в шаге 3, для всех возможных u. Квантовое преобразование Фурье применяют к семейству отдельных функций g_u, индексируемых по u, где

$$g_u = \begin{cases} 1, & \text{если } f(x) = u, \\ 0, & \text{в противном случае,} \end{cases}$$

причём у всех одинаковый период. Необходимо отметить, что амплитуды в состояниях с различными u никогда не интерферируют (складываются или взаимоуничтожаются) друг с другом. Преобразование $U_{QFT} \otimes I$ можно записать как

$$U_{QFT} \otimes I : C \sum_{u \in R} \sum_{x=0}^{2^n-1} g_u(x)|x,\, f(x)\rangle \to C' \sum_{u \in R} \sum_{x=0}^{2^n-1} \sum_{c=0}^{2^n-1} G_u(c)|c,\, u\rangle,$$

где $G_u(c)$ — это дискретное преобразование Фурье $g_u(x)$, а R — диапазон $f(x)$.

Измеряем c и повторяем шаги 4 и 5 как прежде.

7. Задачи поиска

Большой класс задач можно определять как задачи поиска вроде «найти x из множества возможных решений, такое, что утверждение $P(x)$ — истинно». Диапазон подобных задач широк: от поиска информации в базе данных до закраски графа. Например, задачу закраски графа можно рассматривать как поиск такого обозначения цветов вершин, что утверждение «все примыкающие вершины имеют разные цвета» является верным. Аналогично задача сортировки может быть рассмотрена, как поиск перестановки, для которой утверждение «перестановка x переводит первоначальное состояние сортировки в желаемое» являлось бы верным.

В задаче *неупорядоченного* поиска ничего не известно о структуре пространства решений и об утверждении P. Например, определение $P(x_0)$ не дает никакой информации о возможном значении $P(x_1)$ для $x_0 \neq x_1$. В задаче *упорядоченного* поиска можно использовать информацию о пространстве поиска и об утверждении P.

Например, поиск по алфавитному списку является задачей упорядоченного поиска, и алфавитный порядок используется для построения алгоритма. В других случаях, скажем, в задачах, где нужно найти хотя бы одно решение (3- SAT или закраска графа) структуру задачи можно использовать для построения эвристических алгоритмов, которые быстро дают решения для некоторых отдельных случаев. Но в общем случае, когда мы имеем задачу неупорядоченного поиска, лучшее, что можно сделать классическим путём — это последовательно проверять истинность каждого утверждения $P(x_i)$. Для поискового пространства из N элементов обычная задача неупорядоченного поиска требует $O(N)$ проверок P. На квантовом же компьютере, как показал Гровер, задачу неупорядоченного поиска можно решить с большой вероятностью производя около $O(\sqrt{N})$ проверок P. Таким образом, квантовый алгоритм Гровера [Grover 1996] является заведомо более эффективным, чем любой алгоритм для неупорядоченного поиска, выполняемый на классическом компьютере.

Оказывается, для неупорядоченного поиска алгоритм Гровера является оптимальным [Bennett et al. 1997; Boyer et al. 1996; Zalka 1997]. Однако для большинства поисковых задач требуется упорядоченный поиск. Поскольку существуют классические эвристические алгоритмы, использующие упорядоченность, то можно ожидать, что существуют также и эффективные квантовые алгоритмы для упорядоченного поиска. Серф и др. [Cerf et al. 1998] используют алгоритм Гровера вместо классического поиска внутри эвристического алгоритма, чтобы показать, что возможно квадратичное ускорение, когда речь идёт о решении NP-сложных задач.

Брассард и др. [Brassard et al. 1998], опираясь на алгоритм Гровера, показали, что общий классический эвристический поиск имеет квантовый аналог с квадратичным ускорением.

Есть некоторая надежда на то, что для некоторых упорядоченных задач существует ускорение большее, чем квадратичное. Возможно, подобные алгоритмы потребуют новых подходов, которые заключаются не просто в квантовом исполнении классических алгоритмов. Если алгоритм Шора рассматривать в качестве поиска множителей, то он может послужить примером алгоритма, который достигает экспоненциального ускорения, используя структуру задачи (теорию чисел) нестандартным способом, уникальным для квантовых вычислений.

Тед Хогг также разработал несколько эвристических квантовых алгоритмов упорядоченного поиска. Его подход является совершенно неклассическим, в нём используются весьма нетривиальные свойства квантовых вычислений. Единственный минус его подхода заключается в том, что, как и во многих эвристических алгоритмах, использование упорядоченности является усложнённым, и при этом очень трудно определить вероятность получения верного ответа при одной итерации алгоритма. Следовательно, пока ещё не понятно, насколько эффективны алгоритмы Хогга. В классической теории эффективность эвристических алгоритмов оценивается с помощью эмпирического тестирования. Но, поскольку, при моделировании квантовых операций на классическом компьютере наблюдается экспоненциальное замедление, то эмпирическое тестирование квантовых алгоритмов сегодня невозможно, разве что за небольшими исключением. Алгоритм Хогга в применении к некоторым задачам упорядоченного поиска, является более эффективным, чем алгоритм Гровера, но ускорение при этом является полиномиальным. С теоретической точки зрения — это менее интересно, но с практической — даже малое полиномиальное ускорение этих вычислительных задач имеет огромное значение. До тех пор, пока не будет создано больших квантовых компьютеров или лучших приёмов для анализа таких алгоритмов, эффективность нельзя будет определить точно.

7.1. Поисковый алгоритм Гровера

Алгоритм Гровера ведет поиск элемента x, который делает верным некоторое утверждение, в неупорядоченном списке размером N. Пусть n будет таким, что $2^n \geqslant N$, и пусть U_p будет квантовым вентилем, который вычисляет классическую функцию $P(x)$, проверяющую истинность утверждения (истине соот-

ветствует 1):

$$U_p : |x,\, 0\rangle \to |x,\, P(x)\rangle.$$

Первый шаг — стандартный для квантовых вычислений, описанный в подразделе 5.2. Вычислим P для всех возможных входов x_i применяя U_P к регистру, содержащему суперпозицию $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{n-1} |x\rangle$ для всех 2^n возможных входов x вместе с регистром, установленным в 0. Сделав это, придём к

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{n-1} |x,\, P(x)\rangle. \tag{2}$$

Сложным является извлечение полезного результата из этой суперпозиции.

Для любого x_0, при котором $P(x_0)$ — истинно, $|x_0,\, 1\rangle$ будет частью суперпозиции уравнения 2. Т. к. амплитуда такого состояния равна $\frac{1}{\sqrt{2^n}}$, вероятность того, что случайное измерение суперпозиции даст x_0 — всего лишь 2^{-n}. Хитрость состоит в том, чтобы изменить квантовое состояние в ур. 2 таким образом, что амплитуды векторов $|x_0,\, 1\rangle$, для которых P истинно, сильно возрастают, а амлитуды векторов $|x,\, 0\rangle$, для которых P ложно — уменьшаются.

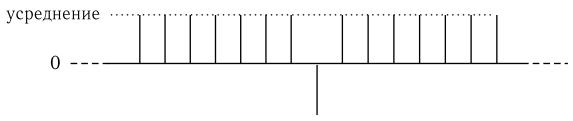
Пусть такое преобразование квантового состояния было выполнено, тогда легко измерить последний кубит квантового состояния, который задает $P(x)$. Так как амплитуда состояния, соответствующего истине была увеличена, то существует высокая вероятность, что и при измерении мы получим 1. В этом случае измерение проектирует состояние (2) на подпространство $\frac{1}{\sqrt{2^k}} \sum_{i=1}^{k} |x_i,\, 1\rangle$, где k — число решений. Дальнейшее измерение оставшихся битов даст одно из этих решений. Если измерение кубита $P(x)$ дает значение 0, тогда весь процесс повторяется снова, и суперпозицию ур. 2 надо вычислять заново.

