КРИС БЕРНХАРД

КВАНТОВЫЕ ВЫЧИСЛЕНИЯ ДЛЯ НАСТОЯЩИХ АЙТИШНИКОВ

The MIT Press

Quantum Computing for Everyone

Chris Bernhardt

The MIT Press
Cambridge, Massachusetts
London, England

КРИС БЕРНХАРД

КВАНТОВЫЕ ВЫЧИСЛЕНИЯ ДЛЯ НАСТОЯЩИХ АЙТИШНИКОВ

ПИТЕР®

Санкт-Петербург • Москва • Екатеринбург • Воронеж
Нижний Новгород • Ростов-на-Дону
Самара • Минск

2020

ББК 32.973.2-018+22.31
УДК 004.4:530.145
Б51

Бернхард Крис

Б51 Квантовые вычисления для настоящих айтишников. — СПб.: Питер, 2020. — 240 с.: ил. — (Серия «Библиотека программиста»).

ISBN 978-5-4461-1332-3

Квантовые вычисления часто упоминаются в новостях: Китай телепортировал кубит с Земли на спутник; алгоритм Шора поставил под угрозу ныне используемые методы шифрования; квантовое распределение ключей снова сделает шифрование надежным средством защиты; алгоритм Гровера увеличит скорость поиска данных.

Но что все это означает на самом деле? Как все это работает? Можно ли освоить эту тему без знания математики?

Нет, если вы хотите по-настоящему понять суть происходящего. Основные идеи берут начало в квантовой механике и часто противоречат здравому смыслу. Попытки описать их обычными словами обречены на провал, потому что эти явления не имеют отражения в обыденной жизни. Хуже того, словесные описания часто создают впечатление, что мы что-то поняли, хотя на самом деле все не так плохо — нам не придется сильно углубляться в математику, достаточно того, что пытались вбить в наши головы в старших классах школы.

Квантовые вычисления — это удивительный сплав квантовой физики и информатики, объединяющий самые яркие идеи из физики двадцатого века и позволяющий по-новому взглянуть на компьютерные технологии.

16+ (В соответствии с Федеральным законом от 29 декабря 2010 г. № 436-ФЗ.)

ББК 32.973.2-018+22.31
УДК 004.4:530.145

ISBN 978-0262039253 англ.
ISBN 978-5-4461-1332-3

Оглавление

Посвящается Генрике

Благодарности

За помощь в подготовке этой книги я признателен многим людям. Мэтт Коулман (Matt Coleman), Стив Лемей (Steve LeMay), Дэн Райан (Dan Ryan), Крис Стейкер (Chris Staecker) и три не назвавшихся рецензента с особым тщанием вычитывали разные версии рукописи. Их предложения здорово помогли улучшить книгу. Я также благодарю Мэри Ли (Marie Lee) и ее команду из MIT Press за поддержку и превращение рукописи в книгу.

Введение

Цель этой книги — познакомить с квантовыми вычислениями всех, кто знаком с курсом математики средней школы и готов немного потрудиться. В этой книге мы будем знакомиться с кубитами, запутанностью (квантовых состояний), квантовой телепортацией и квантовыми алгоритмами, а также с другими темами, имеющими отношение к квантовым компьютерам. Задача состоит не в том, чтобы дать смутное представление об этих понятиях, а в том, чтобы сделать их кристально ясными.

Квантовые вычисления часто упоминаются в новостях: Китай телепортировал кубит с Земли на спутник; алгоритм Шора поставил под угрозу ныне используемые методы шифрования; квантовое распределение ключей снова сделает шифрование надежным средством защиты; алгоритм Гровера увеличит скорость поиска данных. Но что все это означает в действительности? Как все это работает? Об этом я и собираюсь рассказать.

Можно ли освоить эту тему без знания математики? Нет, если вы хотите по-настоящему понять суть происходящего. Основные идеи берут начало в квантовой механике и часто противоречат здравому смыслу. Попытки описать их обычными словами обречены на провал, потому что эти явления не имеют отражения в обыденной жизни. Хуже того, словесные описания часто создают впечатление, что мы что-то поняли, хотя на самом деле это не так. Однако все не так плохо — нам не придется сильно углубляться в математику. Моя роль как математика — максимально упростить объяснения, придерживаясь абсолютных основ, и дать элементарные примеры. Тем не менее в этой книге вы встретитесь с математическими идеями, с которыми наверняка не встречались прежде, и, как и все в математике, при первом знакомстве они могут показаться странными. Поэтому для вас важно не пропускать примеры, а внимательно изучить каждый шаг в вычислениях.

Квантовые вычисления — это удивительный сплав квантовой физики и информатики. Они включают в себя ряд самых потрясающих идей

из физики XX века и предлагают совершенно новый взгляд на компьютерные вычисления. Основой квантовых вычислений является кубит. В книге вы узнаете, что такое кубиты и что происходит при их измерении. Классическая единица информации — бит — может иметь только одно из двух значений — 0 или 1. Если бит равен 0, прочитав его, мы получим 0. Если он равен 1, прочитав его, мы получим 1. В обоих случаях состояние бита останется неизменным. В случае с кубитами ситуация совершенно иная. Кубит может иметь одно из бесконечного множества состояний в суперпозиции, как 0, так и 1, — но при попытке измерить его, как в классическом случае, мы просто получим одно из двух значений, 0 или 1. Акт измерения меняет состояние кубита. Такое положение дел достаточно точно описывается простой математической моделью.

Кубиты также могут быть запутанными. Измеряя состояние одного из кубитов, мы влияем на состояние других. Такое явление не встречается в обыденной жизни, но оно прекрасно описывается нашей математической моделью.

Эти три понятия — суперпозиция, измерение и запутанность — являются ключевыми понятиями в квантовой механике. Познакомившись с ними, вы увидите, как их можно использовать в вычислениях. И здесь на сцену выходит человеческая изобретательность.

Математики часто приводят красивые доказательства, содержащие неожиданные идеи. Я буду поступать именно таким образом, освещая разные темы. Теорема Белла, квантовая телепортация, сверхплотная кодировка — все это драгоценности, поджидающие нас впереди. А схема исправления ошибок и алгоритм Гровера вызывают настоящий восторг.

К концу книги вы будете понимать основные идеи, лежащие в основе квантовых вычислений, и познакомитесь с несколькими гениальными и красивыми конструкциями. Вы также узнаете, что квантовые и классические вычисления не являются двумя отдельными дисциплинами: квантовые вычисления являются более фундаментальной формой вычислений, то есть все, что можно вычислить с применением классических подходов, можно вычислить и на квантовом компьютере. Кубит, а не бит — вот базовая единица вычислений. Вычисления, по сути, являются квантовыми вычислениями.

Наконец, хочу особо подчеркнуть, что эта книга рассказывает о теории квантовых вычислений. Речь идет о программном, а не аппаратном обеспечении. Я кратко буду упоминать аппаратную часть в нескольких местах и кое-где буду рассказывать, как физически запутать кубиты, но это лишь побочные темы. В этой книге не рассказывается, как собрать квантовый компьютер, — только как использовать его.

Вот краткое содержание книги.

Глава 1. Базовой единицей классических вычислений является бит. Бит может быть представлен чем угодно, что имеет два возможных состояния. Стандартным примером является электрический выключатель, который может быть включен или выключен. Базовой единицей квантовых вычислений является кубит. Его можно представить как спин электрона или поляризацию фотона, но свойства спина и поляризации нам не так близки, как выключатель, находящийся в одном из состояний.

Мы рассмотрим основные свойства спина, начав с классического эксперимента Отто Штерна (Otto Stern) и Уолтера Герлаха (Walther Gerlach), в котором были исследованы магнитные свойства атомов серебра. Мы увидим, что происходит при измерении спина в нескольких разных направлениях. Акт измерения может влиять на состояние кубита. Существует также базовая неопределенность, связанная с измерениями, с которой вы тоже должны познакомиться.

В заключение главы я покажу, что эксперименты, подобные экспериментам со спином, можно проводить с использованием поляризованных фильтров и обычного света.

Глава 2. Квантовые вычисления основаны на линейной алгебре. К счастью, нам потребуется освоить лишь несколько понятий. Эта глава представляет и описывает нужный нам аппарат линейной алгебры и иллюстрирует, как он будет использоваться в последующих главах.

Здесь мы познакомимся с векторами и матрицами и посмотрим, как вычислить длину вектора и как определить, являются ли два вектора перпендикулярными. Глава начинается с описания элементарных операций с векторами и затем демонстрирует, как с помощью матриц выполнить множество таких вычислений одновременно.

На первый взгляд может показаться, что эти сведения бесполезны, но это не так. Линейная алгебра лежит в основе квантовых вычислений. А так как остальная часть книги опирается на математический аппарат, описываемый в этой главе, вы должны внимательно прочитать ее.

Глава 3. В этой главе я покажу, какое отношение к рассматриваемой теме имеют две предыдущие главы. Математическая модель спина, или, что то же самое, поляризации, основана на использовании понятий линейной алгебры. С их помощью мы сможем дать определение кубита и точно описать происходящее при его измерении. Здесь также будет представлено несколько примеров измерения кубитов в разных направлениях.

Глава заканчивается введением в квантовую криптографию, описываемую протоколом BB84.

Глава 4. В этой главе описывается, что подразумевается под запутанностью двух кубитов. Запутанность трудно описать обычными словами, но она легко описывается на языке математики. Здесь будет представлено новое математическое понятие — тензорное произведение. Это самый простой способ объединения математических моделей отдельных кубитов в единую модель, которая описывает коллекцию кубитов.

Хотя сам математический аппарат относительно прост, объяснить запутанность обычными словами не получится, потому что мы не наблюдаем этого явления в обыденной жизни. Измеряя один из пары запутанных кубитов, мы влияем на состояние другого кубита. Альберт Эйнштейн назвал это не понравившееся ему явление «сверхъестественным действием на расстоянии». Мы рассмотрим несколько его примеров.

В конце главы я покажу, почему нельзя использовать явление запутанности для передачи информации быстрее скорости света.

Глава 5. Здесь мы рассмотрим проблемы Эйнштейна с запутанностью и способность теории скрытых переменных сохранить локальный реализм. Мы познакомимся с математикой неравенства Белла — замечательным средством экспериментально определить верность аргумента Эйнштейна. Как известно большинству людей, мнение Эйнштейна было ошибочным, но даже Белл думал, что оно окажется верно.

Артур Экерт (Artur Ekert) заметил, что с помощью окружения проверки неравенства Белла также можно получить ключ шифрования для криптографических нужд и одновременно для проверки наличия подслушивающих устройств. В конце главы мы познакомимся с описанием этого криптографического протокола.

Глава 6. Глава начинается с обзора аспектов стандартных вычислений: битов, вентилей и логических операций. Затем кратко описывает обратимые вычисления и идеи Эда Фредкина (Ed Fredkin). Здесь мы увидим, что вентили Фредкина и вентили Тоффоли (Toffoli) являются универсальными — используя только их, можно сконструировать настоящий компьютер. Завершается глава описанием бильярдного компьютера Фредкина. На самом деле эта информация не нужна для дальнейшего обзора, но сама идея настолько интересна, что заслуживает включения в книгу.

Этот компьютер состоит из шаров, сталкивающихся друг с другом и с бортами бильярдного стола, напоминая сталкивающиеся частицы. Это одна из идей, вызвавших у Ричарда Фейнмана (Richard Feynman) интерес к квантовым вычислениям. Фейнман написал несколько ранних работ на эту тему.

Глава 7. Эта глава открывается изучением квантовых вычислений с использованием квантовых цепей. Определяет квантовые вентили. Здесь мы увидим воздействие квантовых вентилей на кубит и обнаружим, что все эти идеи уже рассматривали выше. Мы просто сменим точку зрения. Начнем размышлять об ортогональной матрице не как воздействующей на измерительное устройство, а как воздействующей на кубит. Мы также докажем некоторые удивительные результаты, касающиеся сверхплотного кодирования, телепортации квантов, клонирования и коррекции ошибок.

Глава 8. Это, пожалуй, самая сложная глава. Здесь мы рассмотрим некоторые квантовые алгоритмы и увидим, насколько быстро они могут выполняться в сравнении с классическими алгоритмами. Чтобы иметь возможность говорить о скорости алгоритмов, нам придется познакомиться с разными понятиями из теории сложности. Определив то, что называется *сложностью запроса*, мы исследуем три квантовых алгоритма и покажем, что они выполняются быстрее — с учетом этого типа сложности, — чем их классические аналоги.

Квантовые алгоритмы используют основную структуру решаемой проблемы. Это гораздо больше, чем просто идея квантового параллелизма — помещение входа в суперпозицию всех возможных состояний. Эта глава представляет последний фрагмент математического аппарата — матричное произведение Кронекера (Kronecker). Однако сложность этой темы в действительности обусловлена использованием совершенно нового подхода к вычислениям и отсутствием у нас опыта рассуждения о решении задач с применением этих новых идей.

Глава 9. В последней главе рассматривается влияние квантовых вычислений на нашу жизнь. Мы начнем с краткого описания двух важных алгоритмов, один из которых изобрел Питер Шор, а другой — Лов Гровер.

Алгоритм Шора реализует разложение большого числа на простые сомножители. Это может показаться не особенно важным, но безопасность в интернете зависит от сложности решения этой задачи. Возможность быстро находить разложение на простые сомножители ставит под угрозу текущие методы защиты взаимодействий между компьютерами. Возможно, пройдет немало времени, пока у нас появятся квантовые компьютеры, достаточно мощные для разложения больших чисел, используемых в настоящее время, но угроза более чем реальна, и уже сейчас следует задуматься над тем, как организовать безопасные взаимодействия между компьютерами.

Алгоритм Гровера предназначен для специализированных видов поиска данных. Мы увидим, как он работает на небольшой выборке, и рассмотрим принцип его работы в общем случае. Оба алгоритма, Гровера и Шора, важны не только для задач, которые они решают, но также для новых идей, которые они представляют. Эти базовые идеи будут включаться в новое поколение алгоритмов.

После знакомства с алгоритмами мы переключимся и кратко рассмотрим использование квантовых вычислений для имитации квантовых процессов. Химия на самом базовом уровне относится к квантовой механике. Классическая вычислительная химия основана на вычислении уравнений квантовой механики с использованием классических компьютеров. Эти уравнения являются приблизительными и не учитывают некоторые мелкие детали. Часто они дают удовлетворительные результаты, но в не-

которых случаях их точности оказывается недостаточно. В таких случаях требуется учитывать мелкие детали, а квантовые компьютеры должны быть способны передать их.

В этой главе также кратко рассматривается создание реальных машин. Это очень быстро развивающаяся область. Первые машины уже доступны для продажи. В облаке есть даже одна машина, которую каждый может использовать бесплатно. Вероятно, скоро мы вступим в эпоху *квантового превосходства*. (Я объясню, что это значит.)

Квантовые вычисления — не новый тип вычислений, а открытие истинной их природы. В этом заключается ключевая мысль книги.

От издательства

Ваши замечания, предложения, вопросы отправляйте по адресу comp@piter.com (издательство «Питер», компьютерная редакция).

Мы будем рады узнать ваше мнение!

На веб-сайте издательства www.piter.com вы найдете подробную информацию о наших книгах.

1 Спин

Любые вычисления включают ввод данных, выполнение операций с ними согласно некоторым правилам и вывод окончательного ответа. Основной единицей данных в классических вычислениях является *бит*. В квантовых вычислениях основной единицей данных является *квантовый бит* (quantum bit), или просто *кубит* (qubit).

Классический бит соответствует одной из двух альтернатив. Все, что может находиться только в одном из двух состояний, может представлять бит. Далее мы увидим разные примеры битов, такие как логическое утверждение, которое может иметь истинное или ложное состояние, выключатель, находящийся в состоянии «включено» или «выключено», и даже наличие или отсутствие бильярдного шара.

Кубит, как и бит, включает эти альтернативы, но, в отличие от бита, может также находиться в комбинации этих двух состояний. Что это значит? Какие комбинации двух состояний могут быть и какие физические объекты могут представлять кубиты? Что может служить аналогом выключателя в квантовых вычислениях?

Кубит может быть представлен спином электрона или поляризацией фотона. Это определение верно, но выглядит практически бесполезным, потому что большинство из нас ничего не знает о спине электрона и поляризации фотона и не сталкивается с этими понятиями в повседневной жизни. Поэтому начнем с элементарного введения и познакомимся с понятиями спина и поляризации. Для этого рассмотрим основополагающий

эксперимент, выполненный Отто Штерном и Уолтером Герлахом, в котором они исследовали магнитные свойства атомов серебра.

В 1913 году Нильс Бор предложил планетарную модель, описывающую строение атома, за которую в 1922 году был удостоен Нобелевской премии. Согласно этой модели, атом состоит из положительно заряженного ядра, вокруг которого вращаются отрицательно заряженные электроны. Бор считал, что орбиты имеют круглую форму и определенные радиусы. На самой близкой к ядру орбите могут находиться не более двух электронов. После заполнения этой орбиты электроны начинают заполнять следующую, где могут находиться не более восьми электронов. Атом серебра имеет 47 электронов. Два из них находятся на самой внутренней орбите, восемь — на следующей, по восемнадцать на третьей и четвертой орбитах и на последней, пятой, орбите — оставшийся единственный электрон.

Электроны, вращающиеся по круговым орбитам, генерируют магнитные поля. Электроны на внутренних орбитах связаны в пары, при этом электроны в парах вращаются в противоположных направлениях, в результате чего возбуждаемые ими магнитные поля компенсируют друг друга. Однако единственный электрон на внешней орбите генерирует магнитное поле, которое не компенсируется другими электронами. Это означает, что атом можно считать маленьким магнитом, имеющим северный и южный полюс.

Штерн и Герлах поставили эксперимент, чтобы проверить, могут ли оси север-юг этих магнитиков иметь любое направление или же они имеют определенную ориентацию. Для этого они пропустили пучок атомов серебра через пару магнитов, как показано на рис. 1.1. V-образная форма магнитов обеспечила более сильное воздействие со стороны южного магнита. Если северный полюс атома серебра направлен вверх, а южный вниз, он будет притягиваться обоими магнитами установки, но воздействие со стороны южного полюса будет сильнее, и частица отклонится вверх. Аналогично, северный полюс атома серебра направлен вниз, а южный вверх, он будет отталкиваться обоими магнитами установки, и снова воздействие со стороны южного полюса будет сильнее, и частица отклонится вниз. После прохождения через аппаратуру атомы серебра оседают на пластинке.

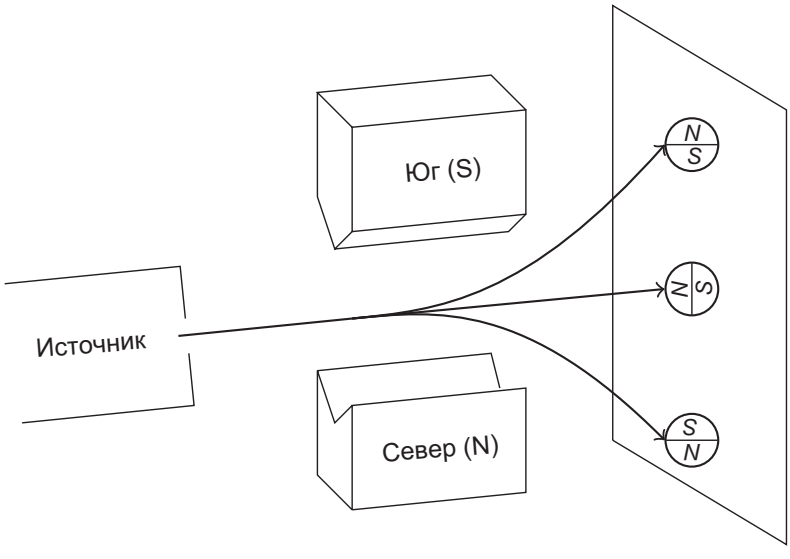


Рис. 1.1. Установка Штерна—Герлаха

С точки зрения классической теории магнитные поля атомов могут быть ориентированы в любых направлениях. Если магнитная ось север-юг атома имеет горизонтальную ориентацию, такой атом не отклонится под воздействием магнитов. В общем случае величина отклонения должна соответствовать углу наклона магнитной оси атома к горизонтали, с максимальным отклонением для атомов, ось которых ориентирована строго вертикально.

Если классическая теория верна, тогда, после прохождения через установку достаточно большое количество атомов серебра, на пластинке должна появиться непрерывная вертикальная линия. Но Штерн и Герлах получили иную картину. Они обнаружили на пластинке только две точки: в крайней верхней и крайней нижней позициях. Все атомы вели себя как магниты, ось которых ориентирована строго по вертикали. Никакой другой ориентации обнаружено не было. Как такое возможно?

Прежде чем приступить к анализу результатов эксперимента, переключим наше внимание с атомов на электроны. Не только сами атомы, но и их компоненты действуют подобно маленьким магнитам. Изучая квантовые компьютеры, мы часто будем говорить об электронах и их спинах. Если,

как в эксперименте с атомами серебра, измерить направление спина[1], можно обнаружить, что электрон отклоняется в направлении либо северного, либо южного полюса. И снова вы увидите, что электроны, подобно атомам серебра, ведут себя как маленькие магниты с осью север-юг, ориентированной строго по вертикали. Не найдется ни одного электрона с любой другой ориентацией.

На практике невозможно измерить спин свободного электрона, используя установку Штерна—Герлаха, как в эксперименте с атомами серебра, потому что электрон имеет отрицательный заряд, а магнитное поле отклоняет заряженные частицы. Тем не менее диаграммы на рис. 1.2 и рис. 1.3 дают простое и понятное представление результатов измерения спинов с разной ориентацией. Глядя на эти диаграммы, вообразите, что вы — источник электронов; между вами и плоскостью книжной страницы находятся магниты. Точка показывает, в какую сторону отклонится электрон. На рис. 1.2 слева показано отклонение электрона под воздействием магнитов, а справа изображен сам электрон в виде магнита с обозначенными северным и южным полюсами. В этой ситуации можно сказать, что *электрон имеет вертикальный спин N*. На рис. 1.3 изображен другой возможный исход эксперимента, когда *электрон имеет вертикальный спин S*.