Алгоритм Гровера состоит из следующих шагов:

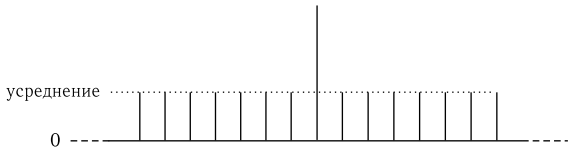
(1) Подготовка регистра, содержащего суперпозицию всех возможных значений $x_i \in [0 \ldots 2^n - 1]$.

(2) Вычисление $P(x_i)$ от этого регистра.

(3) Изменение амплитуды a_j на $-a_j$ для такого x_i, что $P(x_j) = 1$. (Эффективный алгоритм выполнения этой операции описывается в подразделе 7.1.2.) График амплитуд после этого шага:



(4) Применение инверсии относительно среднего для увеличения амплитуды x_j, соответствующего $P(x_j) = 1$. (Квантовый алгоритм для эффективного выполнения инверсии относительно среднего рассматривается в подразделе 7.1.1.) Результирующие амплитуды выглядят как



Амплитуда всех x_i, для которых $P(x_i) = 0$ была незначительно снижена.

(5) Повторение 2,3,4-го шагов $\frac{\pi}{4}\sqrt{2^n}$ раз.

(6) Считывание результата.

Бойер и др. [Boyer et al. 1996] провели детальный анализ реализации алгоритма Гровера. Они доказали, что этот алгоритм является оптимальным (с точностью до постоянного множителя), то есть ни один другой квантовый алгоритм не может выполнить неупорядоченный поиск быстрее. Они также показали, что, если существует только один x_0, такой что $P(x_0)$, то после $\frac{\pi}{8}\sqrt{2^n}$ итераций шагов 2,3 и 4 вероятность ошибки равна 0,5. После выполнения $\frac{\pi}{4}\sqrt{2^n}$ итераций вероятность ошибки снижается до 2^{-n}. И, что интересно, дополнительные итерации увеличивают её. Например, после $\frac{\pi}{2}\sqrt{2^n}$ итераций вероятность ошибки приближается к 1.

Существует множество классических алгоритмов, где процедура повторяется много раз для получения лучшего результата. Повторяя квантовые процедуры, можно улучшить результат, но после определённого количества повторений результат ухудшается. Квантовые процедуры — это унитарные преобразования, которые являются вращениями комплексного пространства. Таким образом, сначала повторное применение квантового преобразования поворачивает состояние к желаемому состоянию, а потом, очевидно, повороты будут приводить к удалению от желаемого состояния.

Следовательно, чтобы получить удовлетворительный результат от повторного применения квантового преобразования, надо знать, когда остановиться. Брассард и др. [Brassard et al. 1998] описывают расширение алгоритма Гровера, в котором используется преобразование Фуре для определения числа решений и оптимального количества итераций. Это расширение в общем, не увеличивает сложность алгоритма.

Гровер применил свой алгоритм для получения квадратичного ускорения в некоторых непоисковых задачах, например, таких как вычисление средней величины функции [Grover 1998]. Используя подобные приёмы, Гровер также показал, что некоторые поисковые задачи, которые на классических компьютерах выполняются за $O(\log N)$, могут быть решены за $O(1)$ на квантовом компьютере. Поиск Гровера можно использовать в других квантовых вычилсениях в качестве подпрограммы. Байрон и др. [Biron et al. 1998] показали, что алгоритм Гровера можно применять для произвольного начального распределения амплитуд, и что при этом сохраняется сложность порядка $O(\sqrt{N})$.

7.1.1. Инверсия относительно среднего. Чтобы осуществить инверсию относительно среднего на квантовом компьютере, она должна быть унитарным преобразованием. Более того, чтобы решить задачу за время $O(\sqrt{N})$, инверсия должна быть реализована эффективно. Как вкратце будет показано, инверсию можно выполнить используя $O(n) = O\big(\log(N)\big)$ квантовых вентилей.

Нетрудно заметить, что преобразование

$$\sum_{i=0}^{N-1} a_i|x_i\rangle \to \sum_{i=0}^{N-1} (2A - a_i)|x_i\rangle,$$

где A обозначает среднее a_j, является матрицей $N \times N$

$$D = \begin{pmatrix} \frac{2}{N} - 1 & \frac{2}{N} & \dots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} - 1 & \dots & \frac{2}{N} \\ \dots & \dots & \dots & \dots \\ \frac{2}{N} & \frac{2}{N} & \dots & \frac{2}{N} - 1 \end{pmatrix}.$$

Так как $DD^* = I$, то D — унитарно и, следовательно, является возможным преобразованием квантового состояния.

Теперь вернёмся к вопросу об эффективности реализации этого преобразования. Покажем, что его можно разложить на $O(n) = O\big(\log(N)\big)$ простейших квантовых вентилей. Следуя работе Гровера, D можно определить как $D = WRW$, где W — преобразование Уолша – Адамара (из раздела 4), а

$$R = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & -1 & 0 & \dots \\ 0 & \dots & \dots & 0 \\ 0 & \dots & 0 & -1 \end{pmatrix}.$$

Чтобы убедиться, что $D = WRW$, предположим, что $R = R' - I$, где I — тождественный оператор, а

$$R' = \begin{pmatrix} 2 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots \\ 0 & \dots & \dots & 0 \\ 0 & \dots & 0 & 0 \end{pmatrix}.$$

Теперь $WRW = W(R' - I)W = WR'W - I$. Легко проверить, что

$$WR'W = \begin{pmatrix} \frac{2}{N} & \frac{2}{N} & \dots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} & \frac{2}{N} & \dots \\ \frac{2}{N} & \dots & \dots & \frac{2}{N} \\ \frac{2}{N} & \dots & \frac{2}{N} & \frac{2}{N} \end{pmatrix}.$$

Таким образом, $WR'W - I = D$.

7.1.2. Изменение знака. Здесь мы покажем в общих чертах удивительно простой способ инверсии амплитуды тех состояний, при которых $P(x) = 1$.

Пусть U_P есть квантовая схема, которая выполняет преобразование U_P: $|x,\, b\rangle \to |x,\, b \oplus P(x)\rangle$. Применим U_P к суперпозиции $|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{n-1} |x\rangle$ и выберем $b = \frac{1}{\sqrt{2}}|0\rangle - |1\rangle$, чтобы прийти в состояние, для которого знак всех x, при которых. $P(x) = 1$ будет изменён, а b останется неизменным.

Для того чтобы увидеть это, положим $X_0 = \{x|P(x) = 0\}$, $X_1 = \{x|P(x) = 0\}$ и применим U_P

$$
\begin{aligned}
U_P(|\psi,\, b\rangle) &= \frac{1}{\sqrt{2^{n+1}}} U_P \left(\sum_{x \in X_0} |x,\, 0\rangle + \sum_{x \in X_1} |x,\, 0\rangle - \sum_{x \in X_0} |x,\, 1\rangle - \sum_{x \in X_1} |x,\, 1\rangle \right) = \\
&= \frac{1}{\sqrt{2^{n+1}}} \left(\sum_{x \in X_0} |x,\, 0 \oplus 0\rangle + \sum_{x \in X_1} |x,\, 0 \oplus 1\rangle - \sum_{x \in X_0} |x,\, 1 \oplus 0\rangle - \sum_{x \in X_1} |x,\, 1 \oplus 1\rangle \right) = \\
&= \frac{1}{\sqrt{2^{n+1}}} \left(\sum_{x \in X_0} |x,\, 0\rangle + \sum_{x \in X_1} |x,\, 1\rangle - \sum_{x \in X_0} |x,\, 1\rangle - \sum_{x \in X_1} |x,\, 0\rangle \right) = \\
&= \frac{1}{\sqrt{2^n}} \left(\sum_{x \in X_0} |x\rangle - \sum_{x \in X_1} |x\rangle \right) \oplus b.
\end{aligned}
$$

Амплитуда состояний в X_1 инвертирована, что и требовалось.