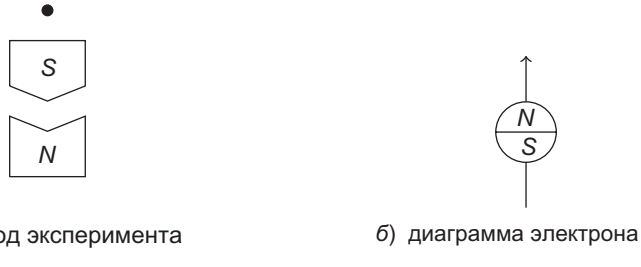


Рис. 1.2. Электрон с вертикальным спином *N*

Чтобы понять причину отклонения, полезно вспомнить, что южный магнит оказывает более сильное воздействие, чем северный, поэтому для определения направления отклонения можно учитывать влияние только

[1] Мы продолжим использовать термин *спин*, потому что это стандартная терминология. Но в данном случае мы просто определяем ориентацию полюсов магнита.

этого магнита. Если электрон ориентирован северным полюсом к южному магниту, он будет притянут и отклонится в сторону южного магнита. Если электрон ориентирован южным полюсом к южному магниту, он оттолкнется и отклонится в сторону северного магнита.

а) исход эксперимента *б*) диаграмма электрона

Рис. 1.3. Электрон с вертикальным спином *S*

Разумеется, вертикальная ориентация не является особым случаем. Например, если повернуть магниты на 90°, электроны все так же будут отклоняться в сторону северного или южного магнита. В этом случае они будут вести себя как магниты с осью север-юг, ориентированной в горизонтальном направлении, как показано на рис. 1.4 и 1.5.

а) исход эксперимента *б*) диаграмма электрона

Рис. 1.4. Электрон со спином *N*, повернутым под углом 90°

а) исход эксперимента *б*) диаграмма электрона

Рис. 1.5. Электрон со спином *S*, повернутым под углом 90°

В следующих главах мы будем поворачивать магниты на разные углы, которые будем измерять по часовой стрелке, начиная с угла 0°, обознача-

ющего вертикальное направление вверх, и символом θ будем обозначать угол поворота от направления вертикально вверх. На рис. 1.6 изображен электрон со спином *N*, направленным под углом θ°.

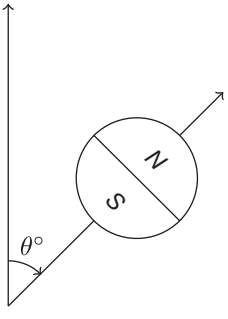
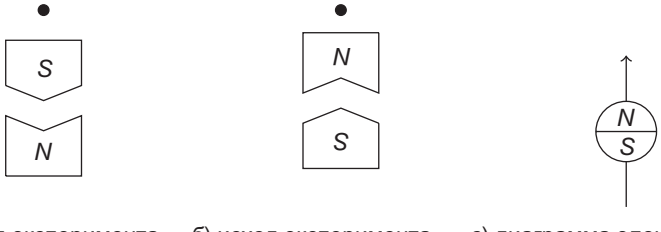


Рис. 1.6. Электрон со спином *N*, повернутым под углом θ°

Иногда спин описывается как *верхний*, *нижний*, *левый* или *правый*. Наше описание спина *N* электрона в направлении под углом 0° выглядит несколько громоздко, но оно устраняет неоднозначность и помогает избежать некоторых ловушек при использовании понятий *верх*, *низ* и т. д., особенно при повороте установки на угол 180°. Например, на рис. 1.7 изображены две ситуации, когда спин *N* электрона направлен под углом 0°, что эквивалентно спину *S*, направленному под углом 180°.



а) исход эксперимента *б*) исход эксперимента *в*) диаграмма электрона

Рис. 1.7. Электрон со спином *N*, повернутым под углом 0°

Прежде чем продолжить знакомство со спином электрона, остановимся и рассмотрим аналогию, которую будем иногда использовать.

«Квантовые» часы[1]

Представьте часы с привычным циферблатом. Кроме циферблата в часах есть стрелка. Однако вам запрещено смотреть на циферблат. Вы можете только задавать вопросы. Вам нужно узнать, в каком направлении указывает стрелка. Казалось бы, для этого достаточно задать именно этот простой вопрос. Но это тоже запрещено. Вы можете только спросить, указывает ли стрелка на какое-то число на циферблате, например, указывает стрелка на двенадцать или на четыре. Если бы это были обычные часы, потребовалась бы определенная доля везения, чтобы получить ответ «да», потому что большую часть времени стрелка не будет указывать на какое-то конкретное число. Но квантовые часы отличаются от обычных. Они отвечают «да» или сообщают, что стрелка указывает в направлении, противоположном упомянутому в вопросе. Если мы спросим, указывает ли стрелка на число двенадцать, часы ответят «да» или сообщат, что стрелка указывает на число шесть. Если мы спросим, указывает ли стрелка на число четыре, часы ответят «да» или сообщат, что стрелка указывает на число десять. Это довольно курьезная ситуация, но она полностью аналогична спину электрона.

Как уже говорилось выше, спин электрона станет тем понятием, которое будет использовано для определения кубита. Чтобы выполнить вычисления, нам нужно понять правила, управляющие измерением спина. Для начала посмотрим, что случится, если измерение выполнить несколько раз.

Измерения в одном направлении

Измерения повторимы. Если повторить то же самое измерение, мы получим тот же самый результат. Например, представьте, что мы решили измерить спин электрона в вертикальном направлении. Для этого повторим тот же эксперимент, поместив еще две установки позади первой. Одну расположим точно на пути электронов, отклоняемых вверх первой установкой, а вторую — на пути электронов, отклоняемых вниз. Электроны,

[1] В данном случае не имеются в виду высокоточные атомные, или квантовые, часы — реальный прибор для измерения времени. — *Примеч. ред.*

отклоняемые первой установкой вверх, также будут отклоняться вверх следующей установкой, а электроны, отклоняемые первой установкой вниз, будут отклоняться вниз следующей за ней. Это означает, что электроны, первоначально имеющие спин *N* в направлении 0°, сохранят спин *N* в направлении 0° в повторном эксперименте. Аналогично, если электрон первоначально имеет спин *S* в направлении 0° и мы повторим тот же самый эксперимент, то обнаружим, что электрон все так же имеет спин *S* в направлении 0°. А теперь вернемся к аналогии с часами: если повторно спросить, указывает ли стрелка на двенадцать, мы повторно получим тот же самый ответ: стрелка всегда будет указывать либо на число двенадцать, либо всегда на число шесть.

Разумеется, вертикальная ориентация не является особым случаем. Если провести первое измерение в направлении θ° и затем продолжать повторять измерения в том же направлении, мы каждый раз будем получать тот же самый результат. В результате мы получим строку, состоящую только из букв *N* или только из букв *S*.

А теперь посмотрим, что получится, если повторные измерения производить в других направлениях, отличных от первоначального. Например, что получится, если первое измерение выполнить по вертикали, а второе по горизонтали?

Измерения в разных направлениях

Измерим спин электрона сначала в вертикальном, а потом в горизонтальном направлении. Для этого пошлем пучок электронов через первый детектор и измерим спин в вертикальном направлении. Как и в предыдущем мысленном эксперименте, добавим еще два детектора, расположив их за первым так, чтобы они находились точно на пути электронов, вылетающих из первого детектора. Но на этот раз эти два дополнительных детектора повернем на угол 90° и измерим спин в горизонтальном направлении.

Сначала рассмотрим пучок электронов, которые отклоняются первым детектором вверх, — все они имеют спин *N* в направлении 0°. Но когда они преодолеют второй детектор, мы увидим, что одна половина из них имеет

спин *N*, а другая половина — спин *S* в направлении 90°. Выбор южного или северного спина в направлении 90° будет полностью случайным. Невозможно сказать, какой спин, *N* или *S*, получит в результате измерения в направлении 90° электрон, имевший спин *N* в направлении 0°. Аналогичное поведение можно наблюдать у электронов, для которых первый детектор определил спин *S* в вертикальном направлении, — одна половина получит горизонтальный спин *N*, а другая — горизонтальный спин *S*. В результате мы получим совершенно случайные последовательности из *N* и *S*.

Это все равно что сначала спросить у наших часов, указывает ли стрелка на число двенадцать, а затем — указывает ли она на число три. Если у нас будет большое число таких часов и каждому задать эту пару вопросов, ответ на второй вопрос всегда будет случайным. В половине случаев часы ответят, что стрелка указывает на три, а в половине случаев — что она указывает на девять. Ответы на первый вопрос в этом случае никак не влияют на ответы на второй вопрос.

Наконец, посмотрим, что получится, если выполнить три измерения. Сначала по вертикали, потом по горизонтали и затем снова по вертикали. Рассмотрим поток электронов, вылетающих из первого детектора со спином *N* в направлении 0°. Мы уже знаем, что при измерении в направлении 90° половина из них получит спин *N*, а половина — спин *S*. Теперь ограничимся только потоком электронов со спином *N* после первых двух измерений и измерим их спин в третий раз в вертикальном направлении. Мы увидим, что ровно половина из этих электронов имеет спин *N* в направлении 0° и половина — спин *S*. И снова последовательность букв *N* и *S* будет выглядеть совершенно случайной. Тот факт, что первоначально электроны имели спин *N* в вертикальном направлении, не означает, что после повторного измерения в вертикальном направлении (после промежуточного горизонтального) они сохранят спин *N*.

Какие выводы можно сделать из полученных результатов? Их три, и все они очень важны.

Во-первых, если снова и снова задавать один и тот же вопрос, мы всегда будем получать один и тот же ответ. Это говорит нам о том, что иногда можно получить определенные ответы. Ответы на каждый вопрос будут даваться не случайно.

Во-вторых, если задать последовательность вопросов, конечный результат может оказаться непредсказуемым.

В-третьих, измерения влияют на результаты. Мы видели, что если трижды задать один и тот же вопрос, мы трижды получим один и тот же ответ. Но если первый и третий вопросы будут идентичны, а второй будет отличаться от них, ответы на первый и третий вопросы могут оказаться разными. Например, если трижды спросить, указывает ли стрелка на число двенадцать, на каждый вопрос мы получим один и тот же ответ. Но если сначала спросить, указывает ли стрелка на число двенадцать, затем на число три, а потом опять на двенадцать, ответы на первый и третий вопрос могут оказаться разными. Единственное различие между этими двумя сценариями — второй вопрос, то есть этот вопрос должен влиять на результат следующего вопроса. Мы еще немного поговорим об этих наблюдениях и начнем с измерений.

Измерения

Рассмотрим аналогию из классической механики — расчет траектории мяча, летящего в воздухе. Траекторию можно рассчитать с использованием формул, но для этого нужно знать некоторые параметры, такие как масса мяча и начальная скорость. Как измеряются параметры, несущественно для расчетов. Просто предположим, что они известны. Неявно предполагается, что акт измерения не влияет на решение задачи, то есть измерения не влияют на моделируемую систему. Для примера броска мяча в воздух это вполне оправданно. Мы можем измерить начальную скорость, используя, например, полицейский радар. В этом случае фотоны, испускаемые радаром, будут отскакивать от мяча и оказывать на него определенное влияние, но оно настолько мало, что им можно пренебречь. В основе классической механики лежит простая философия: измерения оказывают влияние на изучаемые объекты, но эксперимент можно спроектировать так, что эффект этих влияний окажется незначительным и им можно пренебречь.

В квантовой механике обычно рассматриваются маленькие частицы, такие как атомы или электроны. Здесь фотоны, отскакивающие от них, оказывают

более значительное влияние, которым нельзя пренебречь. Чтобы выполнить какое-то измерение, нужно взаимодействовать с системой. Эти взаимодействия будут вносить возмущения в систему, поэтому мы не сможем их игнорировать. Уже не удивительно, что измерение становится одним из основных компонентов теории, но удивительно, как это происходит. Например, рассмотрим случай измерения спина электрона сначала в вертикальном, а потом в горизонтальном направлении. Мы уже видели, что половина электронов, имеющих спин *N* в направлении 0° после прохождения первого детектора, будут иметь спин *N* в направлении 90° при измерении вторым детектором. Может показаться, что мощность магнитов оказывает некоторое влияние на результат. Возможно, они настолько мощные, что заставляют магнитные оси электронов поворачиваться вдоль силовых линий магнитного поля измерительного устройства, и при использовании менее мощных магнитов их влияние уменьшится, и мы получим другие результаты. Однако это неверное представление о месте измерений в теории. Как мы увидим далее, для нашей модели важна не «мощность», а сам факт наличия процесса измерений, каким бы он ни был. Далее в книге мы рассмотрим математический аппарат, который описывает измерение спина в квантовой механике. Мы увидим, что каждый раз, когда производится измерение, система изменяется некоторыми предопределенными способами, которые зависят от типа выполняемого измерения, но не от его мощности.

Включение измерений в теорию — одно из различий классической и квантовой механики. Другое различие относится к случайности.

Случайность

Квантовая механика предполагает случайность получаемых результатов. Например, если сначала измерить спин электронов в вертикальном, а потом в горизонтальном направлении и записать результаты второго измерения, мы получим строку из символов *N* и *S*. Символы будут следовать в совершенно случайном порядке. Например, эта строка может выглядеть так: *NSSNNNSS...*

Классический способ получить случайную последовательность из двух символов, каждый из которых имеет 50-процентную вероятность по-

явления, — подбрасывание монеты. Так, подбрасывая монету, мы можем получить последовательность *OPPOOOPP...* Несмотря на то что эти два примера дают похожие результаты, случайность в них интерпретируется совершенно по-разному.

Бросание монеты можно описать с позиции классической механики. Его можно смоделировать с использованием численных методов. Чтобы вычислить, как упадет монета, орлом или решкой, нужно предварительно измерить начальные параметры: вес монеты, высоту над поверхностью земли, силу удара большим пальцем по монете, точное место удара пальцем по монете, местоположение монеты и т. д. и т. п. На основе всех этих значений теория сможет точно сказать, какой стороной вверх упадет монета. На самом деле здесь нет никакой случайности. Бросание монеты только выглядит случайным, потому что каждый раз, когда мы бросаем монету, начальные условия немного отличаются. Эти небольшие отличия могут изменить результат. В классической механике нет настоящей случайности, только то, что мы называем *чувствительностью к начальным условиям* — небольшое изменение на входе может усилиться и привести к совершенно иному исходу. В квантовой механике случайность имеет совершенно иную природу. Здесь случайность настоящая.

Последовательность *NSSNNNSS...*, полученная в результате измерения спина в двух направлениях, носит истинно случайный характер, в чем мы убедимся далее. Последовательность результатов бросков монеты *OPPOOOPP...* только кажется случайной. Законы классической физики четко определены, и имей мы возможность проводить измерения с бесконечной точностью, эта случайность исчезла бы.

На данном этапе это объяснение вызывает недоверие. Эйнштейну эта интерпретация, конечно же, не понравилась, и он сказал, что «Бог не играет в кости». Быть может, существует какая-то более глубокая теория? Если бы мы имели больше информации о начальных параметрах электронов, может, тогда бы конечный результат перестал выглядеть случайным? Нет ли каких-то *скрытых переменных*, узнав значения которых можно объяснить результаты и случайность перестанет быть случайностью? Мы еще вернемся к этим вопросам и познакомимся с математической теорией, в которой используется истинная случайность. Мы увидим интересный эксперимент, помогающий отличить скрытую

переменную от истинной случайности. Этот эксперимент проводился неоднократно, и его результаты всегда показывали, что случайность реальна и нет никаких простых скрытых переменных, которые могли бы устранить ее.

В начале этой главы было сказано, что кубит может быть представлен спином электрона или поляризацией фотона. Поэтому теперь давайте посмотрим, как связаны модели спина и поляризации.

Фотоны и поляризация

Часто говорят, что мы ничего не знаем о странных квантовых явлениях лишь потому, что они имеют невероятно малый размер и не проявляются в масштабах нашей обыденной жизни. В этом есть доля правды, однако есть эксперимент, полностью идентичный измерению спина электронов, который можно провести с использованием очень простого оборудования. Он касается поляризованного света.

Для экспериментов понадобятся три квадратика поляризованной пленки. Расположите два квадрата друг перед другом. Один квадрат удерживайте неподвижным, а другой поверните на 90°. Вы увидите, что свет свободно проходит сквозь оба фильтра, когда их направления поляризации совпадают, но полностью блокируется, когда один из фильтров поворачивается на 90°. Пока мы не наблюдаем ничего особенно интересного. Теперь поверните фильтры так, чтобы свет не проходил через них, возьмите третий фильтр, поверните его на 45° и вдвиньте его между двумя первыми фильтрами. Удивительно, но теперь свет свободно проходит через три фильтра, хотя перед этим он не проходил через два первых.

Я услышал об этом эксперименте с тремя фильтрами несколько лет тому назад. Я спросил у своего друга физика, есть ли у него поляризованная пленка. Он пригласил меня в свою лабораторию, забитую всякой всячиной, отрезал кусок пленки и передал мне. Я разрезал его на три квадрата, примерно дюйм на дюйм каждый, и провел этот эксперимент — все, что я слышал, подтвердилось! Это очень простой и удивительный эксперимент. С тех пор я ношу эти три квадратика в бумажнике.

Измеряя поляризацию фотонов, можно обнаружить, что они поляризованы в двух перпендикулярных направлениях, каждое из которых перпендикулярно направлению движения фотонов. Поляризованный фильтр пропускает фотоны, поляризованные в одном направлении, и поглощает фотоны, поляризованные в другом направлении. Фильтры подобны установке Штерна—Герлаха. Прохождение света через фильтр можно считать измерением. Как и в случае со спином, возможны два исхода: либо поляризация фотона соответствует направлению поляризации фильтра, и тогда фотон проходит сквозь него, либо поляризация фотона перпендикулярна направлению поляризации фильтра, и тогда фотон поглощается.

Предположим, что поляризация фильтра имеет вертикальную ориентацию, то есть он пропускает фотоны, поляризованные вертикально, и поглощает фотоны, поляризованные горизонтально, и рассмотрим несколько экспериментов, соответствующих тем, которые мы описали, когда рассматривали спин электрона.

Допустим, что у нас имеется два фильтра с одинаковой ориентацией, то есть они оба пропускают фотоны с вертикальной поляризацией. Если посмотреть на каждый фильтр в отдельности, они оба будут выглядеть слегка затемненными, как и ожидалось, потому что оба поглощают некоторые фотоны — те, что имеют горизонтальную поляризацию. Если теперь совместить два фильтра, мы заметим лишь минимальные изменения. Величина света, пропускаемого через два фильтра, примерно равна величине света, пропускаемого каждым из них в отдельности. Эта ситуация изображена на рис. 1.8.

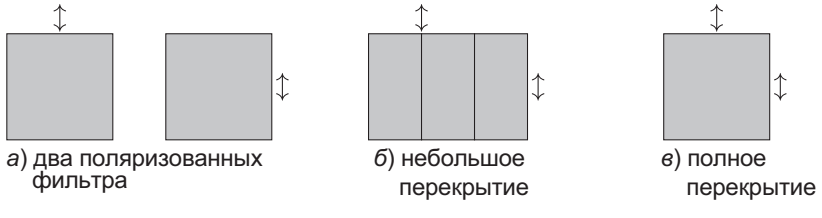


Рис. 1.8. Два линейно поляризованных фильтра с одинаковой ориентацией

Теперь повернем один из фильтров на 90°. Если допустить, что речь идет об обычном свете, а не о свете, отражающемся от зеркальной поверхности

или исходящем от экрана компьютера, в потоке света в равной пропорции будут присутствовать вертикально и горизонтально поляризованные фотоны и оба фильтра в отдельности будут выглядеть одинаково затемненными. Повторим опыт с совмещением фильтров. На этот раз свет не будет проходить через пару перекрывающихся фильтров, как показано на рис. 1.9.

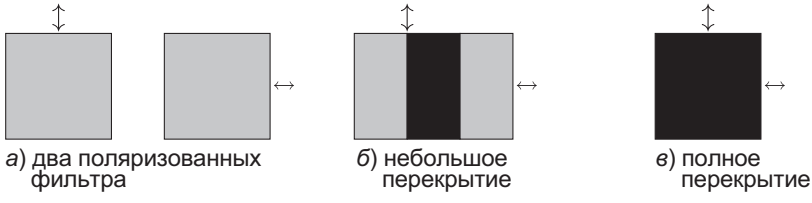


Рис. 1.9. Два линейно поляризованных фильтра с разной ориентацией

Третий эксперимент: взять третий фильтр и повернуть его на 45°. При нормальном освещении поворот фильтра не вызывает видимых изменений. Он все так же остается немного затемненным. А теперь поместите его между двумя другими фильтрами, один из которых ориентирован по вертикали, а другой по горизонтали. Как уже отмечалось выше, результат может удивить вас. Через все три фильтра будет проникать некоторая часть света (как показано на рис. 1.10). Эти поляризованные фильтры явно действуют не как обычные фильтры. Через три фильтра проникает больше света, чем через два!

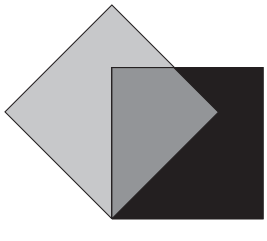


Рис. 1.10. Три линейно поляризованных фильтра с разной ориентацией

Сейчас я кратко расскажу, что происходит, а чуть позже в книге вы увидите математическую модель, описывающую спин и поляризацию.

Вспомним наши квантовые часы. Мы можем спросить, указывает стрелка на число двенадцать или на шесть. В ответ на любой из этих вопросов часы сообщат нам, на какое число указывает стрелка, просто ответы «да»/«нет» поменяются местами. В случае с поляризованными фильтрами аналогичные вопросы задаются их поворотом на 90°, а не на 180°. В ответ мы получим ту же самую информацию. Разница лишь в том, что в случае ответа «да» фотон проникает через фильтр и мы можем выполнить дополнительные измерения с ним, но в случае ответа «нет» фильтр поглотит фотон и мы не сможем задать ему никаких других вопросов.

В первых двух экспериментах участвовали только два фильтра, сообщающие нам одно и то же: при повторном измерении мы получаем тот же самый результат. В обоих экспериментах мы дважды измеряем поляризацию в вертикальном и горизонтальном направлениях. В этих экспериментах фотоны, проникающие через первый фильтр, имеют вертикальную ориентацию поляризации. В первом эксперименте, где второй фильтр тоже был ориентирован вертикально, мы дважды задали вопрос: «Фотон поляризован вертикально?» — и дважды получили ответ: «Да». Во втором эксперименте мы изменили второй вопрос на: «Фотон поляризован горизонтально?» — и получили ответ: «Нет». Оба эксперимента дали нам одну и ту же информацию, но отрицательный ответ на второй вопрос во втором эксперименте означает, что фотон был поглощен и поэтому недоступен для дальнейших измерений.