7.2. Эвристический поиск

7.2.1. Замечание к преобразованию Уолша – Адамара. Существует другое представление преобразования Уолша – Адамара, описанного в подразделе 4.1.1, полезное для понимания того, как можно использовать это преобразование для построения квантовых алгоритмов. n-битное преобразование Уолша – Адамара можно представить в виде матрицы W $2^n \times 2^n$ с элементами W_{rs}, где r и s варьируются от 0 до $2^n - 1$. Мы покажем, что

$$W_{rs} = \frac{1}{\sqrt{2^n}} (-1)^{r \cdot s},$$

где $r \cdot s$ это число общих единичных битов в двоичном представлении r и s.

Чтобы понять это равенство, заметим, что

$$W\big(|r\rangle\big) = \sum_s W_{rs} |s\rangle.$$

Пусть $r_{n-1} \ldots r_0$ будет двоичным представлением r, а $s_{n-1} \ldots s_0$ — двоичным

представлением s, тогда

$$W\big(|r\rangle\big) = \big(H \otimes \ldots \otimes H\big)\big(|r_{n-1}\rangle \otimes \ldots \otimes |r_0\rangle\big) =$$
$$= \frac{1}{\sqrt{2^n}}\big(|0\rangle + (-1)^{r_{n-1}}|1\rangle\big) \otimes \ldots \otimes \big(|0\rangle + (-1)^{r_0}|1\rangle\big) =$$
$$= \frac{1}{\sqrt{2^n}} \sum_{s=0}^{2^n-1} (-1)^{s_{n-1}r_{n-1}}|s_{n-1}\rangle \otimes \ldots \otimes (-1)^{s_0 r_0}|s_0\rangle == \frac{1}{\sqrt{2^n}} \sum_{2^n-1}^{s=0} (-1)^{s\cdot r}|s\rangle.$$

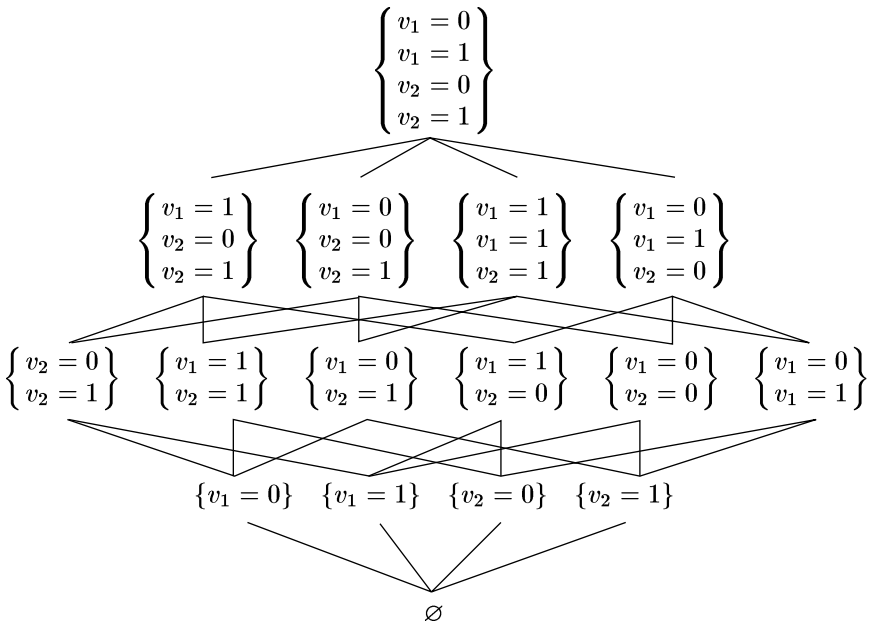


Рис. 4. Решётка переменных присвоений CSP (ограниченно выполняемая задача).

7.2.2. Обзор алгоритмов Хогга. В ограниченно-выполнимой задаче есть n переменных $V = \{v_1, \ldots, v_n\}$, которые могут принимать m разных значений $X = \{x_1, \ldots, x_m\}$, подчиненных определенным ограничениям $C_1, \ldots C_l$. Решения ограниченно-выполнимой задачи лежат в пространстве присвоений x_i к v_j $V \times X$. Существует естественная решёточная структура, определяемая исходя из ограничений. На рисунке 20 показано пространство присвоений U и его решеточная структура для $n = 2$, $m = 2$, $x_1 = 0$ и $x_2 = 1$. Отметим, что решётка включает как неполные, так и бессмысленные присвоения.

Используя стандартное соответствие между множествами занумерованных элементов и двоичными последовательностями, в которых 1 на n-м месте соответствует включению n-го элемента, а 0 — исключению, этим множествам

можно поставить в соответствие стандартные базисные векторы квантового пространства состояний. Например, рисунок 5 отображает решётку рисунка 4, переписанную в кет обозначениях, где элементы были перечислены в следующем порядке: $v_1 = 0$, $v_1 = 1$, $v_2 = 0$ и $v_2 = 1$.

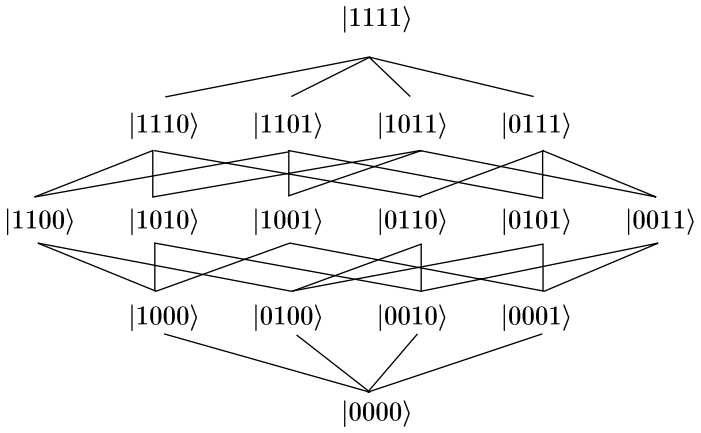
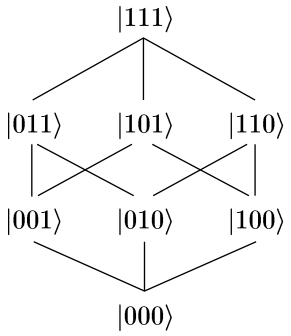


Рис. 5. Решётка переменных присвоений в кет-форме

Если хотя бы одно состояние нарушает ограничение, то все состояния решётки, находящиеся выше него, тоже нарушают ограничения. Подход, который Хогг применяет при построении квантовых алгоритмов для ограниченно выполняемых задач, состоит в следующем. Сначала амплитуда сосредоточена в состоянии $|0 \ldots 0\rangle$, затем она итерационно передвигается вверх по решётке от множеств к супермножествам, удаляясь от множеств, которые нарушают ограничения. Следует отметить, что в отличие от алгоритмов Шора и Гровера, которые начинаются с вычисления функции в суперпозиции всех выходных значений одновременно, этот алгоритм начинается совсем по-другому.

Хогг представляет два пути [Hogg 1996; Hogg 1998] построения унитарной матрицы для передвижения амплитуды вверх по решётке. Мы опишем оба способа, а затем то, как он отодвигает амплитуду от «плохих» множеств.

Движение амплитуды вверх: способ 1. Существует простое преобразование, которое передвигает амплитуду от множеств к супермножествам. Любая амплитуда, связанная с пустым множеством одинаково распределяется среди всех множеств с единичными элементом. Любая амплитуда, связанная с одноэлементным множеством одинаково распределяется среди всех двухэлементных множеств, которые содержат этот элемент и т. д (см. рисунок для решётки трехэлементного множества).



Нам необходимо преобразовать

$$|000\rangle \to 1/\sqrt{3}(|001\rangle + |010\rangle + |100\rangle)$$
$$|001\rangle \to 1/\sqrt{3}(|011\rangle + |110\rangle + |101\rangle)$$
$$\ldots$$

Вот как выглядит матрица этого преобразования (как обычно, базисные векторы расположены в соответствии со своим двоичным представлением)

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
\frac{1}{\sqrt{3}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{1}{\sqrt{3}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 \\
\frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \frac{1}{\sqrt{3}} & 0 & 0 & \frac{1}{\sqrt{2}} & 0 & 0 & 0 \\
0 & 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 0
\end{pmatrix}$$

К сожалению это преобразование не является унитарным. Хогг [Hogg 1996] опирается на тот факт, что ближайшая (в соответствующей метрике) унитарная матрица U_m к произвольной матрице M может быть найдена с использованием разложения $M = UDV^T$, где D — диагональная матрица, а U и V унитарные матрицы. Произведение $U_M = UV^T$ представляет ближайшую к M унитарную матрицу. Поскольку U_m находится достаточно близко к M, то U_m будет вести себя примерно как M, и таким образом будет передвигать амплитуду от множеств к супермножествам.

Движение амплитуды вверх: способ 2. В этом подходе используется [Hogg 1998] преобразование Уолша – Адамара. Хогг полагает, что требуемая матрица имеет форму WDW, где W это преобразование Уолша – Адамара, а D —

диагональная матрица, чьи элементы зависят только от размера множеств. Хогг рассчитывает элементы D, которая максимизирует движение амплитуды от множества к своему супермножеству. В этих расчетах используется свойство

$$W_{rs} = \frac{1}{\sqrt{N}}(-1)^{|r \cdot s|} = \frac{1}{\sqrt{N}}(-1)^{|r \cap s|},$$

упоминаемое в подразделе 7.2.1.

Сдвиг амплитуды от «плохих» множеств. Чтобы отодвигать амплитуды от множеств, которые нарушают ограничения, Хогг предлагает регулирование фаз множеств, исходя из значений пределов, при которых они могут нарушать ограничения. При этом амплитуда, распределённая по множествам, которые обладают «плохими» подмножествами уничтожается, а амплитуда, распределённая по множествам от всех «хороших» подмножеств увеличивается.

В зависимости от конкретной задачи различные способы будут работать здесь более или менее эффективно. В одном из способов он предлагает инверсию фазы всех «плохих» множеств, которые приводят к сокращениям в амплитуде супермножеств, исходящих от «хороших» и «плохих» множеств. Эта фазовая инверсия может быть реализована подобно тому, как это делается в алгоритме Гровера (7.1.2) с некоторым P, которое проверяет, удовлетворяет ли данное состояние всем условиям ограничения или нет. Другое предложение состоит, в том, чтобы предать произвольные фазы «плохим» множествам, так, чтобы в среднем вклад в амплитуду супермножества от «плохих» подмножеств был нулевым. Возможны и другие подходы.

Из-за того, что сокращение, возникающее в результате фазового изменения, является разным для разных задач, вероятность получения решения трудно поддается анализу. Было проделано несколько небольших экспериментов, и вывод можно сделать такой: цена поиска всё же возрастает экспоненциально, хотя и значительно медленней, чем при случае неупорядоченном поиске. И пока не будет создано достаточного больших квантовых компьютеров или лучших приёмов для анализа квантовых алгоритмов, определить эффективность будет сложно.

8. Исправление квантовых ошибок

Изоляция квантового состояния — основная проблема, препятствующая созданию квантовых компьютеров. Взаимодействие частиц, представляющих кубиты, с внешней средой возмущает квантовое состояние, нарушая когерентность, преобразует его непредсказуемым образом, иногда даже не унитарно.

Стин [Stean 1998] оценил, что декогерентность любой из предложенных систем на 7 порядков больше той, что необходима для нормальной работы алгоритма Шора с числами, содержащими 130 десятичных разрядов. Однако, добавление так называемой коррекции ошибок снижает влияние декогерентности, и снова даёт надежды на осуществление алгоритма Шора для больших чисел.

На первый взгляд, квантовая коррекция ошибок очень похожа на классическую, где тоже вводятся дополнительные биты для обнаружения и исправления

ошибок. Но, конечно, квантовая коррекция ошибок гораздо сложнее, ведь мы имеем дело не с двоичными данными, а с квантовыми состояниями.

Квантовая коррекция ошибок должна воссоздавать точно некоторое квантовое состояние. Трудности здесь связаны с невозможностью клонирования или копирования. Однако, оказывается, эти трудности преодолимы, и квантовые ошибки всё-таки можно исправлять.

8.1. Описание ошибок

Будем полагать, что все ошибки являются результатом квантового взаимодействия кубитов и окружающей среды. Возможные ошибки для каждого отдельного кубита, будем представлять линейными комбинациями операторов: (I) (отсутствие ошибки), (X) (инверсия), (Z)(фазовая ошибка), (Y) (инверсия и фазовая ошибка). Таким образом, общее выражение однокубитовой ошибки есть некоторое преобразование вида: $e_1 I + e_2 X + e_3 Y + e_4 Z$. Взаимодействие с окружающей средой преобразует отдельные кубиты согласно выражению

$$|\psi\rangle \to (e_1 I + e_2 X + e_3 Y + e_4 Z)|\psi\rangle = \sum_i e_i E_i |\psi\rangle.$$

Для больших квантовых регистров ошибки так же выражаются линейными комбинациями унитарных операторов ошибок E_i. Эти операторы являются тензорными произведениями операторов ошибок отдельных кубитов $\{I,\ X,\ Y,\ Z\}$ или более общих многокубитовых операторов ошибок. В любом случае, ошибку можно записать как $\sum_i e_i E_i$.

8.2. Восстановление квантового состояния

В классическом случае, корректирующий код для некоторого набора ошибок E_i состоит из преобразования C, которое отображает n битов данных в $(n+k)$-битный код, а так же из преобразования выделения ошибки S_c, которое отображает $(n+k)$-битный код в индекс i корректируемой ошибки E_i, то есть $i = S_c\big(E_i(C(x))\big)$. Если $y = E_j\big(C(x)\big)$ для некоторой корректируемой ошибки, то $S_c(y)$ можно использовать для восстановления значения $C(x)$, а именно $E^{-1}_{S_{C(y)}}(y) = C(x)$.

Теперь рассмотрим квантовый случай. Во-первых, состояние регистра может быть суперпозицией базисных векторов. Во вторых, ошибка может быть линейной комбинацией операторов корректируемых ошибок E_i. При этом оказывается, что восстановление закодированного квантового состояния всё же является возможным.

Зададим корректирующий код C и преобразование выделения ошибки S_c. Таким образом, n-битное квантовое состояние $|\psi\rangle$ закодировано в $(n+k)$-битном квантовом состоянии $|\varphi\rangle = C|\psi\rangle$.