Фильтр в третьем эксперименте, который повернут на 45°, измеряет поляризацию под углами 45° и 135°. Мы знаем, что фотоны, прошедшие через первый фильтр, поляризованы вертикально. При измерении вторым фильтром одна половина фотонов оказывается поляризованной под углом 45°, а другая — под углом 135°. Фотоны с углом поляризации 45° проходят через фильтр, а другие поглощаются им. Третий фильтр снова измеряет поляризацию в вертикальном и горизонтальном направлениях. Достигшие его фотоны имеют поляризацию 45°, но когда мы измеряем поляризацию в вертикальном и горизонтальном направлениях, одна половина из них оказывается поляризованной вертикально, а другая — горизонтально. Фильтр поглощает вертикально поляризованные фотоны и пропускает горизонтально поляризованные.

Заключение

В начале этой главы мы отметили, что классические биты могут быть представлены самыми обычными объектами, такими как выключатели, имеющие два состояния («включено» и «выключено»), а кубиты — спином электронов или поляризацией фотонов. Спин и поляризация малознакомы нам и обладают свойствами, совершенно непохожими на классические аналоги.

Чтобы измерить спин, сначала нужно выбрать направление и затем провести измерение в этом направлении. Спин *квантуется*:[1] при измерении мы получаем только два возможных ответа, а не непрерывный спектр ответов. Мы можем связать эти результаты с классическими битами. Например, получив ответ *N*, мы можем считать его двоичной цифрой 0, а получив ответ *S*, мы можем считать его двоичной цифрой 1. Именно так мы получаем ответы в квантовых вычислениях. Последний этап вычислений — измерение. В результате мы получим одно из двух, что можно интерпретировать как 0 или 1. Хотя фактические вычисления осуществляются с использованием кубитов, окончательный ответ получается в терминах классических битов.

Мы пока только начали свое знакомство с квантовыми вычислениями, поэтому весьма ограничены в своих возможностях. Но мы уже можем генерировать случайные строки из двоичных цифр. Эксперимент, генерирующий строки из символов *N* и *S*, можно переиначить и интерпретировать его результаты как строки из 0 и 1. Измерение спинов электронов сначала в вертикальном, а потом в горизонтальном направлении даст нам случайную строку из 0 и 1. Это, пожалуй, самое простое, что мы можем сделать с кубитами, но что особенно удивительно, мы не можем сделать то же самое с помощью классического компьютера. Классические компьютеры действуют исключительно детерминированно. Они могут вычислять разные строки, которые пройдут любые проверки на случайность, но они будут псевдослучайными, а не случайными. Они вычисляются с помощью некоторой детерминированной функции и, зная алгоритм

[1] Квантование — процедура построения чего-либо с помощью дискретного набора величин, например целых чисел, в отличие от построения с помощью непрерывного набора величин, например вещественных чисел.

функции и начальное значение, вы сможете получить в точности ту же самую строку. Не существует классических компьютерных алгоритмов, способных генерировать по-настоящему случайные строки. Уже сейчас мы видим, что квантовые вычисления имеют некоторые преимущества перед классическими.

Прежде чем начать описывать другие квантовые вычисления, нужно создать точную математическую модель, которая описывает происходящее при измерении спина в разных направлениях. Мы начнем создание такой модели в следующей главе, где познакомимся с линейной алгеброй — алгеброй матриц и векторов.

2 Линейная алгебра

Квантовая механика основана на линейной алгебре. Общая теория использует бесконечномерные векторные пространства. К счастью для нас, чтобы описать спин или поляризацию, достаточно конечных размерностей, что существенно упрощает жизнь. Нам понадобится лишь несколько инструментов. Их список приводится в конце этой главы. В остальной части этой главы я расскажу, как использовать эти инструменты и какой смысл несут вычисления. Здесь вы увидите много примеров, и нам нужно тщательно исследовать каждый из них. Представленный здесь математический аппарат очень важен для понимания последующих объяснений. Как и многое в математике, имеющиеся здесь выкладки могут показаться сложными при первом знакомстве, но по мере практики они становятся понятнее. Фактические вычисления основываются только на сложении и вычитании чисел, хотя иногда будут встречаться операции извлечения квадратного корня и тригонометрические функции.

Мы будем использовать обозначения Поля Дирака (Paul Dirac). Дирак был одним из основателей квантовой механики, и предложенная им система обозначений широко используется в квантовой механике и квантовых вычислениях. Она редко применяется за пределами этих дисциплин, что довольно странно, учитывая ее элегантность и удобство.

Для начала мы познакомимся поближе с числами, которые будем использовать. Это действительные числа — обычные десятичные числа, знакомые всем нам. Практически во всех других книгах по квантовым вычислениям используются комплексные числа — они имеют отношение к вычислению

квадратного корня из отрицательных значений. Итак, давайте разберемся, почему мы будем их использовать.

Комплексные и действительные числа

Действительные числа просты в использовании. Комплексные числа намного сложнее. Чтобы использовать комплексные числа, следует поговорить об их модулях и понять, зачем нам нужен сопряженный элемент. Для того, что мы собираемся делать, комплексные числа не нужны и только добавляют дополнительные сложности. Но почему тогда, спросите вы, во всех других книгах используются комплексные числа? Что можно делать с комплексными числами такого, чего нельзя делать с действительными? Давайте кратко ответим на эти вопросы.

Как вы помните, мы измеряли спин электрона под разными углами. Все эти углы лежат в одной плоскости, однако мы живем в трехмерном мире. Мы рассмотрели задачу измерения спина, проведя аналогию с квантовыми часами, где можно только спрашивать о направлении стрелки, движущейся по двумерному циферблату. Если добавить третье измерение, плоский циферблат квантовых часов превратится в глобус, в котором стрелка направлена из центра к поверхности. У таких часов можно спросить, например, указывает ли стрелка на Нью-Йорк. На этот вопрос такие часы ответят либо «да», либо сообщат, что стрелка указывает на точку, диаметрально противоположную Нью-Йорку. Математическая модель спина в трех измерениях использует комплексные числа. Однако вычисления с участием кубитов, которые мы будем рассматривать, должны измерять спин только в двух измерениях. Поэтому хотя наше описание на основе действительных чисел не настолько всеобъемлющее как на основе комплексных чисел, его для наших нужд будет вполне достаточно.

Наконец, комплексные числа дают элегантный способ соединения тригонометрических и экспоненциальных функций. В самом конце книги мы рассмотрим алгоритм Шора. Его трудно было бы объяснить без использования комплексных чисел. Но этот алгоритм требует также использования цепных дробей наряду с результатами из теории чисел и результатами оценки скорости алгоритма проверки простых чисел. Чтобы понять все

нюансы алгоритма Шора, нужно обладать серьезными математическими знаниями. Поэтому мы просто познакомимся с основными идеями, лежащими в его основе, и посмотрим, как они сочетаются друг с другом. Отмечу еще раз, что в дальнейших описаниях будут использоваться только действительные числа.

Итак, для того, что мы собираемся сделать, комплексные числа не нужны. Но если после прочтения этой книги вы захотите продолжить изучение квантовых вычислений, они понадобятся вам при исследовании более сложных тем.

А теперь, разобравшись, почему мы будем использовать только действительные числа, начнем знакомство с векторами и матрицами.

Векторы

Вектор — это список чисел. *Мерность* вектора — это количество чисел в списке. Если список записан по вертикали, его называют *вектором-столбцом,* или *кет*. Если список записан по горизонтали, его называют *вектором-строкой,* или *бра*. Числа, составляющие вектор, часто называют *элементами*. Ниже приводятся трехмерный кет и четырехмерный бра:

$$\begin{bmatrix} 2 \\ 0{,}5 \\ -3 \end{bmatrix}, \begin{bmatrix} 1 & 0 & -\pi & 23 \end{bmatrix}.$$

Названия *бра* и *кет*[1] были предложены Полем Дираком. Он также предложил систему обозначений для записи имен векторов этих двух типов: кет с именем v обозначается как $|v\rangle$, а бра с именем w — как $\langle w|$. То есть можно записать:

$$|v\rangle = \begin{bmatrix} 2 \\ 0{,}5 \\ -3 \end{bmatrix} \text{ и } \langle w| = \begin{bmatrix} 1 & 0 & -\pi & 23 \end{bmatrix}.$$

[1] Бра и кет (*англ.* bra-ket < bracket — скобка).

Позже вы узнаете, почему имена окружают разные символы и почему с одной стороны используется угловая скобка. А пока важно запомнить, что кеты — это столбцы (представьте повторяющийся звук «к»), а бра — это векторы, элементы которых записаны по горизонтали.

Диаграммы векторов

Двух- или трехмерный вектор можно изобразить как стрелку. Рассмотрим, например, вектор $|a\rangle = \begin{bmatrix} 3 \\ 1 \end{bmatrix}$. (В дальнейшем мы часто будем использовать кеты для примеров, но если хотите, можете заменить их на бра.) Первый элемент, 3 в этом примере, определяет смещение вдоль оси *X* конечной точки вектора относительно его начала. Второй элемент определяет смещение вдоль оси *Y*. В качестве начала вектора можно выбрать любую точку на координатной плоскости — если поместить начало вектора в точку (*a, b*), тогда конечная точка вектора будет иметь координаты (*a* + 3, *b* + 1). Обратите внимание: если начальную точку вектора поместить в начало координат, конечная точка будет находиться в координатах, заданных в элементах вектора. Это очень удобно, и мы часто будем рисовать векторы с начальной точкой в начале координат. На рис. 2.1 изображен один и тот же кет с разными начальными точками.

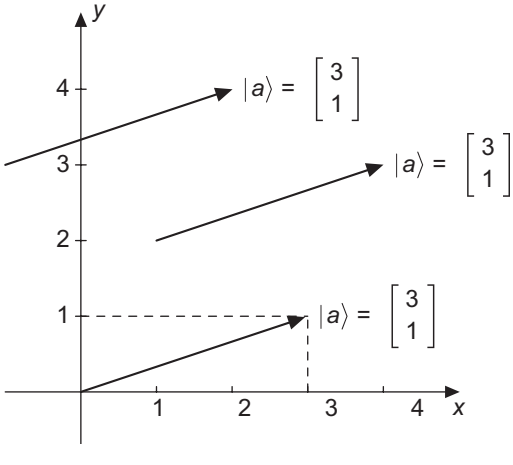


Рис. 2.1. Один и тот же кет с разными начальными точками

Длина вектора

Длина вектора, как нетрудно догадаться, — это расстояние от начальной до конечной точки. Длина вычисляется как квадратный корень от суммы квадратов элементов. (Это следует из теоремы Пифагора.) Длина кета $|a\rangle$ обозначается как $\||a\rangle\|$, то есть для $|a\rangle = \begin{bmatrix} 3 \\ 1 \end{bmatrix}$ мы получим $\||a\rangle\| = \sqrt{3^2 + 1^2} = \sqrt{10}$.

В более общем случае, если $|a\rangle = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix}$, тогда $\||a\rangle\| = \sqrt{a_1^2 + a_2^2 + \cdots a_n^2}$.

Вектор с длиной, равной 1, называется *единичным* вектором. Позже вы узнаете, что кубиты представлены единичными векторами.

Скалярное произведение

Вектор можно умножить на число. (В линейной алгебре числа часто называют скалярами, и под скалярным произведением понимается умножение на число.) Чтобы найти скалярное произведение, нужно каждый элемент вектора умножить на заданное число. Например, умножение кета

$$|a\rangle = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix}$$

на число c дает в результате

$$c|a\rangle = \begin{bmatrix} ca_1 \\ ca_2 \\ \vdots \\ ca_n \end{bmatrix}.$$

Нетрудно проверить, что умножение вектора на положительное число c увеличивает его длину в c раз. Мы можем использовать это свойство для

получения векторов разной длины, указывающих в одном направлении. В частности, нам часто нужен будет единичный вектор, указывающий в направлении, заданном неединичным вектором. Длина любого ненулевого вектора $|a\rangle$ равна $\||a\rangle\|$, поэтому умножив его на обратную величину длины, мы получим единичный вектор. Например, для $|a\rangle = \begin{bmatrix} 3 \\ 1 \end{bmatrix}$ и $\||a\rangle\| = \sqrt{10}$ мы получим

$$|u\rangle = \frac{1}{\sqrt{10}}\begin{bmatrix} 3 \\ 1 \end{bmatrix} = \begin{bmatrix} \frac{3}{\sqrt{10}} \\ \frac{1}{\sqrt{10}} \end{bmatrix},$$

и далее

$$\||u\rangle\| = \sqrt{\left(\frac{3}{\sqrt{10}}\right)^2 + \left(\frac{1}{\sqrt{10}}\right)^2} = \sqrt{\frac{9}{10} + \frac{1}{10}} = \sqrt{1} = 1.$$

То есть $|u\rangle$ — единичный вектор, указывающий в том же направлении, что и вектор $|a\rangle$.

Сложение векторов

Два вектора одного типа — два кета или два бра — и с одинаковой мерностью можно сложить и получить новый вектор того же типа и с той же мерностью. Первый элемент этого нового вектора является суммой первых элементов исходных векторов, второй элемент — суммой вторых элементов и т. д. Например, если

$$|a\rangle = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} \text{ и } |b\rangle = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix},$$

тогда

$$|a+b\rangle = \begin{bmatrix} a_1 + b_1 \\ a_2 + b_2 \\ \vdots \\ a_n + b_n \end{bmatrix}.$$

Сумму векторов можно графически изобразить, используя известное *правило параллелограмма*. Если вектор $|b\rangle$ изобразить так, что его начальная точка будет находиться в конечной точке вектора $|a\rangle$, тогда вектор, соединяющий начальную точку вектора $|a\rangle$ и конечную точку вектора $|b\rangle$, будет представлять сумму $|a+b\rangle$. На рисунке это будет выглядеть как треугольник.

Векторы $|a\rangle$ и $|b\rangle$ можно поменять ролями, поместив начальную точку вектора $|a\rangle$ в конечную точку вектора $|b\rangle$. Тогда вектор, соединяющий начальную точку вектора $|b\rangle$ и конечную точку вектора $|a\rangle$, будет представлять сумму $|b+a\rangle$. И снова мы получим треугольник. Мы знаем, что $|a+b\rangle = |b+a\rangle$. Поэтому если нарисовать треугольники, изображающие $|a+b\rangle$ и $|b+a\rangle$, совместив их по вектору результата, мы получим параллелограмм, диагональ которого представляет обе суммы, $|a+b\rangle$ и $|b+a\rangle$, как показано на рис. 2.2, где $|a\rangle = \begin{bmatrix} 3 \\ 1 \end{bmatrix}$ и $|b\rangle = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$, а результат соответственно $|a+b\rangle = |b+a\rangle = \begin{bmatrix} 4 \\ 3 \end{bmatrix}$.

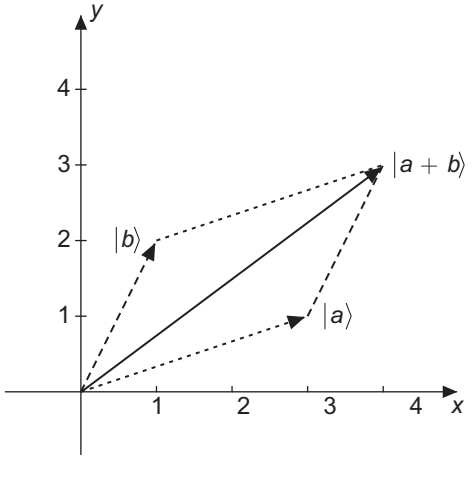


Рис. 2.2. Определение суммы векторов с использованием закона параллелограмма

Ортогональные векторы

Рисунок 2.2 показывает некоторые основные свойства операции сложения векторов. Одно из важнейших свойств вытекает из теоремы Пифагора. Мы знаем, что если a, b и c — это длины сторон треугольника, то равенство $a^2 + b^2 = c^2$ верно тогда и только тогда, когда треугольник является прямоугольным. То есть два вектора, $|a\rangle$ и $|b\rangle$, перпендикулярны, только если $\||a\rangle\|^2 + \||b\rangle\|^2 = \||a+b\rangle\|^2$.

Слово *ортогональный* является синонимом слова *перпендикулярный* и широко используется в линейной алгебре. Соответственно, свойство, описанное выше, можно изложить немного иначе: два вектора, $|a\rangle$ и $|b\rangle$, ортогональны, только если $\||a\rangle\|^2 + \||b\rangle\|^2 = \||a+b\rangle\|^2$.

Умножение бра на кет

Если имеются два вектора, бра и кет, с одинаковой мерностью, их можно перемножить — бра слева от оператора умножения и кет справа — и получить в результате число. Ниже показано, как это делается, где предполагается, что оба вектора, $\langle a|$ и $|b\rangle$, являются n-мерными:

$$\langle a| = \begin{bmatrix} a_1 & a_2 & \cdots & a_n \end{bmatrix} \text{ и } |b\rangle = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}.$$

Для обозначения произведения достаточно просто поместить векторы рядом друг с другом, без использования какого-либо символа оператора между ними. Произведение записывается как $\langle a||b\rangle$. Если сократить эту запись еще больше и удалить одну вертикальную черту, мы получим $\langle a|b\rangle$. Именно такое обозначение мы будем использовать далее. Вот как выглядит формула вычисления произведения бра на кет:

$$\langle a|b\rangle = \begin{bmatrix} a_1 & a_2 & \cdots & a_n \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n .$$

Вертикальные черты в обозначениях бра и кета «совместились», что помогает запомнить, что бра имеет вертикальную черту справа, а кет — слева. Результат состоит из термов, заключенных в угловые скобки. Названия «бра» («bra») и «кет» («ket») заимствованы из слова «bracket» (группа, связка), которое является почти точным сочетанием двух имен. Это довольно расплывчатая игра слов, но она тоже помогает запомнить, что в этом произведении бра находится слева от кета.

В линейной алгебре это произведение часто называют *внутренним*, или *скалярным*, произведением, но в квантовой механике принято использовать название бра-кет (bra-ket). Мы тоже будем использовать его далее в книге. Теперь, дав определение произведению бра-кет, посмотрим, что можно получить с его помощью. Для начала вернемся к вычислению длины.

Произведение бра-кет и длина

Если обозначить кет как $|a\rangle$, тогда определение бра $\langle a|$ с тем же именем будет иметь очевидный вид. Они оба будут иметь одни и те же элементы, но в векторе $|a\rangle$ они будут располагаться по вертикали, а в векторе $\langle a|$ — по горизонтали.

$$|a\rangle = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} \langle a| = \begin{bmatrix} a_1 & a_2 & \cdots & a_n \end{bmatrix}.$$

Соответственно, $\langle a|a\rangle = a_1^2 + a_2^2 + \ldots + a_n^2$, то есть длину вектора $|a\rangle$, можно кратко записать как $\||a\rangle| = \sqrt{\langle a|a\rangle}$.

Вернемся к примеру, где мы определяли длину

$$|a\rangle = \begin{bmatrix} 3 \\ 1 \end{bmatrix} : \langle a|a\rangle = \begin{bmatrix} 3 & 1 \end{bmatrix} \begin{bmatrix} 3 \\ 1 \end{bmatrix} = 3^2 + 1^2 = 10.$$

Затем извлекаем корень квадратный и получаем $\||a\rangle| = \sqrt{10}$.

Единичные векторы тоже будут играть важную роль в наших исследованиях. Чтобы проверить, является ли вектор единичным — имеет дли-

ну 1, — мы снова воспользуемся тем, что кет $|a\rangle$ является единичным, только если $\langle a|a\rangle = 1$.

Еще одно важное понятие — ортогональность. Произведение бра-кет может сообщить нам, являются ли два вектора ортогональными.

Произведение бра-кет и ортогональность

Два кета, $|a\rangle$ и $|b\rangle$, ортогональны тогда и только тогда, когда $\langle a|b\rangle = 0$. Сначала рассмотрим пару примеров, а потом познакомимся с математическим обоснованием.

Пусть $|a\rangle = \begin{bmatrix} 3 \\ 1 \end{bmatrix}$, $|b\rangle = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$ и $|c\rangle = \begin{bmatrix} -2 \\ 6 \end{bmatrix}$. Вычислим $\langle a|b\rangle$ и $\langle a|c\rangle$.

$$\langle a|b\rangle = \begin{bmatrix} 3 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \end{bmatrix} = 3 + 2 = 5,$$

$$\langle a|c\rangle = \begin{bmatrix} 3 & 1 \end{bmatrix} \begin{bmatrix} -2 \\ 6 \end{bmatrix} = -6 + 6 = 0.$$

Поскольку $\langle a|b\rangle \neq 0$, мы можем сказать, что $|a\rangle$ и $|b\rangle$ не ортогональны. Поскольку $\langle a|c\rangle = 0$, мы можем сказать, что $|a\rangle$ и $|c\rangle$ ортогональны.

Почему? Вот доказательство на примере двумерных кетов.

Пусть $|a\rangle = \begin{bmatrix} a_1 \\ a_2 \end{bmatrix}$ и $|b\rangle = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}$, тогда $|a\rangle + |b\rangle = \begin{bmatrix} a_1 + b_1 \\ a_2 + b_2 \end{bmatrix}$. Вычислим квадрат длины $|a\rangle + |b\rangle$.

$$\begin{aligned}
\big\||a\rangle + |b\rangle\big\|^2 &= \begin{bmatrix} a_1 + b_1 & a_2 + b_2 \end{bmatrix} \begin{bmatrix} a_1 + b_1 \\ a_2 + b_2 \end{bmatrix} = \\
&= (a_1 + b_1)^2 + (a_2 + b_2)^2 = \\
&= \left(a_1^2 + 2a_1b_1 + b_1^2\right) + \left(a_2^2 + 2a_2b_2 + b_2^2\right) = \\
&= \left(a_1^2 + a_2^2\right) + \left(b_1^2 + b_2^2\right) + 2\left(a_1b_1 + a_2b_2\right) = \\
&= \big\||a\rangle\big\|^2 + \big\||b\rangle\big\|^2 + 2\langle a|b\rangle.
\end{aligned}$$

Очевидно, что результат будет равен $\||a\rangle\|^2 + \||b\rangle\|^2$, только если $2\langle a|b\rangle = 0$. Теперь вспомним наше наблюдение, что два вектора, $|a\rangle$ и $|b\rangle$, ортогональны, только если $\||a\rangle\|^2 + \||b\rangle\|^2 = \||a+b\rangle\|^2$. Используя наш расчет квадрата длины $|a\rangle + |b\rangle$, это наблюдение можно сформулировать иначе: два вектора, $|a\rangle$ и $|b\rangle$, ортогональны, только если $\langle a|b\rangle = 0$.