Допустим, что декогентность приводит к состоянию $\sum_i e_i E_i|\varphi\rangle$ для некоторой комбинации корректируемых ошибок E_i. Первоначальное состояние $|\varphi\rangle$ можно восстановить следующим образом

(1) Применяем оператор выделения признака ошибки S_c к квантовому состоянию с добавлением достаточного количества вспомогательных $|0\rangle$ кубитов

$$S_C\left(\sum_i e_i E_i|\varphi\rangle\right)\otimes|0\rangle=\sum_i e_i\Big(E_i|\varphi\rangle\otimes|i\rangle\Big).$$

Квантовый параллелизм дает суперпозицию различных ошибок (индексируемых через i).

(2) Измеряем компоненту $|i\rangle$ результата. Это даст некоторую (случайную) величину i_0 и спроектирует состояние на

$$E_{i_0}|\varphi,\, i_0\rangle.$$

(3) Применяем обратное преобразование для ошибки $E_{i_0}^{-1}$ к первым $n+k$ кубитам состояния $E_{i_0}|\varphi,\, i_0\rangle$, чтобы получить исходное состояние $|\varphi\rangle$.

Заметим, что на шаге (2) суперпозиция нескольких ошибок проектируется на отдельную ошибку. Следовательно, для шага (3) необходимо только одно обратное преобразование ошибки.

8.3. Пример коррекции ошибок

Рассмотрим тривиальный корректирующий код C, отображающий $|0\rangle\to|000\rangle$ и $|1\rangle\to|111\rangle$. С помощью C мы можем корректировать ошибку инверсии отдельного кубита

$$E=\{I\otimes I\otimes I, X\otimes I\otimes I,\; I\otimes X\otimes I,\; I\otimes I\otimes X\}.$$

Оператор выделения ошибки есть

$$S\colon |x_0,\, x_1,\, x_2,\, 0,\, 0,\, 0\rangle\to|x_0,\, x_1,\, x_2,\, x_0 \text{ xor } x_1,\, x_0 \text{ xor } x_2,\, x_1 \text{ xor } x_2\rangle,$$

с соответствующими операторами коррекции ошибки, представленными в таблице ниже (заметим, что для этого примера $E_i=E_i^{-1}$).

Инвертированный бит	Признак ошибки	Коррекция ошибки
—	$\|000\rangle$	—
0	$\|110\rangle$	$X\otimes I\otimes I$
1	$\|101\rangle$	$I\otimes X\otimes I$
2	$\|011\rangle$	$I\otimes I\otimes X$

Рассмотрим квантовый бит $|\psi\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$, кодируемый следующим образом

$$C|\psi\rangle=|\varphi\rangle=\frac{1}{\sqrt{2}}\big(|000\rangle-|111\rangle\big)$$

и ошибку

$$E=\frac{4}{5}X\otimes I\otimes I+\frac{3}{5}I\otimes X\otimes I.$$

Состояние с ошибкой имеет вид

$$E|\varphi\rangle = \left(\frac{4}{5}X\otimes I\otimes I + \frac{3}{5}I\otimes X\otimes I\right)\left(\frac{1}{\sqrt{2}}\left(|000\rangle - |111\rangle\right)\right) =$$
$$= \frac{4}{5}X\otimes I\otimes I + \frac{3}{5}I\otimes X\otimes I\left(\frac{1}{\sqrt{2}}\left(|000\rangle - |111\rangle\right)\right) =$$
$$= \frac{4}{5\sqrt{2}}X\otimes I\otimes I\big(|000\rangle - |111\rangle\big) + \frac{3}{5\sqrt{2}}I\otimes X\otimes I\big(|000\rangle - |111\rangle -\big) =$$
$$= \frac{4}{5\sqrt{2}}\big(|100\rangle - |011\rangle\big) + \frac{3}{5\sqrt{2}} - \big(|010\rangle - |101\rangle\big).$$

Затем к выражению $\big(E|\varphi\rangle\big)\otimes|000\rangle$ применим оператор определения признака ошибки:

$$S_C\left(\left(E|\varphi\rangle\right)\otimes|000\rangle\right) = S_C\left(\frac{4}{5\sqrt{2}}\big(|100000\rangle - |011000\rangle\big) + \frac{3}{5\sqrt{2}}\big(|010000\rangle - |101000\rangle\Big) =\right.$$
$$= \frac{4}{5\sqrt{2}}\big(|100110\rangle - |011110\rangle\big) + \frac{3}{5\sqrt{2}}\big(|010101\rangle - |101101\rangle\big)$$
$$= \frac{4}{5\sqrt{2}}\big(|100\rangle - |011\rangle\big)\otimes|110\rangle + \frac{3}{5\sqrt{2}}\big(|010\rangle - |101\rangle\big)\otimes|101\rangle.$$

Измерив последние три бита этого состояния, получим либо $|110\rangle$, либо $|101\rangle$. Учитывая возможный результат измерения, запишем состояние как

$$\frac{1}{\sqrt{2}}\big(|100\rangle - |011\rangle\big)\otimes|110\rangle.$$

Измерение обладает удивительным свойством вызывать исчезновение всех ошибок в сумме, кроме одной. От оставшейся ошибки можно избавиться применив к первым трём битам обратный оператор оператора ошибки $X\oplus I\oplus I$, соответствующий измеренному значению $|110\rangle$. Тогда мы получим

$$\frac{1}{\sqrt{2}}\big(|000\rangle - |111\rangle\big) = C|\psi\rangle = |\varphi\rangle.$$

9. Выводы

Квантовые вычисления — это новейшее направление, способное в корне изменить наши представления о вычислениях, программировании и теории сложности. Разработка новых приёмов программирования для квантовых компьютеров — важнейшая задача для программистов и других специалистов. Квантовая запутанность и фазовые компенсация открывают принципиально новые вычислительные возможности. Программирование больше не состоит из простого пошагового составления алгоритма, а требует новых приёмов, например фазовых

преобразований, смешивания и распределения амплитуд для получения полезных выходных данных.

Мы попытались представить подробное описание положения вещей в области квантовых вычислений для программистов и других специалистов, приступающих к изучению данной области науки.

Мы описали некоторые из квантово-механических эффектов, такие, как экспоненциальность пространства состояний, запутанность состояний, линейность квантовых преобразований, которые и делают квантовый параллелизм возможным.[1] Несмотря на то, что квантовые вычисления должны быть линейными и обратимыми, любой классический алгоритм может быть реализован на квантовом компьтере. Но настоящая мощь этих новых машин, т. е. экспоненциальный параллелизм, может быть использована только с применением новаторских методов программирования. Такие методы начали разрабатываться лишь недавно.

Мы описали алгоритм Шора разложения чисел на множители за полиномиальное время, который стимулировал исследования в области квантовых вычислений. Алгоритм Шора, при наличии действующего квантового компьютера, отправит в небытиё многие современные криптографические системы. Алгоритм поиска, разработанный Гровером, может обеспечить лишь полиномиальное ускорение, но и этот факт строго доказывает, что квантовые компьютеры значительно мощнее классических. Несмотря на то, что алгоритм Гровера является оптимальным, существует надежда создать более быстрые алгоритмы для задач упорядоченного поиска. Мы описали один из подходов к созданию таких алгоритмов, предложенный Хоггом.