Мы рассмотрели доказательство на примере двумерных кетов, но оно распространяется на кеты любой мерности.

Ортонормированный базис

Слово «ортонормированный» состоит из двух слов: «орто» — от «ортогональный» и «нормированный» — от «нормализованный», что в данном случае означает «единичный». Для случая двумерных кетов ортонормированный базис состоит из двух единичных кетов, ортогональных друг к другу. В общем случае, когда речь идет о *n*-мерных кетах, ортонормированный базис состоит из *n* единичных кетов, взаимно ортогональных друг к другу.

Для начала рассмотрим двумерные кеты. Множество всех двумерных векторов обозначается как $\mathbb{R}^2$. Ортонормированный базис для $\mathbb{R}^2$ состоит из двух ортогональных единичных векторов $|b_1\rangle$ и $|b_2\rangle$. То есть чтобы проверить, образуют ли два кета ортонормированный базис, нужно сначала убедиться, что они оба являются единичными векторами, а затем проверить их ортогональность. Оба этих условия можно проверить с помощью произведений бра-кет: $\langle b_1|b_1\rangle = 1$, $\langle b_2|b_2\rangle = 1$ и $\langle b_1|b_2\rangle = 0$.

Вот стандартный пример, который называют *стандартным базисом*:

$$|b_1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{и} \quad |b_2\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Нетрудно убедиться, что в данном случае оба свойства бра-кет выполняются. Кроме стандартного базиса

$$\left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}$$

существует бесконечное множество других ортонормированных базисов, например, вот два из них:

$$\left\{\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{-1}{\sqrt{2}}\end{bmatrix},\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{bmatrix}\right\} \text{ и } \left\{\begin{bmatrix}\frac{1}{2}\\ \frac{\sqrt{3}}{2}\end{bmatrix},\begin{bmatrix}\frac{-\sqrt{3}}{2}\\ \frac{1}{2}\end{bmatrix}\right\}.$$

В предыдущей главе мы рассматривали задачу измерения спина частицы. Мы измеряли спин сначала в вертикальном, а потом в горизонтальном направлении. Математическая модель измерения спина в вертикальном направлении опирается на использование стандартного базиса. Поворот измерительной установки математически описывается выбором нового ортонормированного базиса. Все три двумерных базиса, перечисленные выше, будут играть важную роль в интерпретации спина, поэтому векторы, составляющие базисы, мы будем обозначать не буквами, а стрелками, определяющими направление спина, как показано ниже:

$$|\uparrow\rangle=\begin{bmatrix}1\\0\end{bmatrix},|\downarrow\rangle=\begin{bmatrix}0\\1\end{bmatrix},|\rightarrow\rangle=\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{-1}{\sqrt{2}}\end{bmatrix},|\leftarrow\rangle=\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{bmatrix},|\nearrow\rangle=\begin{bmatrix}\frac{1}{2}\\ \frac{-\sqrt{3}}{2}\end{bmatrix},$$

$$\text{и } |\swarrow\rangle=\begin{bmatrix}\frac{\sqrt{3}}{2}\\ \frac{1}{2}\end{bmatrix}.$$

Эти три базиса можно записать более компактно:

$$\{|\uparrow\rangle,|\downarrow\rangle\},\{|\rightarrow\rangle,|\leftarrow\rangle\} \text{ и } \{|\nearrow\rangle,|\swarrow\rangle\}.$$

Так как они являются ортонормированными, мы получаем следующие значения произведений бра-кет:

$$\begin{array}{llll}\langle\uparrow|\uparrow\rangle=1 & \langle\downarrow|\downarrow\rangle=1 & \langle\uparrow|\downarrow\rangle=0 & \langle\downarrow|\uparrow\rangle=0\\ \langle\rightarrow|\rightarrow\rangle=1 & \langle\leftarrow|\leftarrow\rangle=1 & \langle\rightarrow|\leftarrow\rangle=0 & \langle\leftarrow|\rightarrow\rangle=0\\ \langle\nearrow|\nearrow\rangle=1 & \langle\swarrow|\swarrow\rangle=1 & \langle\nearrow|\swarrow\rangle=0 & \langle\swarrow|\nearrow\rangle=0\end{array}$$

Векторы как линейные комбинации базисных векторов

Имея кет и ортонормированный базис, можно выразить кет как взвешенную сумму базисных векторов. На данном этапе пока неясно, где это может пригодиться, но позже мы увидим, что это одна из основных идей, на которых основана наша математическая модель. Для начала познакомимся с двумерными примерами.

Любой вектор $|v\rangle$ в $\mathbb{R}^2$ можно записать как сумму его произведений на $|\uparrow\rangle$ и $|\downarrow\rangle$. Это эквивалентно очевидному факту, что для любых чисел c и d уравнение

$$\begin{bmatrix} c \\ d \end{bmatrix} = x_1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + x_2 \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

имеет решение. Очевидно, что корнями этого уравнения являются $x_1 = c$ и $x_2 = d$ и это единственно возможное решение.

Можно ли любой вектор $|v\rangle$ в $\mathbb{R}^2$ записать как сумму его произведений на $|\rightarrow\rangle$ и $|\leftarrow\rangle$? Имеет ли решение следующее уравнение для любых чисел c и d?

$$\begin{bmatrix} c \\ d \end{bmatrix} = x_1 |\rightarrow\rangle + x_2 |\leftarrow\rangle .$$

Как решить его? Мы можем заменить кеты двумя их двумерными векторами-столбцами, а затем решить получившуюся систему двух линейных уравнений с двумя неизвестными. Но есть гораздо более простой путь, основанный на использовании бра и кетов.

Во-первых, обе стороны уравнения умножим слева на бра $\langle\rightarrow|$. В результате получим следующее уравнение.

$$\langle\rightarrow| \begin{bmatrix} c \\ d \end{bmatrix} = \langle\rightarrow| \left(x_1 |\rightarrow\rangle + x_2 |\leftarrow\rangle \right).$$

Далее, раскроем скобки в правой части уравнения.

$$\langle\rightarrow| \begin{bmatrix} c \\ d \end{bmatrix} = x_1 \langle\rightarrow|\rightarrow\rangle + x_2 \langle\rightarrow|\leftarrow\rangle .$$

Оба произведения бра-кет справа нам известны. Первое равно 1. Второе равно 0. Отсюда сразу находим, что x_1 равно $\langle\rightarrow|\begin{bmatrix} c \\ d \end{bmatrix}$. Достаточно вычислить только это произведение.

$$\langle\rightarrow|\begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} 1/\sqrt{2} & -1/\sqrt{2} \end{bmatrix}\begin{bmatrix} c \\ d \end{bmatrix} = \left(1/\sqrt{2}\right)c - \left(1/\sqrt{2}\right)d = \left(c-d\right)/\sqrt{2}.$$

Соответственно, $x_1 = \left(c-d\right)/\sqrt{2}$.

Аналогичным способом можно найти x_2. Возьмем то же начальное уравнение $\begin{bmatrix} c \\ d \end{bmatrix} = x_1|\rightarrow\rangle + x_2|\leftarrow\rangle$ и обе стороны умножим слева на бра $\langle\leftarrow|$.

$$\langle\leftarrow|\begin{bmatrix} c \\ d \end{bmatrix} = x_1\langle\leftarrow|\rightarrow\rangle + x_2\langle\leftarrow|\leftarrow\rangle = x_1 0 + x_2 1.$$

Таким образом, $x_2 = \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \end{bmatrix}\begin{bmatrix} c \\ d \end{bmatrix} = \left(1/\sqrt{2}\right)c + \left(1/\sqrt{2}\right)d = \left(c+d\right)/\sqrt{2}.$

Соответственно, можно записать

$$\begin{bmatrix} c \\ d \end{bmatrix} = \frac{\left(c-d\right)}{\sqrt{2}}|\rightarrow\rangle + \frac{\left(c+d\right)}{\sqrt{2}}|\leftarrow\rangle.$$

Правая часть — это сумма векторов, каждый из которых является произведением некоторого скаляра на базисный вектор. Выше я описал ее как взвешенную сумму базисных векторов, но будьте осторожны с ее интерпретацией. Скаляры необязательно должны быть положительными. Они могут быть отрицательными. В нашем примере, если бы число *c* было равно –3, а *d* равно 1, оба веса, $\left(c-d\right)/\sqrt{2}$ и $\left(c+d\right)/\sqrt{2}$, получились бы отрицательными. Именно поэтому вместо термина *взвешенная сумма* используется термин *линейная комбинация базисных векторов*.

Теперь перейдем к *n* измерениям. Допустим, у нас имеется *n*-мерный кет $|v\rangle$ и ортонормированный базис $\left\{|b_1\rangle,|b_2\rangle,\cdots,|b_n\rangle\right\}$. Можно ли представить $|v\rangle$ как линейную комбинацию базисных векторов? Если да, является ли эта комбинация уникальной? Является ли решение уравнения

$$|v\rangle = x_1|b_1\rangle + x_2|b_2\rangle + \cdots + x_i|b_i\rangle + \cdots + x_n|b_n\rangle$$

уникальным? И снова ответ на этот вопрос: «да». Чтобы убедиться в этом, посмотрим, как найти значение x_i. Вычисления производятся точно так же, как в случае с двумя измерениями. Сначала умножим обе стороны уравнения на $\langle b_i|$. Мы знаем, что $\langle b_i|b_k\rangle$ равно 0, если $i \neq k$, и равно 1, если $i = k$. То есть после умножения на бра правая сторона упрощается до x_i, и мы получаем $\langle b_i|v\rangle = x_i$. Отсюда следует, что $x_1 = \langle b_1|v\rangle$, $x_2 = \langle b_2|v\rangle$ и т. д. Соответственно, мы можем записать $|v\rangle$ как линейную комбинацию базисных векторов:

$$|v\rangle = \langle b_1|v\rangle|b_1\rangle + \langle b_2|v\rangle|b_2\rangle + \cdots + \langle b_i|v\rangle|b_i\rangle + \cdots + \langle b_n|v\rangle|b_n\rangle.$$

На данный момент все это выглядит несколько абстрактно, но все станет ясно в следующей главе. Разные ортонормированные базисы соответствуют выбору разных ориентаций при измерении спина. Числа, указанные в произведениях бра-кет, такие как $\langle b_i|v\rangle$, называют *амплитудами вероятности*. Если возвести в квадрат $\langle b_i|v\rangle$, мы получим вероятность перехода $|v\rangle$ к $|b_i\rangle$ при измерении. Все это будет объяснено далее в книге, но понимание уравнения, записанного выше, имеет решающее значение для этого.

Упорядоченные базисы

Упорядоченный базис — это базис, в котором векторы следуют в определенном порядке, то есть имеется первый вектор, второй вектор и т. д. Если $\{|b_1\rangle, |b_2\rangle, \cdots, |b_n\rangle\}$ является базисом, мы будем обозначать упорядоченный базис как $(|b_1\rangle, |b_2\rangle, \cdots, |b_n\rangle)$, заменяя фигурные скобки круглыми. Например, рассмотрим $\mathbb{R}^2$. Напомню, что это стандартный базис $\{|\uparrow\rangle, |\downarrow\rangle\}$. Два множества эквивалентны, если они содержат одни и те же элементы, — порядок элементов не имеет значения, то есть $\{|\uparrow\rangle, |\downarrow\rangle\} = \{|\downarrow\rangle, |\uparrow\rangle\}$. Эти два множества идентичны.

Однако для упорядоченного базиса порядок следования базисных векторов имеет значение. $(|\uparrow\rangle, |\downarrow\rangle) \neq (|\downarrow\rangle, |\uparrow\rangle)$. Первый вектор в упорядоченном базисе слева не равен первому вектору в упорядоченном базисе справа, то есть эти два множества различны.

Различия между упорядоченными и неупорядоченными базисами могут показаться обусловленными избыточным педантизмом, но на самом деле это не так. Мы увидим несколько примеров, когда имеется один и тот же

набор базисных векторов, но следующих в разном порядке. Перестановка базисных векторов даст нам важную информацию.

Например, выше уже говорилось, что стандартный базис $\{|\uparrow\rangle,|\downarrow\rangle\}$ соответствует измерению спина электрона в вертикальном направлении. Упорядоченный базис $(|\uparrow\rangle,|\downarrow\rangle)$ соответствует измерению спина, когда южный полюс магнита в измерительной установке находится вверху. Если перевернуть установку на 180°, это будет равносильно перестановке элементов базиса и использованию упорядоченного базиса $(|\downarrow\rangle,|\uparrow\rangle)$.

Длины векторов

Допустим, у нас есть кет $|v\rangle$ и ортонормированный базис $\{|b_1\rangle, |b_2\rangle, \cdots, |b_n\rangle\}$, мы знаем, что $|v\rangle$ можно записать в виде линейной комбинации базисных векторов. В результате получаем $|v\rangle = \langle b_1|v\rangle|b_1\rangle + \langle b_2|v\rangle|b_2\rangle + \cdots + \langle b_i|v\rangle|b_i\rangle + \cdots + \langle b_n|v\rangle|b_n\rangle$. Для простоты запишем это равенство как $|v\rangle = c_1|b_1\rangle + c_2|b_2\rangle + \cdots + c_i|b_i\rangle + \cdots + c_n|b_n\rangle$. Существует очень удобная формула вычисления длины $|v\rangle$: $\||v\rangle\|^2 = c_1^2 + c_2^2 + \cdots c_i^2 \cdots + \cdots c_n^2$.

Давайте убедимся в ее истинности. Мы знаем, что $\||v\rangle\|^2 = \langle v|v\rangle$.

Используя соотношение $\langle v| = c_1\langle b_1| + c_2\langle b_2| + \cdots + c_n\langle b_n|$, получаем

$$\langle v|v\rangle = \left(c_1\langle b_1| + c_2\langle b_2| + \cdots + c_n\langle b_n|\right)\left(c_1|b_1\rangle + c_2|b_2\rangle + \cdots + c_n|b_n\rangle\right).$$

Следующим шагом развернем произведение в круглых скобках. Может показаться, что мы получим месиво из членов уравнения, но это не так. Снова вспомним, что $\langle b_i|b_k\rangle$ равно 0, если $i \neq k$, и равно 1, если $i = k$. Все произведения бра-кет для членов с разными индексами будут равны 0. Единственными ненулевыми произведениями бра-кет будут те, в которых участвуют члены с одинаковыми индексами, и каждое из них будет равно 1. В результате мы получаем $\langle v|v\rangle = c_1^2 + c_2^2 + \cdots + c_i^2 + \cdots c_n^2$.

Матрицы

Матрицы — это прямоугольные массивы чисел. Матрица M с m строками и n столбцами называется матрицей $m \times n$. Вот примеры:

$$A = \begin{bmatrix} 1 & -4 & 2 \\ 2 & 3 & 0 \end{bmatrix} B = \begin{bmatrix} 1 & 2 \\ 7 & 5 \\ 6 & 1 \end{bmatrix}.$$

A имеет две строки и три столбца, то есть это матрица 2×3. B — это матрица 3×2. Векторы бра и кеты можно рассматривать как специальные типы матриц: бра имеют только одну строку, а кеты — только один столбец.

Операция *транспонирования* матрицы M размером $m \times n$ обозначается как M^T. Ее результатом является матрица $n \times m$, полученная взаимной заменой строк и столбцов в матрице M, то есть когда i-я строка из M становится i-м столбцом в M^T, а j-й столбец из M становится j-й строкой в M^T. Для наших матриц A и B получаем:

$$A^T = \begin{bmatrix} 1 & 2 \\ -4 & 3 \\ 2 & 0 \end{bmatrix} B^T = \begin{bmatrix} 1 & 7 & 6 \\ 2 & 5 & 1 \end{bmatrix}.$$

Векторы-столбцы можно считать матрицами с единственным столбцом, а векторы-строки — матрицами с единственной строкой. Согласно такой интерпретации, отношения между бра и кетами с одинаковыми именами можно выразить как $\langle a| = |a\rangle^T$ и $|a\rangle = \langle a|^T$.

Для обобщенной матрицы с несколькими строками и столбцами можно считать, что ее строки — это бра, а столбцы — кеты. В примере выше матрица A состоит из двух бра, расположенных друг над другом, или из трех кетов, расположенных друг за другом. Аналогично, матрица B состоит из трех бра, расположенных друг над другом, или из двух кетов, расположенных друг за другом.

Эта идея используется в операции умножения матриц. Произведение обозначается как AB и в вычислениях используются бра из A и кеты из B. (Не забывайте, что в операции умножения бра всегда находятся слева, а кеты справа.)

$$A = \begin{bmatrix} \langle a_1| \\ \langle a_2| \end{bmatrix},$$

где $\langle a_1| = \begin{bmatrix} 1 & -4 & 2 \end{bmatrix}$ и $\langle a_2| = \begin{bmatrix} 2 & 3 & 0 \end{bmatrix}$.

$$B = \begin{bmatrix} |b_1\rangle & |b_2\rangle \end{bmatrix}, \text{ где } |b_1\rangle = \begin{bmatrix} 1 \\ 7 \\ 6 \end{bmatrix} \text{ и } |b_2\rangle = \begin{bmatrix} 2 \\ 5 \\ 1 \end{bmatrix}.$$

Произведение AB вычисляется, как показано ниже:

$$AB = \begin{bmatrix} \langle a_1| \\ \langle a_2| \end{bmatrix} \begin{bmatrix} |b_1\rangle & |b_2\rangle \end{bmatrix} = \begin{bmatrix} \langle a_1|b_1\rangle & \langle a_1|b_2\rangle \\ \langle a_2|b_1\rangle & \langle a_2|b_2\rangle \end{bmatrix} =$$
$$= \begin{bmatrix} 1\times 1 - 4\times 7 + 2\times 6 & 1\times 2 - 4\times 5 + 2\times 1 \\ 2\times 1 + 3\times 7 + 0\times 6 & 2\times 2 + 3\times 5 + 0\times 1 \end{bmatrix} =$$
$$= \begin{bmatrix} -15 & -16 \\ 23 & 19 \end{bmatrix}.$$

Обратите внимание, что мерность бра в A равна мерности кетов в B. Это совершенно необходимо, чтобы получить произведения бра-кет. Также отметьте, что $AB \neq BA$. Для данного примера BA — это матрица 3×3, то есть даже ее размер отличается от размера AB.

В общем случае для матриц A размером $m \times r$ и B размером $r \times n$ мы записываем матрицу A как множество r-мерных бра, а матрицу B — как множество r-мерных кетов.

$$A = \begin{bmatrix} \langle a_1| \\ \langle a_2| \\ \vdots \\ \langle a_m| \end{bmatrix} B = \begin{bmatrix} |b_1\rangle & |b_2\rangle & \cdots & |b_n\rangle \end{bmatrix}.$$

Произведением AB является матрица $m \times n$, которая имеет элемент $\langle a_i|b_j\rangle$ в i-й строке и j-м столбце, то есть

$$AB = \begin{bmatrix} \langle a_1|b_1\rangle & \langle a_1|b_2\rangle & \cdots & \langle a_1|b_j\rangle & \cdots & \langle a_1|b_n\rangle \\ \langle a_2|b_1\rangle & \langle a_2|b_2\rangle & \cdots & \langle a_2|b_j\rangle & \cdots & \langle a_2|b_n\rangle \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \langle a_i|b_1\rangle & \langle a_i|b_2\rangle & \cdots & \langle a_i|b_j\rangle & \cdots & \langle a_i|b_n\rangle \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \langle a_m|b_1\rangle & \langle a_m|b_2\rangle & \cdots & \langle a_m|b_j\rangle & \cdots & \langle a_m|b_n\rangle \end{bmatrix}.$$

Перестановка матриц местами дает произведение BA, но мы не сможем вычислить его, если m не будет равно n, потому что бра и кеты будут иметь разные мерности. Но даже если m будет равно n и мы сможем выполнить умножение, в результате получится матрица $r \times r$. Она не будет равна матрице AB размером $n \times n$, если n не равно r. И даже если n, m и r равны друг другу, все равно AB обычно получается отличной от BA. Чтобы подчеркнуть этот факт, мы говорим, что операция умножения матриц *не является коммутативной*.

Матрицы с одинаковым числом строк и столбцов называются *квадратными*. *Главной диагональю* квадратной матрицы называют диагональ, соединяющую верхний левый элемент с правым нижним. Квадратная матрица, все элементы на главной диагонали которой равны 1, а остальные равны 0, называется *единичной* матрицей. Единичная матрица $n \times n$ обозначается как I_n.

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \; I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \; \cdots$$

Единичная матрица получила такое название потому, что умножение матрицы на единичную матрицу подобно умножению числа на 1. Допустим, что A — это матрица $m \times n$. Тогда $I_m A = A I_n = A$.

Матрицы дают удобный способ вычислений с использованием бра и кетов. Следующий раздел покажет способ использования.

Вычисления с матрицами

Пусть имеется множество n-мерных кетов $\{|b_1\rangle, |b_2\rangle, \cdots, |b_n\rangle\}$ и нужно проверить, представляют ли они ортонормированный базис. Сначала нужно убедиться, что все они являются единичными векторами, а затем проверить их взаимную ортогональность. Мы уже видели, как проверить оба этих условия с использованием бра и кетов, но матрицы позволяют выразить эти вычисления проще.

Начнем с того, что сформируем матрицу A размером $n \times n$:

$$A = \begin{bmatrix} |b_1\rangle & |b_2\rangle & \cdots & |b_n\rangle \end{bmatrix},$$

затем транспонируем ее.

$$A^T = \begin{bmatrix} \langle b_1| \\ \langle b_2| \\ \vdots \\ \langle b_n| \end{bmatrix}.$$

Затем найдем произведение A^TA.

$$A^T A = \begin{bmatrix} \langle b_1| \\ \langle b_2| \\ \vdots \\ \langle b_n| \end{bmatrix} \begin{bmatrix} |b_1\rangle & |b_2\rangle & \cdots & |b_n\rangle \end{bmatrix} = \begin{bmatrix} \langle b_1|b_1\rangle & \langle b_1|b_2\rangle & \cdots & \langle b_1|b_n\rangle \\ \langle b_2|b_1\rangle & \langle b_2|b_2\rangle & \cdots & \langle b_2|b_n\rangle \\ \vdots & \vdots & \vdots & \vdots \\ \langle b_n|b_1\rangle & \langle b_n|b_2\rangle & \cdots & \langle b_n|b_n\rangle \end{bmatrix}.$$

Обратите внимание, что элементы на главной диагонали получившейся матрицы свидетельствуют о том, являются ли кеты единичными, а элементы вне диагонали свидетельствуют об ортогональности соответствующих пар кетов. Это означает, что множество векторов является ортонормированным базисом тогда и только тогда, когда $A^TA = I_n$. Это уравнение позволяет кратко выразить все, что нужно проверить.

Несмотря на компактность выражения, мы все равно должны выполнить вычисления, чтобы найти все элементы. Нужно вычислить все элементы главной диагонали, чтобы проверить, являются ли все векторы единичными. Но вычислять элементы, находящиеся в матрице под главной диагональю, не нужно. Если $i \neq j$, тогда один из пары элементов, $\langle b_i|b_k\rangle$ или $\langle b_k|b_i\rangle$, будет находиться выше, а другой ниже главной диагонали. Эти два произведения бра-кет равны, и поэтому достаточно вычислить только одно из них. После проверки диагональных элементов на равенство 1 нам останется лишь проверить, что все элементы над (или под) главной диагональю равны 0.

Теперь, убедившись, что $\{|b_1\rangle, |b_2\rangle, \cdots, |b_n\rangle\}$ является ортонормированным базисом, предположим, что у нас имеется кет $|v\rangle$ и требуется выразить его как линейную комбинацию базисных векторов. Мы уже знаем, как это сделать.

$$|v\rangle = \langle b_1|v\rangle|b_1\rangle + \langle b_2|v\rangle|b_2\rangle + \cdots + \langle b_t|v\rangle|b_t\rangle + \cdots + \langle b_n|v\rangle|b_n\rangle.$$

Все необходимые вычисления можно выполнить с помощью матрицы A^T.

$$A^T|v\rangle = \begin{bmatrix} \langle b_1| \\ \langle b_2| \\ \vdots \\ \langle b_n| \end{bmatrix} |v\rangle = \begin{bmatrix} \langle b_1|v\rangle \\ \langle b_2|v\rangle \\ \vdots \\ \langle b_n|v\rangle \end{bmatrix}.$$

Это была длинная глава, в которой мы познакомились с обширным математическим аппаратом. Но математический фундамент построен, и теперь в нашем распоряжении множество способов выполнения вычислений. Три ключевые идеи, которые понадобятся нам позже, обобщены в заключительном разделе. (Я поместил их описание в конец главы, чтобы потом было проще найти их.) Но прежде чем закончить, познакомимся с некоторыми соглашениями о выборе имен.

Ортогональные и унитарные матрицы

Квадратная матрица M, состоящая из действительных чисел и для которой произведение M^TM дает единичную матрицу, называется *ортогональной* матрицей.

Как было показано в предыдущем разделе, чтобы проверить, является ли множество кетов ортонормированным базисом, можно сформировать матрицу из этих кетов, а затем проверить ортогональность получившейся матрицы. Ортогональные матрицы пригодятся нам, когда мы будем рассматривать квантовые логические вентили. Эти вентили тоже соответствуют ортогональным матрицам.

Вот две важные ортогональные матрицы:

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix} \text{ и } \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Матрица 2×2 соответствует упорядоченному базису $\left(|\leftarrow\rangle, |\rightarrow\rangle\right)$, с которым мы встретимся в следующей главе. Там мы увидим, как он связан

с измерением спина в горизонтальном направлении. Потом мы еще несколько раз встретимся с этой матрицей. Эта матрица соответствует специальному вентилю, который называется *вентилем Адамара* (Hadamard gate).

Матрица 4×4 соответствует стандартному базису для $\mathbb{R}^4$ и упорядочению с чередованием двух последних векторов. Эта матрица связана с вентилем *CNOT*. Что такое вентили, я расскажу позже, но отмечу, что практически все квантовые цепи состоят только из вентилей этих двух типов. То есть эти ортогональные матрицы играют очень важную роль!

(Если бы мы использовали комплексные числа, элементы матриц могли бы быть комплексными числами. Матрицы с комплексными элементами, подобные ортогональным матрицам, называют *унитарными*.[1] Действительные числа являются подмножеством комплексных чисел, поэтому все ортогональные матрицы одновременно являются унитарными. Заглянув практически в любую книгу по квантовым вычислениям, вы увидите, что в них матрицы вентиля *CNOT* и вентиля Адамара называются унитарными, но мы будем называть их ортогональными. И то и другое правильно.)

Инструменты линейной алгебры

Далее перечисляются три основные задачи, которые мы будем решать снова и снова. Все они достаточно простые. Для каждой приводится метод ее решения.

(1) Дано множество n-мерных кетов $\{|b_1\rangle, |b_2\rangle, \cdots, |b_n\rangle\}$. Требуется проверить, является ли оно ортонормированным базисом.

Для этого сначала нужно сконструировать матрицу $A = \begin{bmatrix} |b_1\rangle & |b_2\rangle & \cdots & |b_n\rangle \end{bmatrix}$. Затем вычислить A^TA. Если в результате получится единичная матрица, значит, это множество является ортонормированным базисом.

[1] Матрица M является унитарной, если $M^\dagger M$ является единичной матрицей, где $M^\dagger$ означает сначала транспонирование матрицы M, а затем взятие сопряжений для всех элементов.

(2) Дан ортонормированный базис $\{|b_1\rangle, |b_2\rangle, \cdots, |b_n\rangle\}$ и кет $|v\rangle$. Требуется выразить этот кет в виде линейной комбинации базисных векторов, то есть решить уравнение

$$|v\rangle = x_1|b_1\rangle + x_2|b_2\rangle + \cdots x_i|b_i\rangle \cdots + x_n|b_n\rangle.$$

Для этого сначала нужно сконструировать матрицу $A = \begin{bmatrix} |b_1\rangle & |b_2\rangle & \cdots & |b_n\rangle \end{bmatrix}$. Затем матрицу

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = A^T|v\rangle = \begin{bmatrix} \langle b_1|v\rangle \\ \langle b_2|v\rangle \\ \vdots \\ \langle b_n|v\rangle \end{bmatrix}.$$

(3) Дан ортонормированный базис $\{|b_1\rangle, |b_2\rangle, \cdots, |b_n\rangle\}$ и $|v\rangle = c_1|b_1\rangle + c_2|b_2\rangle + \cdots c_i|b_i\rangle \cdots + c_n|b_n\rangle$. Требуется найти длину $|v\rangle$.

Используйте формулу $\||v\rangle\|^2 = c_1^2 + c_2^2 + \cdots c_i^2 \cdots + \cdots c_n^2$.

Теперь, имея необходимые инструменты, вернемся к изучению спина.

3 Спин и кубиты

В главе 1 описывались особенности измерения спина электрона. Мы видели, что при измерении спина в вертикальном направлении получается не непрерывный диапазон значений, а только два из них: северный полюс электрона направлен либо вертикально вверх, либо вертикально вниз. Если измерить спин в вертикальном направлении, а потом еще раз в том же направлении, в обоих случаях мы получим один и тот же результат. Если первое измерение покажет, что северный полюс электрона направлен вверх, то и второе измерение покажет то же самое. Мы также видели, что если сначала провести измерение в вертикальном направлении, а затем в горизонтальном, половина электронов будет иметь спин *N*, а половина — спин *S* в направлении 90°. Совершенно неважно, в каком направлении выполнялось первое измерение; второе измерение даст случайный выбор между *N* и *S*. В главе 2 был представлен математический аппарат линейной алгебры. Цель этой главы — соединить знания, полученные в двух первых главах, и представить математическую модель, описывающую измерение спина. Затем я покажу, как эта модель связана с кубитами. Но перед этим познакомимся с математикой вероятности.

Вероятность

Представьте, что мы много раз подряд бросаем монету и подсчитываем количество бросков и выпадений решки. Если монета правильная, без изъянов, то она с равной вероятностью будет падать орлом или решкой

вверх — отношение числа выпадений решки к общему число бросков будет близко к 1/2. Мы говорим, что вероятность исхода «решка» равна 0,5.

В общем случае эксперимент — мы будем называть эксперименты измерениями — имеет ограниченное число возможных исходов. Обозначим их как E_1, E_2, ..., E_n. Также примем, что результатом эксперимента, или измерения, может быть только один из этих исходов. Выпадение результата E_i имеет *вероятность* p_i. Вероятности — это числа от 0 до 1 и сумма вероятностей всех исходов равна 1. В случае с броском монеты возможны два исхода, орел или решка. Если монета правильная, без изъянов, вероятность каждого события равна 1/2.

А теперь вернемся к экспериментам со спином частиц из главы 1 и используем чуть более формальные обозначения для их описания. Допустим, мы собираемся измерить спин в направлении 0°. В данном случае возможны два исхода, которые мы обозначим как *N* и *S*. Оба связаны с определенной вероятностью. Обозначим через p_N вероятность исхода *N*, а через p_S — вероятность исхода *S*. Если мы уже знаем, что электрон имеет спин *N* в направлении 0°, то при повторном измерении в том же направлении мы получим тот же результат, то есть в этом случае $p_N = 1$, а $p_S = 0$. С другой стороны, если известно, что электрон имеет спин *N* в направлении 90° и повторное измерение выполняется в направлении 0°, мы с равной вероятностью получим исход *N* или *S*, то есть в этом случае $p_N = p_S = 0{,}5$.

Математика квантового спина

Теперь познакомимся с математической моделью, описывающей квантовый спин. В ней используются и вероятности, и векторы.

Основная модель задается векторным пространством. Измерение имеет множество возможных исходов. Число исходов определяется размерностью этого базового векторного пространства. Любое измерение спина имеет лишь два возможных исхода, то есть базовое векторное пространство является двумерным. Возьмем пространство $\mathbb{R}^2$ — это стандартная двумерная плоскость, которую все мы хорошо знаем. В нашем случае это вполне оправданно, потому что мы вращаем измерительную установку только в одной плоскости. Если бы мы захотели рассмотреть все воз-

можные углы поворота установки в трехмерном пространстве, базовое векторное пространство все равно осталось бы двумерным — любое измерение всегда дает один из двух возможных результатов, — но вместо векторов с действительными числами нам пришлось бы использовать векторы с комплексными элементами. В этом случае базовым векторным пространством было бы комплексное двумерное пространство, обозначаемое как $\mathbb{C}^2$. По причинам, перечисленным в предыдущей главе, нас вполне устроит $\mathbb{R}^2$.

Мы будем рассматривать не все векторы в $\mathbb{R}^2$, а только единичные. Для кетов это означает, что мы ограничимся формулой $|v\rangle = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}$, где $c_1^2 + c_2^2 = 1$. Выбор направления для измерения спина соответствует выбору упорядоченного ортонормированного базиса $(|b_1\rangle, |b_2\rangle)$. Два вектора в базисе соответствуют двум возможным результатам измерений. Мы всегда будем ассоциировать *N* с первым базисным вектором и *S* — со вторым. До измерения частица имеет *состояние спина*, которое определяется линейной комбинацией $|b_1\rangle$ и $|b_2\rangle$, то есть имеет форму $c_1|b_1\rangle + c_2|b_2\rangle$. Иногда мы будем называть его *вектором состояния* или просто *состоянием*. После измерения вектор состояния перейдет в $|b_1\rangle$ или $|b_2\rangle$. Это одна из основных идей квантовой механики: измерение вызывает изменение вектора состояния. Новое состояние является одним из базисных векторов, связанных с измерением. Вероятность получения конкретного базисного вектора определяется начальным состоянием. Вероятность получить $|b_1\rangle$ равна c_1^2; вероятность получить $|b_2\rangle$ равна c_2^2. Числа c_1 и c_2 называются *амплитудами вероятности*. Важно помнить, что амплитуды вероятности не являются вероятностями. Они могут быть положительными или отрицательными. Вероятностями являются квадраты этих чисел. Чтобы добавить конкретики, вернемся к экспериментам, в которых мы измеряли спин в вертикальном и горизонтальном направлениях.

Как отмечалось в предыдущей главе, упорядоченный ортонормированный базис соответствует измерению спина в вертикальном направлении и задается парой векторов $(|\uparrow\rangle, |\downarrow\rangle)$, где $|\uparrow\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ и $|\downarrow\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$. Первый вектор в базисе соответствует электрону со спином *N* в направлении 0°, а второй вектор — электрону со спином *S* в направлении 0°.

Спин в горизонтальном направлении задается упорядоченным ортонормированным базисом $\left(\left|\rightarrow\right\rangle,\left|\leftarrow\right\rangle\right)$, где

$$\left|\rightarrow\right\rangle=\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{-1}{\sqrt{2}}\end{bmatrix} \text{ и } \left|\leftarrow\right\rangle=\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{bmatrix}.$$

Первый вектор соответствует электрону со спином *N* в направлении 90°, а второй вектор — электрону со спином *S* в направлении 90°.

Сначала мы измеряем спин в вертикальном направлении. Первоначально мы можем не знать состояние спина входящего электрона, но это должен быть единичный вектор, и поэтому его можно записать как $c_1\left|\uparrow\right\rangle+c_2\left|\downarrow\right\rangle$, где $c_1^2+c_2^2=1$. Теперь выполним измерение. Электрон отклонится либо вверх, и в этом случае перейдет в состояние $\left|\uparrow\right\rangle$, либо вниз, и в этом случае перейдет в состояние $\left|\downarrow\right\rangle$. Вероятность отклонения вверх равна c_1^2, а вероятность отклонения вниз равна c_2^2.

Теперь повторим тот же эксперимент, измерив спин еще раз в вертикальном направлении. Допустим, что первая пара магнитов отклонила электрон вверх. Мы знаем, что он имеет состояние спина $\left|\uparrow\right\rangle=1\left|\uparrow\right\rangle+0\left|\downarrow\right\rangle$. После повторного измерения состояние перейдет в $\left|\uparrow\right\rangle$ с вероятностью $1^2=1$ или в $\left|\downarrow\right\rangle$ с вероятностью $0^2=0$. Это означает, что он просто останется в состоянии $\left|\uparrow\right\rangle$ и снова отклонится вверх.

Аналогично, если при первом измерении электрон отклонился вниз, он окажется в состоянии $\left|\downarrow\right\rangle=0\left|\uparrow\right\rangle+1\left|\downarrow\right\rangle$. Сколько бы измерений в вертикальном направлении мы ни провели, он все равно останется в этом состоянии, то есть сколько бы раз мы ни повторили эксперимент, электрон всегда будет отклоняться вниз. Как отмечалось в предыдущей главе, повторив тот же эксперимент, мы получим тот же результат.

Теперь, вместо многократного измерения спина в вертикальном направлении, измерим его сначала в вертикальном направлении, а затем в горизонтальном. Допустим, что мы только что выполнили первое измерение — измерение в вертикальном направлении — и выяснили, что электрон имеет спин *N* в направлении 0°. Теперь он имеет вектор состояния $\left|\uparrow\right\rangle$. Поскольку следующее измерение выполняется в горизонтальном направлении, мы

должны записать этот вектор в терминах ортонормированного базиса, соответствующего этому направлению, то есть мы должны найти значения x_1 и x_2, являющиеся решением уравнения $|\uparrow\rangle = x_1|\rightarrow\rangle + x_2|\leftarrow\rangle$. Мы уже знаем, как это сделать: это второй инструмент из перечисленных в конце предыдущей главы.

Сначала сконструируем матрицу A, расположив кеты из ортонормированного базиса друг за другом.

$$A = \left[|\rightarrow\rangle|\leftarrow\rangle\right] = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}.$$

Затем вычислим $A^T|\uparrow\rangle$, чтобы получить амплитуды вероятности относительно нового базиса.

$$A^T|\uparrow\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}.$$

В результате получаем $|\uparrow\rangle = \frac{1}{\sqrt{2}}|\rightarrow\rangle + \frac{1}{\sqrt{2}}|\leftarrow\rangle$.

В результате измерения в горизонтальном направлении состояние переходит в $|\rightarrow\rangle$ с вероятностью $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$ или в $|\leftarrow\rangle$ с вероятностью $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$. То есть вероятность, что электрон будет иметь спин N в направлении 90°, равна вероятности, что он будет иметь спин S в направлении 90°; обе вероятности равны точно половине.

Обратите внимание, что в действительности в этих расчетах не требовалось вычислять матрицу A. На самом деле нам нужна была только матрица A^T. Эту матрицу можно получить, если взять бра, соответствующие ортонормированному базису, и расположить их друг под другом. Конечно, векторы должны следовать в том же порядке. Порядок слева направо следования кетов соответствует порядку сверху вниз следования бра, то есть первый элемент базиса будет самым верхним бра.

В одном из экспериментов в главе 1 мы измеряли спин три раза. Первое и третье измерения производились в вертикальном направлении, а второе — в горизонтальном. Опишем третье измерение в математических терминах. После второго измерения вектор состояния нашего электрона будет иметь одно из двух значений: $|\rightarrow\rangle$ или $|\leftarrow\rangle$. Теперь мы собираемся выполнить измерение в вертикальном направлении, поэтому выразим его как линейную комбинацию вертикального ортонормированного базиса. В результате получаем

$$|\rightarrow\rangle = \frac{1}{\sqrt{2}}|\uparrow\rangle - \frac{1}{2}|\downarrow\rangle \text{ и } |\leftarrow\rangle = \frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{2}|\downarrow\rangle.$$

В любом случае, в результате измерения спина в вертикальном направлении вектор состояния будет переходить либо в значение $|\uparrow\rangle$, либо в значение $|\downarrow\rangle$, то есть с вероятностью, равной половине.

Эквивалентные векторы состояний

Допустим, дано некоторое число электронов и сказано, что их спины задаются как $|\uparrow\rangle$ или $-|\uparrow\rangle$. Можно ли различить эти два случая? Есть ли такой способ измерения, с помощью которого мы могли бы отличить их друг от друга? Ответ на этот вопрос: «нет».

Чтобы убедиться в этом, предположим, что мы выбираем направление для измерения спина. Это равносильно выбору упорядоченного ортонормированного базиса. Обозначим этот базис как $(|b_1\rangle, |b_2\rangle)$.

Допустим, что электрон имеет состояние $|\uparrow\rangle$. Мы должны найти значения a и b, являющиеся решением уравнения $|\uparrow\rangle = a|b_1\rangle + b|b_2\rangle$. Вероятность, что в результате измерения спин будет иметь значение N, равна a^2, а вероятность, что спин будет иметь значение S, равна b^2.

Теперь допустим, что электрон имеет состояние $-|\uparrow\rangle$. Для тех же самых значений a и b мы имеем $-|\uparrow\rangle = -a|b_1\rangle - b|b_2\rangle$. То есть вероятность, что в результате измерения спин будет иметь значение N, равна $(-a)^2 = a^2$, а вероятность, что спин будет иметь значение S, равна $(-b)^2 = b^2$.

В обоих случаях мы получили одинаковые вероятности, а это значит, что нет такого способа измерения, с помощью которого можно было бы различить электроны с векторами состояний $|\uparrow\rangle$ и $-|\uparrow\rangle$.

Аналогично, электроны с состоянием $|v\rangle$ невозможно отличить от электронов с состоянием $-|v\rangle$. Так как эти состояния неразличимы, они считаются эквивалентными. Утверждение, что электрон имеет спин, заданный вектором $|v\rangle$, равноценно утверждению, что электрон имеет спин, заданный вектором $-|v\rangle$.

Для дополнительной иллюстрации этого обстоятельства рассмотрим четыре кета:

$$\frac{1}{\sqrt{2}}|\uparrow\rangle+\frac{1}{\sqrt{2}}|\downarrow\rangle \quad -\frac{1}{\sqrt{2}}|\uparrow\rangle-\frac{1}{\sqrt{2}}|\downarrow\rangle \quad \frac{1}{\sqrt{2}}|\uparrow\rangle-\frac{1}{\sqrt{2}}|\downarrow\rangle \quad -\frac{1}{\sqrt{2}}|\uparrow\rangle+\frac{1}{\sqrt{2}}|\downarrow\rangle.$$

Согласно предыдущему замечанию, мы знаем, что

$$\frac{1}{\sqrt{2}}|\uparrow\rangle+\frac{1}{\sqrt{2}}|\downarrow\rangle \text{ и } -\frac{1}{\sqrt{2}}|\uparrow\rangle-\frac{1}{\sqrt{2}}|\downarrow\rangle$$

эквивалентны и что

$$\frac{1}{\sqrt{2}}|\uparrow\rangle-\frac{1}{\sqrt{2}}|\downarrow\rangle \text{ и } -\frac{1}{\sqrt{2}}|\uparrow\rangle+\frac{1}{\sqrt{2}}|\downarrow\rangle$$

тоже эквивалентны. Эти четыре кета описывают, самое большее, два различимых состояния. Но что можно сказать о состояниях

$$\frac{1}{\sqrt{2}}|\uparrow\rangle+\frac{1}{\sqrt{2}}|\downarrow\rangle \text{ и } \frac{1}{\sqrt{2}}|\uparrow\rangle-\frac{1}{\sqrt{2}}|\downarrow\rangle?$$

Являются ли они отличными друг от друга состояниями или нет?

Ответ на этот вопрос требует внимательности. Если говорить об измерении спина в вертикальном направлении, эти два кета неразличимы. В обоих случаях мы получим, что вероятности $|\uparrow\rangle$ и $|\downarrow\rangle$ равны половине. Но мы знаем, что

$$\frac{1}{\sqrt{2}}|\uparrow\rangle+\frac{1}{\sqrt{2}}|\downarrow\rangle=|\leftarrow\rangle \text{ и } \frac{1}{\sqrt{2}}|\uparrow\rangle-\frac{1}{\sqrt{2}}|\downarrow\rangle=|\rightarrow\rangle.$$

Следовательно, если измерение производится в направлении 90°, для первого кета мы получим *S*, а для второго *N*. Этот базис различает их, значит, они не эквивалентны.

И еще одно, что пока остается не совсем ясным, — как выбирается базис, связанный с направлением измерения. Мы уже видели, что измерению в вертикальном (0°) направлении соответствует базис

$$\left(\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix}\right),$$

а измерению в горизонтальном (90°) направлении соответствует базис

$$\left(\begin{bmatrix}\frac{1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{bmatrix},\begin{bmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{bmatrix}\right).$$

Но откуда взялись эти базисы? Позже, когда мы будем знакомиться с теоремой Белла, нам понадобятся базисы, соответствующие направлениям 120° и 240°. Как они выглядят? На этот вопрос мы ответим в следующем разделе.