Существует ещё несколько известных квантовых алгоритмов, о которых мы не говорили. Джонс и Моска [Jones and Nosca 1998] описали реализацию алгоритма на 2-х битном квантовом компьютере, при помощи которого можно определить, сбалансирована ли функция или нет. Гровер [Grover 1998] разработал эффективный алгоритм для оценки среднего значения некоторого множества. Позже Гровер, Смолин и Терал предложили квантовый способ решения задачи о взвешивании монеты за один шаг. Несмотря на наличие этих алгоритмов, нам всё-таки ещё не так много известно о том, что может делать квантовый компьютер на практике. Сможем ли мы найти квантовые алгоритмы, которые обеспечат экспоненциальное ускорение при решении других задач, а не только факторизации?

Этот вопрос остается открытым. Среди физиков ходят предположения о том, что квантовые преобразования могут быть слегка нелинейными. До настоящего момента все проведённые эксперименты согласуются с законами стандартной линейной квантовой механики, но небольшая нелинейность все же возможна. Абрамс и Ллойд [Abrams and Lloyd 1998] доказали, что даже небольшая нелинейность может быть использована для решения сложных NP-задач на квантовом

[1] Экспоненциальное квантовое ускорение проистекает из экспоненциальности пространства состояний. Требования же линейности и обратимости, которые были присущи рассмотренным в статье системам, вообще говоря, не обязательны. См., например, статью D. Aharonov, A. Kitaev, N. Nisan «Quantum Circuits with Mixed States» (№ 9806029 в электронном архиве http://xxx.itep.ru/quant-ph). — *Прим. перев.*

компьютере за полиномиальное время. По сути своей, это значит, что вычисления — это фундаментальные физические процессы, и что вопросы их эффективности напрямую зависят от тонких физических явлений.

Уникальные свойства квантовых компьютеров дают новое представление о классах сложности. Например, класс BQP — это набор всех языков, обрабатываемых квантовой машиной Тьюринга за полиномиальное время с конечной вероятностью. Детали исследований, проводимых в области квантовой теории сложности, находятся за рамками данной статьи. Читатели, заинтересовавшиеся анализом временной и пространственной сложности в квантовых вычислениях, могут найти интересующую их информацию в статьях [Bennett 1997] и [Wootters 1998]. В статье [Williams and Clearwater 1998] содержится описание первых результатов исследований в области квантовой теории сложности.

Конечно, пока существуют очень сложные физические проблемы, которые нужно будет преодолеть. Без этого нельзя будет построить практически полезный работающий квантовый компьютер. Декогерентность, т.е. искажение квантового состояния из-за взаимодействия с окружающей средой — ключевая проблема. С развитием квантовой коррекции ошибок в области устранения декогерентности был совершен прорыв, но больше с алгоритмической стороны, чем с физической. Мы уже описали некоторые из применяемых методов коррекции ошибок. Дальнейшие продвижения в области квантовой коррекции ошибок и развитие устойчивых к ошибкам алгоритмов будут также важны для развития квантовых компьютеров, как и успехи в создании квантовых битов.

9.1. Рекомендуемая литература

Обзорная статья Эндрю Стина «Квантовые вычисления» [Stean 1998] предназначена для физиков.

Мы рекомендуем прочитать эту статью, чтобы познакомиться с его точкой зрения по этим вопросам, особенно с его описанием связи между теорией информации и квантовыми вычислениями, а также с его взглядами на теорию коррекции квантовых ошибок, ведь он был одним из главных её основателей. Там дан обзор физических явлений, понимание которых необходимо для создания квантового компьютера. Этот обзор он сделал в июле 1997 года. В его статье более подробно, чем в нашей, описана история развития квантовых вычислений. Также в ней много полезных ссылок. Другие, небольшие, но интересные пособия, можно найти в [Berthiaume 1997].

Лекции по теории вычислений Ричарда Фейнмана [Feynman 1996] содержат перепечатку его лекции *Квантово-механические компьютеры* [Feynman 1985], которая и положила начало всему направлению. В ней также обсуждается термодинамика вычислений, которая непосредственно связана с обратимыми вычислениями и теорией информации.

Книга Колина Уильямса и Скотта Клеаруотера *Исследования в области квантовых вычислений* [Williams ans Clearwater 1998] снабжена программами в виде файлов для пакета «Mathematica», которые моделируют некоторые из квантовых алгоритмов, например, алгоритм Шора.

Вторая часть номера журнала «SIAM Journal of Computing» за октябрь 1997 года содержит 6 полезных лекций по квантовым вычислениям, включая те четыре лекции, на которые мы уже ссылались [Bennett et al. 1997] [Bernstein and Vazirani 1997] [Shor 1997] [Simon 1997].

Большую часть статей, упоминаемых в данной работе, а также многие другие, можно найти на сервере препринтов в Лос Аламосе:[1]

http://xxx.lanl.gov/archive/quant-ph.

Ссылки на исследовательские проекты и другую информацию о квантовых вычислениях можно найти и на нашей странице в Интернет:

http://www.pocs.com/qc.html.

Литература

D. S. Abrams and S. Lloyd, 1998. Nonlinear quantum mechanics implies polynonualtime solution for NP-complete and #p problems. Los Alamos Physics Preprint Archive, http://xxx.lanl.gov/abs/quant-ph/9801041.

A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. H. Margolus, P. W. Shop, T. Sleator, J. A. Smolin, and H. Weinfurter, 1995. Elementary gates for quantum computation. Physical Review A 52, 5, 3457–3467. Preprint at Los Alamos Physics Preprint Archive, http://xxx.lanl.gov/abs/quant-ph/9503016 and at http://vesta.physics.ucla.edu/cgi-bin/uncompress-ps-cgi?torgatsl.ps.

C. H. Bennett, 1992. Quantum cryptography using any two nonorthogonal states. Physical Review Letters 68.

C. H. Bennett, E. Bernstein, G. Brassard, and U. V. Vazirani, 1997. Strengths and weaknesses of quantum computing. Society for Industrial and Applied Mathematics Journal on Computing 26, 5, 1510–1523. Preprint at Los Alamos Physics Preprint Archive, http://xxx.lanl.gov/abs/quant-ph/9701001.

C. H. Bennett and G. Brassard, 1987. Quantum public key distribution reinvented. SIGACTN: SIGACT News (ACM Special Interest Group on Automata and ComputabHity Theory) 18.

C. H. Bennett, G. Brassard, A. K. Andekert, 1992. Quantum cryptography. Scientific American 267,4 (Oct.), 50.

E. Bernstein and U. V. Vazirani, 1997. Quantum complexity theory. Society for Industrial and Applied Mathematics Journal on Computing 26, 5, 1411–1473. A preliminary version of this paper appeared in the Proceedings of the 25th Association for Computing Machinery Symposium on the Theory of Computing.

Berthiaume. 1997. Quantum computation. In Alan L. Selman, Editor, Complexity Theory Retrospective, In Honor of Juris Hartmanis on the Occasion of His Sixtieth Birthday, July 5, 1988, Volume 2.

[1] Читателям, находящимся в России, имеет смысл обращаться к московскому зеркалу этого архива http://xxx.itep.ru/quant-ph. — *Прим. перев.*

D. Biron, O. Biham, E. Biham, M. Grassel and D. A. Lidar 1998. Generalized grover search algorithm for arbitrary initial amplitude distribution. Los Alamos Physics Preprint Archive. http://xxx.lanl.gov/abs/quant-ph/9801066.

D. Boschi, S. Branca, F. D. Martini, L. Hardy and S. Popescu, 1998. Experimental realization of teleporting an unknown pure quantum state via dual classical and einstein-podolski-rosen channels. Physical Review Letters 80, 1121–1125.

D. Bouwmeester, J.-W. Pan, K. Mattle, M. Elbl, H. Weinfurter, A. Andzeilinger, 1997. Experimental quantum teleportation. Nature 390, 575.