Базис, соответствующий заданному направлению спина

Начнем с измерительной установки. В качестве отправной точки выберем вертикальное направление, а затем начнем поворачивать установку по часовой стрелке. Как уже отмечалось, при повороте на 90° измерения производятся в горизонтальном направлении. Когда угол поворота составит 180°, мы вновь будем измерять в вертикальном направлении. Электрон, имеющий спин *N* в направлении 0°, будет иметь спин *S* в направлении 180°, а электрон, имеющий спин *S* в направлении 0°, будет иметь спин *N* в направлении 180°. Очевидно, что северный полюс магнита в одном направлении передает в точности ту же информацию, что и южный полюс магнита в противоположном направлении, а значит, нам достаточно по-

ворачивать установку на углы в диапазоне от 0° до 180°, чтобы охватить все возможные направления.

Теперь перейдем к базисам. За отправную точку возьмем стандартный базис $\left(\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\right)$. Его можно изобразить двумя векторами на координатной плоскости, как показано на рис. 3.1.

Теперь повернем эти векторы. Обобщенный случай поворота векторов на угол α° изображен на рис. 3.2. Вектор $\begin{bmatrix}1\\0\end{bmatrix}$ после поворота превращается в вектор $\begin{bmatrix}\cos(\alpha)\\-\sin(\alpha)\end{bmatrix}$, а вектор $\begin{bmatrix}0\\1\end{bmatrix}$ в превращается в вектор $\begin{bmatrix}\sin(\alpha)\\\cos(\alpha)\end{bmatrix}$.

Поворот на угол α° изменяет первоначальный упорядоченный ортонормированный базис $\left(\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\right)$, превращая его в $\left(\begin{bmatrix}\cos(\alpha)\\-\sin(\alpha)\end{bmatrix}, \begin{bmatrix}\sin(\alpha)\\\cos(\alpha)\end{bmatrix}\right)$.

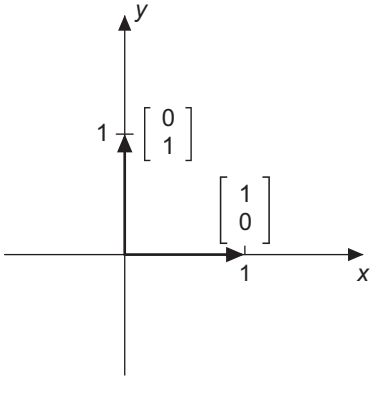


Рис. 3.1. Стандартный базис

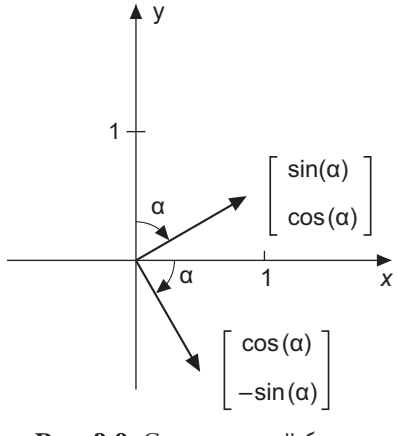
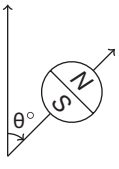


Рис. 3.2. Стандартный базис после поворота на α°

Если стандартный базис повернуть на 90°, он превратится в

$$\left(\begin{bmatrix}\cos(90^\circ)\\-\sin(90^\circ)\end{bmatrix}, \begin{bmatrix}\sin(90^\circ)\\\cos(90^\circ)\end{bmatrix}\right),$$

или, после упрощения, в $\left(\begin{bmatrix}0\\-1\end{bmatrix}, \begin{bmatrix}1\\0\end{bmatrix}\right)$. Как уже отмечалось выше, $\begin{bmatrix}0\\-1\end{bmatrix}$ и $\begin{bmatrix}0\\1\end{bmatrix}$ эквивалентны, соответственно, поворот на 90° возвращает нас к базису, эквивалентному оригинальному, с одним исключением — элементы базиса поменялись местами (то есть поменялись *N* и *S*).



а) угол измерения

$$\left(\begin{bmatrix}\cos\left(\frac{\theta}{2}\right)\\-\sin\left(\frac{\theta}{2}\right)\end{bmatrix}, \begin{bmatrix}\sin\left(\frac{\theta}{2}\right)\\\cos\left(\frac{\theta}{2}\right)\end{bmatrix}\right)$$

б) базис

Рис. 3.3. Поворот измерительной установки на θ°

Обозначим угол поворота измерительной установки как θ, а угол поворота базисных векторов как α. Мы уже видели, что для охвата всего диапазона направлений достаточно поворачивать установку на углы θ от 0° до 180°, а для охвата всего набора базисов достаточно поворачивать базис на углы α от 0° до 90°. Как только мы достигаем θ = 180° или, что равноценно, α = 90°, значения *N* и *S*, измеренные в направлении 0°, меняются местами.

Отсюда следует естественный вывод, что θ = 2α. Следовательно, базис, соответствующий углу θ поворота установки, определяется как

$$\left(\begin{bmatrix}\cos(\theta/2)\\-\sin(\theta/2)\end{bmatrix}, \begin{bmatrix}\sin(\theta/2)\\\cos(\theta/2)\end{bmatrix}\right).$$

Это показано на рис. 3.3.

Поворот установки на 60°

Для иллюстрации нашей формулы посмотрим, что получится, если повернуть измерительную установку, например, на 60°. Допустим, первое измерение показало, что электрон имеет спин *N* в направлении 0° и для

второго измерения мы повернули установку на 60°. Какова вероятность получить результат *N*?

В этом случае базис измерительной установки будет иметь вид

$$\left(\begin{bmatrix}\cos(30^\circ)\\ -\sin(30^\circ)\end{bmatrix}, \begin{bmatrix}\sin(30^\circ)\\ \cos(30^\circ)\end{bmatrix}\right),$$

или, после упрощения, $\left(\begin{bmatrix}\sqrt{3}/2\\ -1/2\end{bmatrix}, \begin{bmatrix}1/2\\ \sqrt{3}/2\end{bmatrix}\right)$.

Поскольку в первом измерении электрон имел спин *N* в направлении 0°, он имел вектор состояния $\begin{bmatrix}1\\0\end{bmatrix}$. Теперь мы должны выразить его как линейную комбинацию новых базисных векторов. Чтобы получить координаты относительно нового базиса, достаточно просто умножить вектор состояния слева на матрицу, состоящую из бра базиса:

$$\begin{bmatrix}\sqrt{3}/2 & -1/2\\ 1/2 & \sqrt{3}/2\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix}=\begin{bmatrix}\sqrt{3}/2\\ 1/2\end{bmatrix},$$

что в результате дает

$$\begin{bmatrix}1\\0\end{bmatrix}=\sqrt{3}/2\begin{bmatrix}\sqrt{3}/2\\ -1/2\end{bmatrix}+1/2\begin{bmatrix}1/2\\ \sqrt{3}/2\end{bmatrix}.$$

Вероятность получить *N* при измерении в направлении 60° равна $\left(\sqrt{3}/2\right)^2=3/4$.

Математическая модель поляризации фотона

В большей части книги мы ограничимся измерением спинов электронов, но в главе 1 говорилось, что все то же самое можно переписать с точки

зрения поляризации фотонов. Поэтому в следующих нескольких разделах мы поговорим о сходстве между спином электрона и поляризацией фотона и рассмотрим математическую модель поляризации.

Для начала примем, что угол 0° соответствует вертикальной ориентации поляризованного фильтра, то есть фильтр пропускает фотоны, поляризованные вертикально, и поглощает фотоны, поляризованные горизонтально. Так же как в случае со спином электронов, ассоциируем стандартный базис $\left(\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix}\right)$ с углом 0°. Вектор $\begin{bmatrix}1\\0\end{bmatrix}$ будет соответствовать вертикально поляризованным фотонам, а вектор $\begin{bmatrix}0\\1\end{bmatrix}$ — горизонтально поляризованным.

После поворота фильтра на угол β° он будет пропускать фотоны, поляризованные в направлении β°, и поглощать фотоны, поляризованные в направлении, перпендикулярном β°.

Математическая модель аналогична модели спина электронов. Для каждого направления существует упорядоченный ортонормированный базис $\left(|b_1\rangle,|b_2\rangle\right)$, соответствующий измерению поляризации в этом направлении. Кет $|b_1\rangle$ соответствует фотону, поляризованному в данном направлении, то есть свободно проходящему через фильтр. Кет $|b_2\rangle$ соответствует фотону, поляризованному ортогонально данному направлению, то есть поглощаемому фильтром.

Состояние поляризации фотона задается кетом $|v\rangle$. Его можно записать как линейную комбинацию векторов базиса: $|v\rangle = d_1|b_1\rangle + d_2|b_2\rangle$.

Когда поляризация измеряется в направлении, заданном упорядоченным базисом, фотон окажется поляризованным в данном направлении с вероятностью d_1^2 и в перпендикулярном направлении — с вероятностью d_2^2; то есть фотон пройдет через фильтр с вероятностью d_1^2 и будет поглощен им с вероятностью d_2^2.

Если по результатам измерения фотон окажется поляризованным в данном направлении — пройдет через фильтр, — тогда фотон получит состояние $|b_1\rangle$.

Базис, соответствующий заданному направлению поляризации

Как уже рассказывалось выше, если повернуть векторы стандартного базиса $\left(\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix}\right)$ на угол α, получится новый ортонормированный базис

$$\left(\begin{bmatrix}\cos(\alpha)\\-\sin(\alpha)\end{bmatrix},\begin{bmatrix}\sin(\alpha)\\\cos(\alpha)\end{bmatrix}\right).$$

Также говорилось, что поворот на угол 90° возвращает к оригинальному базису, за исключением того, что элементы базиса меняются местами.

Теперь рассмотрим поворот поляризованного фильтра на угол β. Когда угол β равен 0°, поляризация измеряется в вертикальном и горизонтальном направлениях. Вертикально поляризованные фотоны беспрепятственно проходят через фильтр, а горизонтально поляризованные поглощаются им. После поворота на угол β, равный 90°, поляризация фотонов все так же измеряется в вертикальном и горизонтальном направлениях, но на этот раз вертикально поляризованные фотоны поглощаются фильтром, а горизонтально поляризованные беспрепятственно проходят насквозь. Случай $\beta = 90°$ соответствует $\alpha = 90°$, и в общем случае обычно можно допустить $\alpha = \beta$.

В заключение отметим, что упорядоченный ортонормированный базис, соответствующий повороту фильтра на угол β, имеет вид

$$\left(\begin{bmatrix}\cos(\beta)\\-\sin(\beta)\end{bmatrix},\begin{bmatrix}\sin(\beta)\\\cos(\beta)\end{bmatrix}\right).$$

Эксперименты с поляризованными фильтрами

Используя нашу модель, опишем эксперименты, которые мы видели в главе 1.

В первом эксперименте использовались два поляризованных фильтра. Один измерял поляризацию в направлении 0°, а другой в направлении 90°. Через эту пару фильтров свет не проникает, как показано на рис. 3.4.

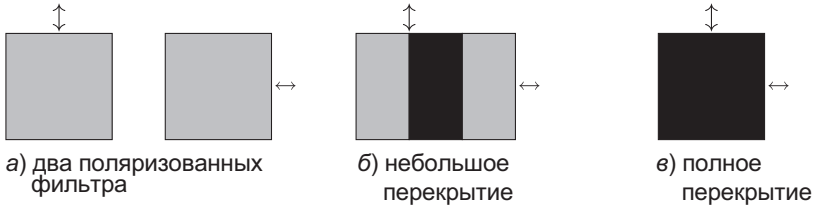


Рис. 3.4. Два поляризованных фильтра

Базис, соответствующий направлению 0°, является стандартным ортонормированным базисом. Базис, соответствующий направлению 90°, тоже является стандартным ортонормированным базисом, но с иным порядком следования элементов. Фотон, прошедший сквозь первый фильтр, вертикально поляризован, поэтому он находится в состоянии $\begin{bmatrix}1\\0\end{bmatrix}$. Второй фильтр пропускает фотоны с вектором состояния $\begin{bmatrix}0\\1\end{bmatrix}$ и поглощает с вектором состояния $\begin{bmatrix}1\\0\end{bmatrix}$. Следовательно, все фотоны, прошедшие через первый фильтр, будут поглощены вторым фильтром.

В эксперименте с тремя фильтрами мы разместили два фильтра так же, как в предыдущем эксперименте, и между ними вставили третий фильтр, повернутый на угол 45°. Теперь группа из трех фильтров пропускает какую-то долю света, как показано на рис. 3.5.

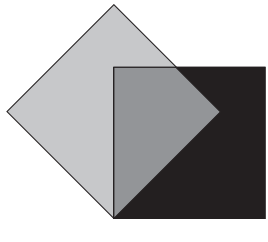


Рис. 3.5. Три поляризованных фильтра

Упорядоченные базисы для трех фильтров имеют вид:

$$\left(\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix}\right),\ \left(\begin{bmatrix}\frac{1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{bmatrix},\begin{bmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{bmatrix}\right) \text{ и } \left(\begin{bmatrix}0\\1\end{bmatrix},\begin{bmatrix}1\\0\end{bmatrix}\right).$$

Фотон, миновавший все три фильтра, пройдет все три измерения. Фотоны, прошедшие через первый фильтр, будут иметь состояние $\begin{bmatrix}1\\0\end{bmatrix}$.

Второе измерение выполняется фильтром, повернутым на 45°. Мы должны переписать состояние фотона с использованием соответствующего базиса:

$$\begin{bmatrix}1\\0\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}\frac{1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{bmatrix}+\frac{1}{\sqrt{2}}\begin{bmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{bmatrix}.$$

Вероятность прохождения фотона через второй фильтр после прохождения через первый равна

$$\left(\frac{1}{\sqrt{2}}\right)^2=\frac{1}{2}.$$

То есть половина фотонов, прошедших через первый фильтр, пройдет и через второй. Прошедшие фотоны теперь будут находиться в состоянии

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

Третий фильтр соответствует измерению с третьим базисом. Перепишем состояние фотона с его использованием:

$$\begin{bmatrix}\frac{1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{bmatrix}=\frac{-1}{\sqrt{2}}\begin{bmatrix}0\\1\end{bmatrix}+\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\end{bmatrix}.$$

Третий фильтр пропускает фотоны с состоянием $\begin{bmatrix}0\\1\end{bmatrix}$. Вероятность этого события равна

$$\left(\frac{-1}{\sqrt{2}}\right)^2 = \frac{1}{2}.$$

Половина фотонов, прошедших через первые два фильтра, пройдет и через третий.

Мы увидели, как математическая модель связывает спин электрона с поляризацией фотона. И эта же модель описывает кубиты.

Кубиты

Классический бит может иметь одно из двух значений, 0 или 1. Он может быть представлен чем угодно, имеющим два взаимоисключающих состояния. Стандартным примером является выключатель, который может находиться в одном из двух состояний, «включено» или «выключено». В классической информатике отсутствует такое понятие, как измерение битов. Бит — это бит. Он может быть или 0, или 1, и это все, что можно о нем сказать. Но ситуация с кубитами намного сложнее, и измерение является важной составляющей математического описания.

Мы определили, что *кубит* может представлять любой единичный кет из $\mathbb{R}^2$. Обычно, если имеется кубит, его требуется измерить. Чтобы измерить его, нужно указать направление измерения. Делается это путем ввода упорядоченного ортонормированного базиса $\left(|b_0\rangle,|b_1\rangle\right)$. Кубит можно записать как линейную комбинацию базисных векторов, которую обычно называют линейной суперпозицией. В общем случае она имеет вид $d_0|b_0\rangle + d_1|b_1\rangle$. После измерения его состояние меняется на $|b_0\rangle$ или $|b_1\rangle$. Вероятность перехода в состояние $|b_0\rangle$ равна d_0^2, а вероятность перехода в состояние $|b_1\rangle$ равна d_1^2. Это все та же модель, что мы использовали до сих пор, но теперь мы связываем классические биты 0 и 1 с базисными векторами. Свяжем базисный вектор $|b_0\rangle$ с битом 0, а базисный вектор $|b_1\rangle$ с битом 1. Итак, измеряя кубит $d_0|b_0\rangle + d_1|b_1\rangle$, мы получим 0 с вероятностью d_0^2 и 1 с вероятностью d_1^2.

Так как кубит может быть любым единичным кетом, а таких единичных кетов бесконечно много, то существует бесконечно большое число возможных значений кубита. Это совсем не похоже на классические вычисления, где биты имеют всего два возможных значения. Однако важно отметить, что для получения информации из кубита его нужно измерить. Измеряя кубит, мы получаем 0 или 1, то есть классический бит.

Рассмотрим несколько показательных примеров с участием Алисы, Боба и Евы.

Алиса, Боб и Ева

Алиса, Боб и Ева — это три персонажа, которые часто появляются в примерах по криптографии. Алиса желает послать конфиденциальное сообщение Бобу. Но беда в том, что Ева имеет злой умысел и хочет прочитать это сообщение. Как Алиса должна зашифровать сообщение, чтобы Боб мог прочитать его, а Ева нет? Это главный вопрос криптографии. Мы еще вернемся к нему, а пока просто остановимся на отправке Алисой потока кубитов Бобу.

Алиса измеряет кубиты, используя ортонормированный базис, который мы обозначим как $(|a_0\rangle, |a_1\rangle)$. Боб измеряет кубиты, присланные Алисой, используя свой ортонормированный базис $(|b_0\rangle, |b_1\rangle)$.

Предположим, что Алиса хочет отправить 0. Она может использовать свою измерительную установку для сортировки кубитов в состоянии $|a_0\rangle$ или $|a_1\rangle$. Так как она хочет послать 0, она посылает кубит в состоянии $|a_0\rangle$. Боб измеряет бит, используя свой упорядоченный базис. Для вычислений требуется записать $|a_0\rangle$ как линейную комбинацию базисных векторов Боба. Она выглядит так: $|a_0\rangle = d_0|b_0\rangle + d_1|b_1\rangle$. Когда Боб измеряет кубит, происходит одно из двух событий: он получает либо состояние $|b_0\rangle$ с вероятностью d_0^2 и записывает 0, либо состояние $|b_1\rangle$ с вероятностью d_1^2 и записывает 1.

Вас может удивить, почему Боб и Алиса не используют один и тот же базис. Если бы они поступили именно так, Боб наверняка получил бы 0, когда Алиса послала 0, и 1 — когда Алиса послала 1. Это верно, но не

забывайте о Еве. Выбрав тот же базис, она получит то же сообщение, что и Боб. Как будет показано позже, для Алисы и Боба есть веские причины выбрать разные базисы, чтобы помешать Еве.

Например, Алиса и Боб могут выбрать для измерения своих кубитов базис

$$\left(\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix}\right)$$

или

$$\left(\begin{bmatrix}\frac{1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{bmatrix},\begin{bmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{bmatrix}\right).$$

Вычисления выполняются точно так же, как в примере, когда мы рассматривали спин в вертикальном и горизонтальном направлениях. Единственное отличие — мы заменили N на 0 и S на 1. Боб получит тот же бит, который хотела послать Алиса, только если они оба выберут один и тот же базис. Если они выберут разные базисы, в половине случаев Боб будет получать правильные биты, а в половине случаев — неправильные. Такой способ передачи информации может показаться бесполезным, но, как будет показано в конце главы, Алиса и Боб вполне могут использовать эти два базиса для защиты своего общения.

Через пару глав мы увидим, как Алиса и Боб будут случайным образом выбирать один из трех базисов, соответствующих измерению спина в направлениях 0°, 120° и 240°. Там нам потребуется проанализировать все возможности, а пока, чтобы получить конкретный пример, предположим, что Алиса выполняет измерения в направлении 240°, а Боб — в направлении 120°.

Мы уже знаем, что ортонормированный базис для направления θ имеет вид

$$\left(\begin{bmatrix}\cos(\theta/2)\\-\sin(\theta/2)\end{bmatrix},\begin{bmatrix}\sin(\theta/2)\\\cos(\theta/2)\end{bmatrix}\right).$$

Соответственно, Алиса использует базис

$$\left(\begin{bmatrix} -1/2 \\ -\sqrt{3}/2 \end{bmatrix}, \begin{bmatrix} \sqrt{3}/2 \\ -1/2 \end{bmatrix}\right),$$

а Боб — базис

$$\left(\begin{bmatrix} 1/2 \\ -\sqrt{3}/2 \end{bmatrix}, \begin{bmatrix} \sqrt{3}/2 \\ 1/2 \end{bmatrix}\right).$$

Так как умножение кета на –1 дает эквивалентный кет, мы можем упростить базис Алисы до

$$\left(\begin{bmatrix} 1/2 \\ \sqrt{3}/2 \end{bmatrix}, \begin{bmatrix} \sqrt{3}/2 \\ -1/2 \end{bmatrix}\right).$$

(Обратите внимание, что этот базис соответствует направлению 60°, которое мы рассматривали выше, но с измененным порядком базисных векторов. В этом нет ничего удивительного. Фактически именно это и ожидалось. Измерение *N* в направлении 240° в точности соответствует измерению *S* в направлении 60°.)

Чтобы послать 0, Алиса должна отправить кубит

$$\begin{bmatrix} 1/2 \\ \sqrt{3}/2 \end{bmatrix}.$$

Чтобы узнать, что Боб получит в результате измерения, мы должны выразить результат как линейную суперпозицию его базисных векторов. Мы можем получить амплитуды вероятности, сформировав матрицу из бра, представляющих его базисные векторы, и умножив кубит на эту матрицу.

$$\begin{bmatrix} 1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{bmatrix} \begin{bmatrix} 1/2 \\ \sqrt{3}/2 \end{bmatrix} = \begin{bmatrix} -1/2 \\ \sqrt{3}/2 \end{bmatrix}.$$

Отсюда следует, что

$$\begin{bmatrix} 1/2 \\ \sqrt{3}/2 \end{bmatrix} = -1/2 \begin{bmatrix} 1/2 \\ -\sqrt{3}/2 \end{bmatrix} + \sqrt{3}/2 \begin{bmatrix} \sqrt{3}/2 \\ 1/2 \end{bmatrix}.$$

Когда Боб измерит кубит, он получит 0 с вероятностью 1/4 и 1 с вероятностью 3/4. Аналогично можно убедиться, что когда Алиса отправит 1, Боб получит 1 с вероятностью 1/4 и 0 с вероятностью 3/4.

Также можно проверить, и это может стать для вас отличным упражнением, что если Алиса и Боб будут иметь выбор из трех базисов, где третий является стандартным базисом, и выберут разные базисы, то Боб всегда будет получать правильный бит с вероятностью 1/4.