M. Boyer, G. Brassard, P. Hoyer and A. Tapp, 1996. Tight bounds on quantum search. In Proceedings of the Workshop on Physics of Computation: PhysComp '96 (Los Alamitos, CA, 1996). Institute of Electrical and Electronic Engineers Computer Society Press. Preprint at Los Alamos Physics Preprint Archive, http://xxx.lanl.gov/abs/quant-ph/9605034.

G. Brassard, P. Hoyer and A. Tapp, 1998. Quantum counting. Preprint at Los Alamos Physics Preprint Archive, http://xxx.lanl.gov/abs/quant-ph/9805082.

N. J. Cerf, L. K. Grover and C. P. Williams, 1998. Nested quantum search and np-complete problems. Preprint at Los Alamos Physics Preprint Archive, http://xxx.lanl.gov/abs/quant-ph/9806078.

J. I. Cirac and P. Zoller, 1995. Quantum computations with cold trapped ions. Physical Review Letters 74, 4091–4094.

D. G. Cory, W. Mass, M. Price, , E. Knill, R. Laflamme, W. H. Zurek, T. P. Havel and S. S. Somaroo, 1998. Experimental quantum error correction. Preprint at Los Alamos Physics Preprint Archive, http://xxx.lani.gov/abs/quant-ph/9802018.

D. Deutsch, 1985. Quantum theory, the Church-Turing principle and the universal quantum computer. Proceedings of the Royal Society of London Ser. A A400, 97–117.

D. Deutsch and R. Jozsa, 1992. Rapid solution of problems by quantum computation. Proceedings of the Royal Society of London Ser. A A439, 553–558.

P. Dirac, 1958. The Principles of Quantum Mechanics (4th ed.). Oxford University Press.

A. K. Ekert, J. Rarity, P. Tapster and G. Palma, 1992. Practical quantum cryptography based on two-photon interferometry. Physical Review Letters 69.

R. Feynman, 1982. Simulating physics with computers. International Journal of Theoretical Physics 21, 6&7, 467–488.

R. Feynman, 1985. Quantum mechanical computers. Optics News 11. Also in Foundations of Physics, 16(6) : 507–531, 1986.

R. Feynman, 1996. In A. J. Hey and R. W. Allen Eds., Feynman Lectures on Computation. Addison-Wesley.

R. P. Feynman, R. B. Leighton and M. Sands, 1965. Lectures on Physics, Vol. III. Addison-Wesley.

N. A. Gershenfeld and I. L. Chuang, 1997. Bulk spin resonance quantum computing. Science 275, 350–356.

G. Greenstein and A. G. Zajonc, 1997. The Quantum Challenge. Jones and Bartlett Publishers, Sudbury, Mass.

L. K. Grover, 1996. A fast quantum mechanical algorithm for database search. In Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing (Philadelphia, Pennsylvania, 22–24 May 1996), pp. 212–219.

L. K. Grover, 1998. A framework for fast quantum mechanical algorithms. Proceedings of the 30th annual ACM symposium on the theory of computing, 53–62. Preprint at Los Alamos Physics Preprint Archive, http: //xxx.lanl.g6v/abs/quant-ph/9711043.

G. H. Hardy, and E. M. Wright, 1979. An Introduction to the Theory of Numbers. Oxford University Press.

T. Hogg, 1996. Quantum computing and phase transitions in combinatorial search. Journal of Artificial Intelligence Research 4, 91–128. Preprint at Los Alamos Physics Preprint Archive, http://xxx.lanl.gov/abs/quant-ph/9508012,

T. Hogg, 1998. Highly structured searches with quantum computers. Physical Review Letters 80, 2473–2473.

R. J. Hughes, W. T. Buttler, P. G. Kwiat, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, and C. G. Peterson, 1999. Practical quantum cryptography for secure free-space communications. Preprint at Los Alamos Physics Preprint Archive, http://xxx.lanl.gov/abs/quant-ph/9905009.

R. J. Hughes, W. T. Buttler, P. G. Kwiat, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson and C. M. Simmons, 1997. Secure communications using quantum cryptography. In S. P. Hotaling and A. R. Pirich Eds., Photonic Quantum Computing, Volume 3076 (1997), pp. 2–11.

T. A. Hungerford, 1974. Algebra. Springer Verlag, New York, Heidelberg, Berlin.

J. A. Jones and M. Mosca, 1998. Implementation of a quantum algorithm on a nuclear magnetic resonance quantum computer. Journal of Chemical Physics 109, 5, 1648–1653. Preprint at Los Alamos Physics Preprint Archive, http://xxx.lani.gov/abs/quant-ph/9801027.

R. Laflamme, E. Knill, W. Zurek, P. Catasti and S. Mariappan, 1997. NMR GHZ. Los Alamos Physics Preprint Archive, http://xxx.lani.gov/abs/quant-ph/9709025.

A. Lenstra and H. Lenstra, Eds. 1993. The Development of the Number Field Sieve, Volume 1554 of Lecture Notes in Mathematics. Springer Verlag.

R. L. Liboff, 1997. Introductory Quantum Mechanics (3rd edition). Addison-Wesley, Reading. Mass.

H.-K. Lo and H. F. Chau, 1999. Unconditional security of quantum key distribution over arbitrarily long distances. Science 283, 2050–2056.

D. Mayers, 1998. Unconditional security in quantum cryptography. Preprint at Los Alamos Physics Preprint Archive, http://xxx.lanl.gov/abs/quant-ph/9802025.

M. A. Nielsen, E. Knill and R. Laflamme, 1998. Complete quantum teleportation using nuclear magnetic resonance. Preprint at Los Alamos Physics Preprint Archive, http://xxx.lanl.gov/abs/quant-ph/9811020.

L. J. Schulman and U. Vazirani, 1998. Scalable NMR quantum computation. Los Alamos Physics Preprint Archive, http://xxx.lani.gov/abs/quant-ph/9804060.

P. W. Shor, 1994. Algorithms for quantum computation: Discrete log and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science (Nov. 1994). pp. 124–134. Institute of Electrical and Electronic Engineers Computer Society Press,
ftp://netlib.att.com/netlib/att/math/shor/quantum.algorithms.ps.Z.

P. W. Shor, 1997. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. Society for Industrial and Applied Mathematics Journal on Computing 26, 5, 1484–1509. Expanded version of [Shor 1994].

D. R. Simon, 1997. On the power of quantum computation. Society for Industrial and Applied Mathematics Journal on Computing 26, 5, 1474–141483. A preliminary version of this paper appeared in the Proceedings of the 35th Annual Symposium on Foundations of Computer Science.

A. Steane, 1996. The ion trap quantum information processor. Los Alamos Physics Preprint Archive,
http://xxx.lanl.gov/abs/quant-ph/9608011.

A. Steane, 1998. Quantum computing. Reports on Progress in Physics 61, 2, 117–173. Preprint at Los Alamos Physics Preprint Archive,
http://xxx.lani.gov/abs/quant-ph/9708022.

B. M. Terhal and J. A. Smolin, 1997. Single quantum querying of a database. Los Alamos Physics Preprint Archive, http://xxx.lani.gov/abs/quant-ph/9705041.

L. M. K. Vandersypen, C. Y. Yannoni, M. H. Sherwood and I. L. Chuang, 1999. Realization of effective pure states for bulk quantum computation. Preprint at Los Alamos Physics Preprint Archive, http://xxx.lanl.gov/abs/quant-ph/9905041.

V. Vedral, A. Barenco and A. K. Ekert, 1996. Quantum networks for elementary arithmetic operations. Physical Review A. Preprint at Los Alamos Physics Preprint Archive, http://xxx.lani.gov/abs/quant-ph/9511018.

J. Watrous, 1998. Relationships between quantum and classical space-bounded complexity classes. In Thirteenth Annual IEEE Conference on Computational Complexity (June 1998).

C. P. Williams and S. H. Clearwater, 1998. Explorations in Quantum Computing. Telos, Springer-VerIag.

W. K. Wootters and W. H. Zurek, 1982. A single quantum cannot be cloned. Nature 299, 802.

C. Zalka, 1997. Grover's quantum searching algorithm is optimal. Los Alamos Physics Preprint Archive, http://xxx.lani.gov/abs/quant-ph/9711070.

Благодарности

Особо мы хотели бы поблагодарить Теда Хогга и Карлоса Макона за интересные беседы о квантовых вычислениях и за оказание помощи в написании этой статьи. Мы также благодарны Ли Корбину, Девиду Голдбергу, Лову Гроверу, Норману Харди, Воганну Протту, Марку Рифелю и экспертам, пожелавшим остаться неизвестными, за подробные комментарии при подготовке статьи.

И конечно мы хотели бы выразить свою благодарность сотрудникам FXPAL, которые с энтузиазмом поддерживали нашу работу.

Приложение

A. Тензорные произведения

Тензорное произведение ($\otimes$) n-мерного и k-мерного векторов есть nk-мерный вектор. Следовательно, если A и B являются преобразованиями над n-мерным и k-мерным векторами соответственно, тогда $A \otimes B$[1] есть преобразование над nk-мерными векторами.

Подробный математический анализ тензорных произведений в этой статье не проводится (подробности см. в [Hungerford 1974]). Для наших целей достаточно будет нескольких алгебраических правил, чтобы вести расчёты с тензорными произведениями. Для матриц A, B, C, D, U, векторов u, x, y скаляров a, b выполняются следующие условия:

$$\begin{aligned}
(A \otimes B)(C \otimes D) &= AC \otimes BD \\
(A \otimes B)(x \otimes y) &= Ax \otimes By \\
(x + y) \otimes u &= x \otimes u + y \otimes u \\
u \otimes (x + y) &= u \otimes x + u \otimes y \\
ax \otimes by &= ab(x \otimes y) \\
\begin{pmatrix} A & B \\ C & D \end{pmatrix} \otimes U &= \begin{pmatrix} A \otimes U & B \otimes U \\ C \otimes U & D \otimes U \end{pmatrix},
\end{aligned}$$

в частности, для скаляров a, b, c, d

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes U = \begin{pmatrix} aU & bU \\ cU & dU \end{pmatrix}.$$

[1] Фактически это правое произведение Кронекера.

Комплексное сопряжение и транспонирование дистрибутивно над тензорными произведениями, т.е.

$$(A \otimes B)^* = A^* \otimes B^*.$$

Матрица U является унитарной, если матрица, сопряженная ей и транспонированная, является обратной к ней: $U^*U = I$. Тензорное произведение нескольких матриц является унитарным, тогда и только тогда, когда каждая матрица из этого произведения унитарна с точностью константы. Пусть $U = A_1 \otimes A_2 \otimes \ldots A_n$. Тогда матрица U унитарна, если $A_i^* A_i = k_i I$ и $\Pi_i k_i = 1$:

$$\begin{aligned} U^*U &= (A_1^* \otimes A_2^* \otimes \ldots \otimes A_n^*)(A_1 \otimes A_2 \otimes \ldots \otimes A_n) = \\ &= A_1^* A_1 \otimes A_2^* A_2 \otimes \ldots \otimes A_n^* A_n = \\ &= k_1 I \otimes \ldots k_n I = I, \end{aligned}$$

где каждое I является тождественной матрицей соответствующей размерности.

Например, дистрибутивный закон позволяет проводить вычисления следующего вида:

$$\begin{aligned} &(a_0|0\rangle + b_0|1\rangle) \otimes (a_1|0\rangle + b_1|1\rangle) = \\ &\quad = (a_0|0\rangle \otimes a_1|0\rangle) + (b_0|1\rangle \otimes a_1|0\rangle) + (a_0|0\rangle \otimes b_1|1\rangle) + (b_0|1\rangle \otimes b_1|1\rangle) = \\ &\quad = a_0 a_1((|0\rangle \otimes |0\rangle) + b_0 a_1(|1\rangle \otimes |0\rangle) + a_0 b_1(|0\rangle \otimes |1\rangle) + b_0 b_1(|1\rangle \otimes |1\rangle) = \\ &\quad = a_0 a_1(|00\rangle + b_0 a_1|10\rangle + a_0 b_1|01\rangle) + a_0 b_1|11\rangle. \end{aligned}$$

B. Непрерывные дроби и извлечение периода из измерения в алгоритме Шора

В общем случае, когда период r не делит 2^m, величина v, измеренная в 4-м шаге алгоритма Шора, с большой вероятностью будет близка к некоторому числу, кратному $\frac{2^m}{r}$, например $j\frac{2^m}{r}$. Целью является извлечение периода r из измеренной величины v. Шора показал, что с большой вероятностью величина v удалена не более, чем на $\frac{1}{2}$ от $j\frac{2^m}{r}$. Таким образом,

$$\left| v - j\frac{2^m}{r} \right| < \frac{1}{2}$$

для некоторой величины j, откуда следует

$$\left| \frac{v}{2^m} - \frac{j}{r} \right| < \frac{1}{2 \cdot 2^m} < \frac{1}{2M^2}.$$

Разница между двумя дробями $\frac{p}{q}$ и $\frac{p'}{q'}$, со знаменателями, меньшими M, ограничена:

$$\left| \frac{p}{q} - \frac{p'}{q'} \right| = \left| \frac{pq' - p'q}{qq'} \right| > \frac{1}{M^2}.$$

Таким образом существует, по крайней мере, одна дробь $\frac{p}{q}$ со знаменателем $q < M$, такая что $\left|\frac{v}{2^m} - \frac{p}{q}\right| < \frac{1}{M^2}$. В наиболее вероятном случае, когда v удалена не более чем на $\frac{1}{2}$ от $j\frac{2^m}{r}$, эта дробь будет равна $\frac{j}{r}$.

Единственная дробь со знаменателем меньшим M, т.е. удалённая не более чем на $\frac{1}{M^2}$ от $\frac{v}{2^m}$, может быть получена эффективным способом с помощью разложения в бесконечную дробь $\frac{v}{2^m}$. Используя последовательности

$$a_0 = \left[\frac{v}{2^m}\right] \qquad \epsilon_0 = \frac{v}{2^m} - a_0$$
$$a_n = \left[\frac{1}{\epsilon_n - 1}\right] \qquad \epsilon_n = \frac{1}{\epsilon_n - 1} - a_n$$
$$p_0 = a_0 \qquad p_1 = a_1 a_0 + 1 \qquad p_n = a_n p_{n-1} + p_{n-2}$$
$$q_0 = 1 \qquad q_1 = a_1 \qquad q_n = a_n q_{n-1} + q_{n-2},$$

вычислим первую дробь $\frac{p_n}{q_n}$ такую, что $q_n < M \leqslant q_{n+1}$. Доказательство правильности этого метода см. в любой книге по теории чисел. В наиболее вероятном случае, когда $\frac{v}{2^m}$ удалена не более чем на $\frac{1}{M^2}$ от $\frac{j}{r}$, кратного $\frac{1}{r}$, дробь, полученная в предыдущей процедуре, есть $\frac{j}{r}$, т.к. она имеет знаменатель, меньший M. Мы принимаем знаменатель q полученной дроби в качестве полученного периода, который будет правильным, когда j и r — взаимно простые.