Амплитуды вероятности и интерференция

Если бросить камень в воду, волны будут распространяться во все стороны от места падения камня. Если бросить два камня, волны, распространяющиеся от одного камня, могут мешать распространению волн, исходящих от другого камня. Если волны совпадают по фазе, то есть если совпадают гребни и провалы, возникнет эффект конструктивной интерференции (резонанса): амплитуда волн, получившихся в результате их сложения, увеличится. Если волны находятся в противофазе, когда гребень одной волны встречается с провалом другой, возникнет эффект деструктивной интерференции: амплитуда волн, получившихся в результате их сложения, уменьшится.

Кубит имеет вид $d_0|b_0\rangle + d_1|b_1\rangle$, где d_0 и d_1 — амплитуды вероятности. Квадраты этих чисел дают вероятности перехода кубита к соответствующему базисному вектору. Вероятности не могут быть отрицательными, но их амплитуды — вполне. Этот факт допускает появление обоих эффектов, конструктивной и деструктивной интерференции.

В качестве примера рассмотрим кубиты, которые обозначим как $|\leftarrow\rangle$ и $|\rightarrow\rangle$. Если измерить их в стандартном базисе, они перейдут в состояние $|\uparrow\rangle$ или $|\downarrow\rangle$. В обоих случаях вероятность перехода равна 1/2. Если перевести их обратно в биты, мы с равной вероятностью получим 0 или 1. Теперь возьмем суперпозицию двух исходных кубитов,

$$|v\rangle = {}^{1}\!/_{\sqrt{2}}|\leftarrow\rangle + {}^{1}\!/_{\sqrt{2}}|\rightarrow\rangle.$$

Если измерить v в горизонтальном направлении, мы с равной вероятностью получим $|\leftarrow\rangle$ или $|\rightarrow\rangle$. Но если измерение выполнить в вертикальном направлении, мы точно получим 0, потому что

$$|v\rangle = 1/\sqrt{2}|\leftarrow\rangle + 1/\sqrt{2}|\rightarrow\rangle = 1/\sqrt{2}\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{bmatrix} + 1/\sqrt{2}\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{-1}{\sqrt{2}}\end{bmatrix} = 1\begin{bmatrix}1\\0\end{bmatrix} + 0\begin{bmatrix}0\\1\end{bmatrix}.$$

Члены в $|\leftarrow\rangle$, которые дают 0, интерферируют конструктивно, а члены в $|\rightarrow\rangle$, которые дают 1, интерферируют деструктивно.

Это будет важно, когда речь пойдет о квантовых алгоритмах. Мы должны тщательно выбирать линейные комбинации, чтобы члены, которые нас не интересуют, компенсировали друг друга, а члены, представляющие интерес, усиливали друг друга.

С одним кубитом мало что можно сделать, но мы точно можем с его помощью обезопасить общение Алисы и Боба.

Алиса, Боб, Ева и протокол BB84

Мы хотим безопасно отправлять сообщения. Вся электронная коммерция в интернете зависит от этого. Стандартный способ, основанный на шифровании и расшифровывании сообщений, состоит из двух этапов. На первом этапе, когда стороны устанавливают соединение, они договариваются о ключе шифрования — длинной строке двоичных цифр. Достигнув договоренности, они используют один и тот же ключ для кодирования и декодирования сообщений, которыми обмениваются друг с другом. Безопасность зависит от ключа. Невозможно расшифровать сообщения, которыми обмениваются эти две стороны, не имея ключа.

Алиса и Боб хотят иметь возможность безопасно общаться друг с другом. Ева хочет подслушать их диалог. Алиса и Боб должны договориться о ключе, но при этом им нужна уверенность, что Ева не узнает его.

Протокол BB84 получил свое название по именам изобретателей, Чарльза Беннетта (Charles Bennett) и Жиля Брассара (Gilles Brassard), а также

года изобретения, 1984. Он использует два упорядоченных ортонормированных базиса: стандартный $\left(\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix}\right)$, который мы использовали для измерения спина в вертикальном направлении и обозначим как V, и

$$\left(\begin{bmatrix}\frac{1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{bmatrix},\begin{bmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{bmatrix}\right),$$

который мы использовали для измерения спина в горизонтальном направлении и обозначим как H. В обоих случаях классический бит 0 будет соответствовать первому вектору в упорядоченном базисе, а 1 — второму.

Алиса выбирает ключ, который она хочет отправить Бобу. Это строка классических битов. Для каждого бита Алиса случайно и с равной вероятностью выбирает один из двух базисов, V или H. Затем она посылает Бобу кубит, состоящий из соответствующего базисного вектора. Например, чтобы послать 0 при выбранном базисе V, она посылает $\begin{bmatrix}1\\0\end{bmatrix}$, при выбранном базисе H она посылает

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

Этот процесс повторяется для каждого бита и для каждого запоминается использовавшийся базис. Для строки из $4n$ двоичных цифр она получит строку из символов V и H длиной $4n$. (Причина, почему используется длина $4n$, а не n, станет ясна чуть ниже, но n должно быть довольно большим числом.)

Боб тоже делает случайный выбор из двух базисов с равной вероятностью. Затем измеряет кубит в выбранном им базисе. Он делает это для каждого бита и для каждого запоминает использовавшийся базис. По окончании передачи он также получает две строки длиной $4n$: одну, состоящую из

нулей и единиц, и другую, состоящую из символов V и H, соответствующих выбранным базисам.

Алиса и Боб выбирают базис для каждого бита случайно. В половине случаев они используют один и тот же базис, а в половине — разные базисы. Если они выберут один и тот же базис, Боб получит тот же бит, что был отправлен Алисой. Если они выберут разные базисы, в половине случаев Боб получит верный бит, а в половине — неверный, то есть когда они выбирают разные базисы, никакой информации не передается.

После этого Алиса и Боб сравнивают свои строки из символов V и H в незашифрованном виде. Они оставляют биты, соответствующие случаям, когда использовался один и тот же базис, и стирают все остальные. Если Ева не перехватила сообщение, они оба получат одну и ту ж строку двоичных цифр длиной около $2n$. Теперь они должны проверить, не подслушала ли их Ева.

Если Ева перехватила кубит по пути от Алисы к Бобу, по логике вещей она должна была бы клонировать его, чтобы одну копию отправить Бобу, а другую измерить. К несчастью Евы, это невозможно. Чтобы извлечь любую информацию, она должна измерить кубит, отправленный Алисой, но это может изменить его — он превратится в один из векторов в базисе, выбранном Евой для измерения. Лучшее, что она может сделать, — выбрать случайно один из двух базисов, измерить кубит и послать его Бобу. Давайте посмотрим, что из этого получится.

Для Алисы и Боба интерес представляют только те измерения, в которых они выбрали одинаковый базис. Ограничимся только этими случаями. В половине случаев, когда Алиса и Боб выбирают одинаковый базис, Ева будет выбирать тот же самый базис, но в половине случаев она выберет другой базис. Если все три базиса одинаковые, все они получат один и тот же бит в результате измерения. Если Ева выберет неверный базис, она отправит кубит, который находится в суперпозиции базисных состояний Боба. Когда Боб измерит этот кубит, он получит 0 или 1 с равной долей вероятности, то есть он получит правильный ответ в половине случаев.

Теперь вернемся к Алисе и Бобу и их строкам битов, которые на данный момент имеют длину $2n$. Они знают, что если Ева не перехватывала кубиты, эти строки будут идентичны. А если Ева перехватывала кубиты,

в половине случаев она выбирала неверный базис, и в этих случаях Боб будет получать неверные биты. То есть если Ева перехватывала кубиты, четверть битов Боба не будет совпадать с битами у Алисы. Теперь они сравнивают половину из $2n$ битов в незашифрованном виде. Если они совпадают, значит, Ева не подслушивала и другие n битов можно использовать как ключ. Если четверть битов не совпала, значит, Ева перехватывала их кубиты и Алисе с Бобом следует подыскать другой способ обезопасить свое общение.

Это хороший пример отправки информации по одному кубиту за раз. Однако с кубитами, которые не взаимодействуют друг с другом, сделать можно очень немного. В следующей главе мы посмотрим, что происходит в случаях, когда имеется два или более кубита. В частности, мы рассмотрим еще одно явление, которое не встречается в обыденной жизни, но играет важную роль в квантовом мире: запутанность.

4 Запутанность

В этой главе мы познакомимся с математической моделью запутанности. Для этого нам понадобится ввести в обиход еще одну идею из линейной алгебры: тензорное произведение. Сначала мы рассмотрим две системы, не взаимодействующие между собой. Благодаря отсутствию взаимодействий мы сможем изучать обе системы по отдельности, без учета наличия другой системы, но посмотрим, как можно объединить две системы, используя тензорные произведения. Затем мы введем понятие тензорного произведения двух векторных пространств и увидим, что большинство векторов в этом произведении представляют то, что мы называем запутанными состояниями.

На протяжении этой главы мы будем работать с двумя кубитами, один из которых находится у Алисы и другой — у Боба. Для начала рассмотрим случай, когда системы Алисы и Боба никак не взаимодействуют. На первый взгляд этот анализ может показаться чем-то очень простым, что выглядит сложно, но когда мы опишем все в терминах тензорных произведений, мы легко сможем распространить основные идеи на более общий случай запутанности.

Однако на этот раз мы используем иной подход, отличающийся от подхода, использовавшегося до сих пор. Вместо знакомства с физическим экспериментом с последующим выводом математической модели мы пойдем другим путем. Мы немного расширим нашу модель и затем посмотрим, что она предсказывает при выполнении экспериментов. Мы увидим, что модель точно предсказывает исход экспериментов, но выводы окажутся довольно неожиданными.

Кубиты Алисы и Боба не запутаны

Допустим, что Алиса производит измерения с использованием ортонормированного базиса $\left(|a_0\rangle,|a_1\rangle\right)$, а Боб — с использованием ортонормированного базиса $\left(|b_0\rangle,|b_1\rangle\right)$. Соответственно, состояние кубита Алисы определяется формулой $|v\rangle = c_0|a_0\rangle + c_1|a_1\rangle$, а состояние кубита Боба — формулой $|w\rangle = d_0|b_0\rangle + d_1|b_1\rangle$. Эти два вектора состояния можно объединить с помощью произведения нового типа, которое называется *тензорным* произведением и возвращает новый вектор, обозначаемый как $|v\rangle \otimes |w\rangle$.

То есть $|v\rangle \otimes |w\rangle = \left(c_0|a_0\rangle + c_1|a_1\rangle\right) \otimes \left(d_0|b_0\rangle + d_1|b_1\rangle\right)$. Как произвести умножение этих двух членов? Самым естественным образом. Раскроем скобки как обычно и выполним алгебраическое умножение вида $(a + b)(c + d)$:

$$\left(c_0|a_0\rangle + c_1|a_1\rangle\right) \otimes \left(d_0|b_0\rangle + d_1|b_1\rangle\right) =$$
$$= c_0 d_0|a_0\rangle \otimes |b_0\rangle + c_0 d_1|a_0\rangle \otimes |b_1\rangle + c_1 d_0|a_1\rangle \otimes |b_0\rangle + c_1 d_1|a_1\rangle \otimes |b_1\rangle.$$

Знакомые с методом *FOIL* перемножения биномов без труда распознают его в этой формуле. Чтобы упростить терминологию, тензорное произведение двух кетов мы будем обозначать, просто помещая их рядом, то есть $|v\rangle \otimes |w\rangle$ мы будем обозначать как $|v\rangle|w\rangle$.

$$|v\rangle|w\rangle = \left(c_0|a_0\rangle + c_1|a_1\rangle\right)\left(d_0|b_0\rangle + d_1|b_1\rangle\right) =$$
$$= c_0 d_0|a_0\rangle|b_0\rangle + c_0 d_1|a_0\rangle|b_1\rangle + c_1 d_0|a_1\rangle|b_0\rangle + c_1 d_1|a_1\rangle|b_1\rangle.$$

Хотя это всего лишь стандартный способ умножения двух выражений, важно помнить об одном аспекте: первый кет в тензорном произведении принадлежит Алисе, а второй — Бобу. Например, запись $|v\rangle|w\rangle$ означает, что $|v\rangle$ принадлежит Алисе, а $|w\rangle$ принадлежит Бобу. Запись $|w\rangle|v\rangle$ означает, что $|w\rangle$ принадлежит Алисе, а $|v\rangle$ принадлежит Бобу. То есть в общем случае $|v\rangle|w\rangle$ не равно $|w\rangle|v\rangle$. Выражаясь техническим языком, тензорное произведение не обладает свойством коммутативности.

Алиса производит измерения со своим ортонормированным базисом $\left(|a_0\rangle,|a_1\rangle\right)$, а Боб — с ортонормированным базисом $\left(|b_0\rangle,|b_1\rangle\right)$. Опишем кубиты Алисы и Боба с использованием тензорной нотации. Это описание включает четыре тензорных произведения, которые вытекают из базисных векторов: $|a_0\rangle|b_0\rangle$, $|a_0\rangle|b_1\rangle$, $|a_1\rangle|b_0\rangle$ и $|a_1\rangle|b_1\rangle$. Эти четыре произведения

образуют ортонормированный базис тензорного произведения систем Алисы и Боба: каждое из них является единичным вектором и все они ортогональны друг к другу.

Пока мы не встретили никаких новых понятий, несмотря на то что ввели новые обозначения. Все это мы уже видели, хотя и в другой упаковке. Например, число c_0d_0 — это амплитуда вероятности. Ее квадрат дает вероятность перехода кубита Алисы в состояние $|a_0\rangle$ и кубита Боба в состояние $|b_0\rangle$, когда Алиса и Боб измерят свои кубиты, то есть они оба прочитают 0. Но мы уже знали, что вероятность перехода кубита Алисы в состояние $|a_0\rangle$ равна c_0^2, а вероятность перехода кубита Боба в состояние $|b_0\rangle$ равна d_0^2. То есть мы действительно знали, что вероятность обоих переходов равна $c_0^2d_0^2$ или $(c_0d_0)^2$, что то же самое. Аналогично числа $c_0^2d_1^2$, $c_1^2d_0^2$ и $c_1^2d_1^2$ дают вероятности, что Алиса и Боб прочитают 01, 10 и 11 соответственно. (Напомню еще раз, что бит Алисы всегда следует первым.)

Далее, заменим каждую амплитуду вероятности одним символом. Пусть это будет: $r=c_0d_0$, $s=c_0d_1$, $t=c_1d_0$ и $u=c_1d_1$, соответственно $|v\rangle|w\rangle=$ $=r|a_0\rangle|b_0\rangle+s|a_0\rangle|b_1\rangle+t|a_1\rangle|b_0\rangle+u|a_1\rangle|b_1\rangle$. Мы знаем, что $r^2+s^2+t^2+u^2=1$, потому что сумма вероятностей всех возможных исходов всегда равна 1. Мы также знаем, что $ru=st$, потому что оба произведения, ru и st, равны произведению $c_0c_1d_0d_1$. Теперь мы приблизились к новой идее. Опишем состояния кубитов Алисы и Боба тензорами вида $r|a_0\rangle|b_0\rangle+s|a_0\rangle|b_1\rangle+t|a_1\rangle|b_0\rangle+u|a_1\rangle|b_1\rangle$. Памятуя, что $r^2+s^2+t^2+u^2=1$, мы можем интерпретировать r, s, t и u как амплитуды вероятности. Но больше не будем настаивать на справедливости равенства $ru = st$. Мы допустим, что r, s, t и u могут иметь любые значения, при условии, что сумма их квадратов равна 1.

Для данного тензора $r|a_0\rangle|b_0\rangle+s|a_0\rangle|b_1\rangle+t|a_1\rangle|b_0\rangle+u|a_1\rangle|b_1\rangle$ с условием $r^2+s^2+t^2+u^2=1$ возможны два случая. Первый случай — когда $ru = st$. В этом случае мы говорим, что кубиты Алисы и Боба *не запутаны*. Второй случай — когда $ru \neq st$. В этом случае мы говорим, что кубиты Алисы и Боба *запутаны*. Это правило легко запомнить, если члены записать в том порядке, в каком мы их представили: 00, 01, 10, 11. В этом порядке ru соответствует внешним членам, а st — внутренним, то есть кубиты не запутаны, если произведение внешних членов равно произведению внутренних, и они запутаны, если произведения не равны.

Рассмотрим примеры, иллюстрирующие оба этих случая.

Незапутанные кубиты

Предположим, нам известно, что кубиты Алисы и Боба задаются как

$$\frac{1}{2\sqrt{2}}|a_0\rangle|b_0\rangle+\frac{\sqrt{3}}{2\sqrt{2}}|a_0\rangle|b_1\rangle+\frac{1}{2\sqrt{2}}|a_1\rangle|b_0\rangle+\frac{\sqrt{3}}{2\sqrt{2}}|a_1\rangle|b_1\rangle.$$

Отсюда легко найти произведение внешних и внутренних амплитуд вероятности. Оба произведения равны $\sqrt{3/8}$, то есть кубиты не запутаны.

Амплитуды вероятности сообщают нам, что случится, когда оба, Алиса и Боб, выполнят измерения. Они получат 00 с вероятностью 1/8, 01 — с вероятностью 3/8, 10 — с вероятностью 1/8 и 11 — с вероятностью 3/8.

Немного сложнее определить, что случится, если измерение выполнит только кто-то один. Предположим, что Алиса выполнила измерение, а Боб нет. Начнем с выявления общих членов с точки зрения Алисы. Перепишем тензорное произведение как

$$|a_0\rangle\left(\frac{1}{2\sqrt{2}}|b_0\rangle+\frac{\sqrt{3}}{2\sqrt{2}}|b_1\rangle\right)+|a_1\rangle\left(\frac{1}{2\sqrt{2}}|b_0\rangle+\frac{\sqrt{3}}{2\sqrt{2}}|b_1\rangle\right).$$

Далее, нам нужно, чтобы выражения в круглых скобках давали единичные векторы, поэтому разделим на соответствующие длины выражения внутри скобок и умножим за пределами скобок. В результате получаем

$$\frac{1}{\sqrt{2}}|a_0\rangle\left(\frac{1}{2}|b_0\rangle+\frac{\sqrt{3}}{2}|b_1\rangle\right)+\frac{1}{\sqrt{2}}|a_1\rangle\left(\frac{1}{2}|b_0\rangle+\frac{\sqrt{3}}{2}|b_1\rangle\right).$$

Теперь можно вынести общий член за скобки. (Не забывайте, что он принадлежит Бобу, поэтому поместим его справа.)

$$\left(\frac{1}{\sqrt{2}}|a_0\rangle+\frac{1}{\sqrt{2}}|a_1\rangle\right)\left(\frac{1}{2}|b_0\rangle+\frac{\sqrt{3}}{2}|b_1\rangle\right).$$

В такой форме записи ясно видно, что состояния не запутаны. Мы получили тензорное произведение кубита Алисы на кубит Боба.

Отсюда можно сделать вывод, что если Алиса выполнит измерение первой, она с равной вероятностью получит 0 или 1. Это измерение не влияет на состояние кубита Боба. Оно было и остается

$$\left(\frac{1}{2}|b_0\rangle + \frac{\sqrt{3}}{2}|b_1\rangle\right).$$

Также по факторизованному выражению можно определить, что если первым измерение выполнит Боб, он получит 0 с вероятностью 1/4 и 1 с вероятностью 3/4. И снова ясно, что измерение Боба не влияет на кубит Алисы.

Когда кубиты не запутаны, измерение одного кубита никак не влияет на другой кубит. Ситуация кардинально меняется в случае с запутанными кубитами. Если кубиты запутаны, измерение одного влияет на другой. Проиллюстрируем это на примере.

Запутанные кубиты

Предположим, нам известно, что кубиты Алисы и Боба задаются как

$$\frac{1}{2}|a_0\rangle|b_0\rangle + \frac{1}{2}|a_0\rangle|b_1\rangle + \frac{1}{\sqrt{2}}|a_1\rangle|b_0\rangle + 0|a_1\rangle|b_1\rangle.$$

Отсюда легко найти произведение внешних и внутренних амплитуд вероятности. Произведение внешних членов равно 0. Так как произведение внутренних членов не равно 0, два кубита запутаны.

Обычно измерения производят оба участника — и Алиса и Боб. Так же как в предыдущем примере, мы можем использовать амплитуды вероятности, чтобы сказать, что случится, когда Алиса и Боб оба измерят свои кубиты. Они получат 00 с вероятностью 1/4, 01 — с вероятностью 1/4, 10 — с вероятностью 1/2 и 11 — с вероятностью 0. Обратите внимание, что в этом нет ничего необычного. Это те же самые вычисления, как в случае с незапутанными кубитами.

Теперь посмотрим, что случится, если измерение выполнит только кто-то один. Сначала предположим, что Алиса выполнила измерение, а Боб нет.

Начнем с выявления общих членов с точки зрения Алисы. Перепишем тензорное произведение как

$$|a_0\rangle\left(\frac{1}{2}|b_0\rangle+\frac{1}{2}|b_1\rangle\right)+|a_1\rangle\left(\frac{1}{\sqrt{2}}|b_0\rangle+0|b_1\rangle\right).$$

Как и прежде, нам нужно, чтобы выражения в круглых скобках давали единичные векторы, поэтому разделим на соответствующие длины выражения внутри скобок и умножим за пределами скобок. В результате получаем

$$\frac{1}{\sqrt{2}}|a_0\rangle\left(\frac{1}{2}|b_0\rangle+\frac{1}{2}|b_1\rangle\right)+\frac{1}{\sqrt{2}}|a_1\rangle\left(1|b_0\rangle+0|b_1\rangle\right).$$

В предыдущем примере члены в круглых скобках были одинаковые, и мы вынесли их за скобки. Но на этот раз они отличаются. Вот что означает запутанность.

Амплитуды вероятности перед кетами Алисы говорят, что при измерении она с равной вероятностью получит 0 или 1. Но когда Алиса получит 0, ее кубит перейдет в состояние $|a_0\rangle$. Комбинированная система перейдет в незапутанное состояние

$$|a_0\rangle\left(\frac{1}{\sqrt{2}}|b_0\rangle+\frac{1}{\sqrt{2}}|b_1\rangle\right),$$

и кубит Боба больше не будет запутан с кубитом Алисы. Он перейдет в состояние

$$\left(\frac{1}{\sqrt{2}}|b_0\rangle+\frac{1}{\sqrt{2}}|b_1\rangle\right).$$

Когда Алиса получит 1, кубит Боба также больше не будет запутан с кубитом Алисы. Он перейдет в состояние $|b_0\rangle$.

Измерение кубита Алисой влияет на кубит Боба. Если она получит 0, кубит Боба перейдет в состояние

$$\left(\frac{1}{\sqrt{2}}|b_0\rangle+\frac{1}{\sqrt{2}}|b_1\rangle\right).$$

Если она получит 1, кубит Боба перейдет в состояние $|b_0\rangle$. Это кажется странным. Алиса и Боб могут находиться далеко друг от друга. Как только она выполняет измерение, кубит Боба становится незапутанным, но его состояние зависит от результата измерения, полученного Алисой.

Для полноты картины посмотрим, что случится, когда первым выполнит измерение Боб.

Итак, начальное тензорное произведение имеет вид

$$\frac{1}{2}|a_0\rangle|b_0\rangle+\frac{1}{2}|a_0\rangle|b_1\rangle+\frac{1}{\sqrt{2}}|a_1\rangle|b_0\rangle+0|a_1\rangle|b_1\rangle.$$

Переписав его с точки зрения Боба, получаем

$$\left(\frac{1}{2}|a_0\rangle+\frac{1}{\sqrt{2}}|a_1\rangle\right)|b_0\rangle+\left(\frac{1}{2}|a_0\rangle+0|a_1\rangle\right)|b_1\rangle.$$

Как обычно, нам нужно, чтобы выражения в круглых скобках давали единичные векторы, поэтому разделим на соответствующие длины выражения внутри скобок и умножим за пределами скобок. В результате получаем

$$\left(\frac{1}{\sqrt{3}}|a_0\rangle+\frac{\sqrt{2}}{\sqrt{3}}|a_1\rangle\right)\frac{\sqrt{3}}{2}|b_0\rangle+\left(1|a_0\rangle+0|a_1\rangle\right)\frac{1}{2}|b_1\rangle.$$

Измерив свой кубит, Боб получит 0 с вероятностью 3/4 и 1 с вероятностью 1/4. Когда Боб получит 0, кубит Алисы перейдет в состояние

$$\left(\frac{1}{\sqrt{3}}|a_0\rangle+\frac{\sqrt{2}}{\sqrt{3}}|a_1\rangle\right).$$

Когда Боб получит 1, кубит Алисы перейдет в состояние $|a_0\rangle$.

Когда первый участник измерит свой кубит, то кубит второго участника немедленно перейдет в одно из двух состояний, в зависимости от результата измерения, полученного первым участником. Это весьма необычно для нашего опыта повседневной жизни. Позже мы увидим некоторые интересные способы использования запутанных кубитов, но сначала рассмотрим возможность общения со сверхсветовой скоростью.

Общение со сверхсветовой скоростью

Общение со сверхсветовой скоростью — это обмен сообщениями, скорость передачи которых превышает скорость света. Из предположения возможности общения со сверхсветовой скоростью можно сделать два явно противоречивых вывода. Во-первых, специальная теория относительности Эйнштейна утверждает, что при движении с большими скоростями, близкими к скорости света, течение времени для движущегося объекта замедляется. Если бы вы могли двигаться со скоростью света, время для вас остановилось бы. А если бы вы могли двигаться быстрее скорости света, время для вас пошло бы вспять. Также теория утверждает, что при приближении к скорости света масса движущегося объекта увеличивается до бесконечности, таким образом, мы никогда не сможем достичь этой скорости. Кроме того, кажется неправдоподобной возможность вернуться назад во времени. Если бы такое было возможно, мы могли бы столкнуться с ситуацией, описанной во многих фантастических романах, когда путешественник во времени предотвращает некоторое событие, из-за чего меняется ход истории. Проще говоря, путешествие во времени приводит к противоречиям. Это относится не только к физическому путешествию, но и к общению. Если бы мы могли отправлять сообщения назад во времени, мы тоже смогли бы повлиять на ход истории — можно представить ситуацию, когда такое общение может вызвать существенные изменения в настоящем — например, предотвратить наше рождение. Отсюда очевидно вытекает мысль, что общение со сверхсветовой скоростью невозможно.

С другой стороны, предположим, что Алиса и Боб находятся на противоположных концах Вселенной и владеют парами запутанных кубитов. Это электроны с запутанными состояниями спинов. У Алисы и Боба имеется по одному электрону из каждой запутанной пары. (Хотя мы и говорим о запутанных электронах, следует понимать, что эти электроны совершенно независимы друг от друга. Запутаны состояния их спинов.)

Когда Алиса измеряет спин своих электронов, спины соответствующих электронов Боба мгновенно переходят в одно из двух отличных состояний. В данном случае «мгновенно» явно быстрее скорости света! Можно ли запутанность использовать для мгновенного общения?

Предположим, что каждая пара запутанных электронов находится в запутанном состоянии спина, которое мы только что рассмотрели:

$$\frac{1}{2}|a_0\rangle|b_0\rangle+\frac{1}{2}|a_0\rangle|b_1\rangle+\frac{1}{\sqrt{2}}|a_1\rangle|b_0\rangle+0|a_1\rangle|b_1\rangle.$$

Предположим также, что Алиса измеряет спин своих электронов первой, раньше, чем Боб измерит спин парных электронов. Мы уже видели, что Алиса получит случайную строку из 0 и 1, в которой цифры встречаются с равной вероятностью.

Теперь предположим, что Боб измерил спины раньше Алисы. Что в этом случае получит Алиса? К моменту, когда Алиса выполнит свои измерения, измерения будут выполнены обоими участниками, поэтому мы можем использовать амплитуды вероятности из начального выражения. Мы знаем, что они получат 00 и 01 с вероятностью 1/4, 10 — с вероятностью 1/2 и 11 — с вероятностью 0. Следовательно, Алиса получит 0 с вероятностью $\frac{1}{4}+\frac{1}{4}=\frac{1}{2}$ и 1 — с вероятностью $\frac{1}{2}+0=\frac{1}{2}$. То есть Алиса получит все ту же случайную строку из 0 и 1, в которой цифры встречаются с равной вероятностью. Но это та же самая ситуация, когда она производила измерения первой. То есть по результатам своих измерений Алиса не может с уверенностью сказать, были ли они сделаны до или после Боба. Все запутанные состояния ведут себя таким образом. Если у Алисы и Боба не будет возможности определить, кто из них первым выполнил измерения, они не смогут передать друг другу никакую информацию.

Мы показали, что Алиса и Боб не могут передавать информацию, когда их кубиты находятся в определенном запутанном состоянии, но приведенные аргументы легко обобщить на любое запутанное состояние. Независимо от состояний своих кубитов, Алиса и Боб не смогут посылать информацию, просто измеряя их.

Теперь, когда мы убедились, что сверхсветовое общение невозможно, перейдем к более прозаической задаче записи тензорных произведений с использованием стандартных базисов. Но позже мы еще вернемся к исследованию запутанных кубитов на примере квантовых часов из предыдущих глав.

Стандартный базис для тензорных произведений

Стандартный базис для $\mathbb{R}^2$ имеет вид $\left(\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix}\right)$. Когда Алиса и Боб оба используют стандартный базис, тензорное произведение приобретает вид

$$r\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}+s\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}+t\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}+u\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}.$$

Соответственно, стандартный упорядоченный базис для $\mathbb{R}^2\otimes\mathbb{R}^2$ имеет вид

$$\left(\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}\right).$$

Так как в его основе лежат четыре вектора — это четырехмерное пространство. Стандартное четырехмерное пространство обозначается как $\mathbb{R}^4$ и имеет упорядоченный базис

$$\left(\begin{bmatrix}1\\0\\0\\0\end{bmatrix},\begin{bmatrix}0\\1\\0\\0\end{bmatrix},\begin{bmatrix}0\\0\\1\\0\end{bmatrix},\begin{bmatrix}0\\0\\0\\1\end{bmatrix}\right).$$

Отождествим базисные векторы в $\mathbb{R}^2\otimes\mathbb{R}^2$ с соответствующими векторами в $\mathbb{R}^4$, сохранив их порядок.

$$\begin{bmatrix}1\\0\\0\\0\end{bmatrix}=\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix},\ \begin{bmatrix}0\\1\\0\\0\end{bmatrix}=\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix},\ \begin{bmatrix}0\\0\\1\\0\end{bmatrix}=\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix},\ \begin{bmatrix}0\\0\\0\\1\end{bmatrix}=\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}.$$

Это легко запомнить, если использовать следующую конструкцию:

$$\begin{bmatrix}a_0\\a_1\end{bmatrix}\otimes\begin{bmatrix}b_0\\b_1\end{bmatrix}=\begin{bmatrix}a_0\begin{bmatrix}b_0\\b_1\end{bmatrix}\\a_1\begin{bmatrix}b_0\\b_1\end{bmatrix}\end{bmatrix}=\begin{bmatrix}a_0b_0\\a_0b_1\\a_1b_0\\a_1b_1\end{bmatrix}.$$

Обратите внимание, что индексы следуют стандартному порядку двоичных чисел: 00, 01, 10, 11.

Как запутать кубиты?

Эта книга описывает математический аппарат, лежащий в основе квантовых вычислений, а не процесс создания квантового компьютера. Мы не собираемся тратить много времени на подробные описания физических экспериментов, но вопрос, как физики создают запутанные частицы, настолько важен, что все же кратко рассмотрим его. Запутанные кубиты можно представить запутанными фотонами или электронами. Хотя мы часто употребляем словосочетание «запутанные частицы», на самом деле это означает лишь то, что запутан вектор, описывающий их состояния, тензор в $\mathbb{R}^2 \otimes \mathbb{R}^2$. Сами частицы существуют совершенно отдельно друг от друга и, как мы только что отметили, могут находиться очень далеко друг от друга. Тем не менее остается нерешенным вопрос: как создать пару частиц, вектор состояния которых запутан? Сначала посмотрим, как получаются запутанные частицы в физических экспериментах. Затем посмотрим, как создать запутанные кубиты с помощью квантовых вентилей.

В настоящее время наиболее распространен метод на основе фотонов. Процесс называется *спонтанным параметрическим рассеянием*. Фотоны, составляющие луч лазера, посылаются через специальный кристалл. Большинство фотонов просто проходят сквозь него, но некоторые делятся на пары. Энергия и импульс должны сохраняться — полная энергия и импульс двух получившихся фотонов должны быть равны энергии и импульсу начального фотона. Законы сохранения гарантируют запутанность состояния, описывающего поляризацию двух фотонов.

Во Вселенной электроны часто запутаны. В начале книги был описан эксперимент Штерна и Герлаха с атомами серебра. Напомню, что спины электронов на внутренних орбитах взаимно компенсируются, поэтому остается единственный электрон на внешней орбите, который передает свой спин атому. На самой внутренней орбите находятся два электрона. Они запутаны, так как их спины взаимно компенсируются. Вот как можно представить вектор состояния, описывающий спин этих электронов

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}-\frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}.$$

Запутанные электроны также встречаются в сверхпроводниках, и эти электроны использовались в экспериментах. Однако часто бывает желательно иметь запутанные частицы, находящиеся далеко друг от друга, как мы увидим далее, когда будем говорить о проверке неравенства Белла.

Главная проблема, связанная с разделением запутанных электронов, которые изначально находятся вблизи друг от друга, состоит в том, что они имеют свойство взаимодействовать с окружением. Их очень сложно разделить, исключив любые взаимодействия. С другой стороны, разделить запутанные фотоны намного проще, но их сложно измерить. Однако есть возможность взять лучшее из обоих миров. Именно так и поступила международная команда ученых из технического университета в Делфте. Они назвали свой метод проверкой неравенства Белла. Они использовали два алмаза, разнесенные на расстояние 1,3 километра друг от друга. Каждый алмаз имел небольшие недостатки — атомы азота кое-где изменяли структуру решетки из атомов углерода. Электроны оказывались в ловушке дефектов. Лазер возбуждал электрон в каждом из алмазов так, что оба электрона испускали фотоны. Излучаемые фотоны были запутаны со спинами электронов, испустивших их. Затем фотоны направлялись по оптоволоконному кабелю навстречу друг другу и встречались в светоделителе — стандартном устройстве, которое обычно используется для деления пучка фотонов на две части, но в данном методе он использовался для запутывания двух фотонов. Затем фотоны измерялись. В результате два электрона оказывались запутанными друг с другом.[1] (В следующей главе я объясню, почему команда поставила этот эксперимент.)

В квантовых вычислениях мы обычно будем вводить незапутанные кубиты, а затем запутывать их, используя вентиль *CNOT*. Позже я подробно объясню, что такое вентили, но по сути вычисления заключаются в простом умножении матриц. Давайте кратко рассмотрим их.

---

[1] Есть короткий видеоролик, рассказывающий об этом: https://www.youtube.com/watch?v=AE8MaQJkRcg/.

Запутывание кубитов с помощью вентиля CNOT

Формальное определение квантового вентиля мы рассмотрим позже, а пока просто отметим, что каждый вентиль соответствует ортонормированному базису или, что эквивалентно, ортогональной матрице.

Стандартный базис четырехмерного пространства $\mathbb{R}^4$ имеет вид

$$\left(\begin{bmatrix}1\\0\\0\\0\end{bmatrix},\begin{bmatrix}0\\1\\0\\0\end{bmatrix},\begin{bmatrix}0\\0\\1\\0\end{bmatrix},\begin{bmatrix}0\\0\\0\\1\end{bmatrix}\right).$$

Вентиль *CNOT* меняет местами два последних элемента. Это дает нам матрицу для вентиля *CNOT*.

$$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}.$$

Этот вентиль воздействует на пары кубитов. Чтобы использовать матрицу, кубиты должны быть записаны с использованием четырехмерных векторов. Рассмотрим пример.

Сначала возьмем незапутанное тензорное произведение

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\1\\0\end{bmatrix}.$$

При передаче кубитов через вентиль они меняются. Кубиты результата получаются умножением на матрицу:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

Этот последний вектор соответствует паре запутанных кубитов — произведение внутренних амплитуд равно 0 и не равно произведению внешних амплитуд. Это выражение можно переписать иначе:

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Мы часто будем использовать запутанные кубиты в этом состоянии. Оно обладает замечательным свойством: если Алиса и Боб производят измерения в стандартном базисе, они оба получат $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$, соответствующий 0, или оба получат $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$, соответствующий 1. Оба случая одинаково вероятны.[1]

Продолжим рассмотрение с использованием аналогии квантовых часов.

Запутанные квантовые часы

Вспомним наши квантовые часы. Мы только можем спросить у часов, указывает ли стрелка в определенном направлении, а часы могут ответить либо «да, указывает», либо «нет, она указывает в противоположном направлении».

Пусть вектор $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ соответствует направлению на число двенадцать, а вектор $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ — направлению на число шесть. Рассмотрим пару часов в запутанном состоянии:

[1] В следующей главе мы увидим, что Алисе и Бобу не требуется придерживаться стандартного базиса. Если оба используют один и тот же ортонормированный базис, неважно какой именно, они оба получат один и тот же результат.

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}+\frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}.$$

На самом деле рассмотрим сто пар часов, каждая из которых находится в таком состоянии. Допустим, что сто часов находятся у вас и парные им часы находятся у меня. Мы с вами оба снова и снова будем задавать один и тот же вопрос: указывает ли стрелка на число двенадцать?

В первом сценарии мы с вами не будем связываться друг с другом, а просто начнем перебирать часы одни за другими и задавать вопрос. Каждый раз часы будут отвечать «да» или «нет». Ответы «да» мы будем записывать как 1 и ответы «нет» как 0. Завершив опрос, каждый из нас получит строку из 0 и 1. Я буду анализировать свою строку, а вы — свою. Обе строки являются случайными последовательностями 0 и 1. Обе цифры встречаются примерно одинаковое число раз. Теперь мы свяжемся друг с другом и сравним наши строки. И ваша, и моя строки — идентичны. Во всех ста случаях строки совпадают.

Во втором сценарии у каждого из нас снова будет по сто часов. Но на этот раз мы договоримся, что вы первым будете выполнять измерения. Вы задаете свой вопрос в час дня, а спустя полчаса я задаю тот же вопрос. В течение этого получаса вы звоните мне и говорите, каким будет ответ моих часов. В конце эксперимента у нас у обоих имеются строки из 0 и 1. Обе строки совпадают во всех символах. Каждый раз, когда вы мне звонили и сообщали результат моих измерений, вы оказывались правы. Можно ли отсюда сделать вывод, что ваши измерения повлияли на мои?

Теперь предположим, что я сознался в небольшом мошенничестве — я не следовал правилам. На самом деле я задал вопрос своим часам за полчаса до вас и узнал ваши ответы раньше, чем вы. Ваши звонки только подтвердили это.

По полученным данным невозможно узнать, следовал ли я правилам или сжульничал. Вы не сможете определить, когда я задавал свой вопрос — до вас или после.

Здесь нет причинно-следственной связи, только корреляция. Как мы видели выше, запутанные часы нельзя использовать для обмена сообще-

ниями между нами. Но сам процесс от этого не выглядит менее мистическим. Альберт Эйнштейн описал запутывание как «сверхъестественное действие на расстоянии». В наши дни многие говорят, что нет никакого действия, только корреляция. Конечно, можно поспорить об определении «действия», но даже если мы согласимся, что нет никакого действия, все равно остается ощущение, что происходит что-то сверхъестественное.

Допустим, что у нас с вами есть пара запутанных квантовых часов и мы разговариваем по телефону. Никто из нас еще не задавал вопросов своим часам, поэтому они все еще находятся в запутанном состоянии. Если в этом состоянии вы зададите своим часам вопрос, указывает ли стрелка на число двенадцать, у вас будут одинаковые шансы получить ответ «да» или «нет». Но как только я задам вопрос своим часам, ваши шансы получить тот или иной ответ будут неравны. Вы получите точно такой же ответ, как и я.

Эта корреляция не выглядела бы сверхъестественной, если бы она имела место, пока часы оставались запутанными, но в тот момент нам было неизвестно, указывали ли стрелки наших часов на число двенадцать. Нам пришлось подождать, пока кто-то из нас задаст вопрос, и как только один из нас узнал ответ, другой будет точно знать, какой ответ он получит.

Но наша модель описывает совсем не это. Наша модель говорит, что выбор ответа на вопрос, в каком направлении указывает стрелка, неизвестен заранее. Выбор происходит, только когда кто-то из нас первым задает свой вопрос. Именно это обстоятельство делает явление сверхъестественным.

В следующей главе мы подробнее рассмотрим это явление. Там мы рассмотрим модель, включающую корреляцию понятным и естественным способом. К сожалению, она ошибочна. Джон Стюарт Белл (John Stewart Bell) придумал гениальный тест, показывающий, что простое объяснение ошибочно и загадочная сверхъестественность никуда не исчезает.

5 Неравенство Белла

Мы познакомились с малой частью математической модели квантовой механики, касающейся спина частиц или поляризации фотонов, и получили математический аппарат, описывающий кубиты. Это стандартная модель, которую часто называют *копенгагенской интерпретацией*, по названию города, где жил и работал Нильс Бор.

Некоторым величайшим физикам начала XX века, включая Альберта Эйнштейна и Эрвина Шредингера, не понравилась эта модель с ее интерпретацией состояний, переходящих в базисные состояния с определенными вероятностями. Они возражали против использования вероятности и идеи действия на расстоянии. Они считали, что должна существовать более удачная модель, использующая «скрытые переменные» и «локальный реализм». Они не возражали против использования копенгагенской модели в вычислениях, но считали необходимым разработку более глубокой теории, объясняющей, почему вычисления дают правильные ответы, — теории, исключающей случайность и объясняющей мистицизм.

Бор и Эйнштейн оба были заинтересованы в развитии философии квантовой механики и провели ряд дискуссий об истинном значении теории. В этой главе мы рассмотрим их точки зрения. У вас может возникнуть вопрос: не отвлекаемся ли мы и действительно ли нужны философские рассуждения для понимания квантовых вычислений? Мы уже знаем, что точка зрения Эйнштейна и Шредингера была ошибочной и копенгагенская модель считается стандартным описанием. Но Эйнштейн и Шре-

дингер были блестящими учеными, и есть множество причин, чтобы познакомиться с их аргументами.

Споры между Бором и Эйнштейном в основном касались локального реализма. Мы подробнее рассмотрим это понятие чуть ниже, а пока отмечу, что локальный реализм фактически означает, что на частицу могут влиять только изменения в ее окрестностях. Практически все мы считаем себя субъектами локального реализма, но квантовая механика показывает, что эта точка зрения неверна. Модель Эйнштейна кажется нам естественной и правильной — по крайней мере мне. Когда я впервые услышал о квантовой запутанности, моим первым устремлением было принятие модели, подобной модели Эйнштейна. Вы тоже можете неправильно воспринимать запутанность. Эти аргументы важны для философии физики и помогут нам понять, почему невозможно исключить мистицизм.

Джон Стюарт Белл был ирландским физиком. Он разработал гениальный тест, способный различить две модели. Многие были удивлены, что модели оказались не только философией, но и теорией, которую можно проверить. Мы изучили только малую часть математического аппарата квантовой механики, но она включает все, что нужно, чтобы понять результаты, полученные Беллом. Его тест был выполнен несколько раз. Сложно устранить все возможные погрешности в подготовке к этому эксперименту, но в течение многих лет исследователи устраняли все больше и больше возможных лазеек. Результаты тестирования всегда соответствовали копенгагенской интерпретации. Поскольку результат, полученный Беллом, является одним из важнейших достижений XX века и мы владеем необходимым математическим аппаратом, есть смысл поближе познакомиться с ним.

Многим из вас наверняка интересно, какое отношение это имеет к квантовым вычислениям. В конце этой главы мы увидим, что идеи, на которых основывается проверка неравенства Белла, можно использовать для шифрования сообщений. Мы снова встретимся с запутанными кубитами, которые использовал Белл, когда начнем рассматривать квантовые алгоритмы. Поэтому данная глава имеет самое непосредственное отношение к квантовым вычислениям. Кроме того, я считаю эти сведения увлекательными и надеюсь, что вас они тоже заинтересуют, поэтому и написал эту главу.

Начнем с обзора запутанных кубитов, представленных в предыдущей главе, и посмотрим, что получится, если измерить их с использованием

разных базисов. Начнем анализ со стандартной копенгагенской модели, которую мы видели в предыдущих главах.

Запутанные кубиты в разных базисах

В предыдущей главе мы рассматривали двое запутанных квантовых часов в состоянии

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}+\frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}.$$

Там мы заметили, что если Алиса и Боб задавали своим часам вопрос, указывает ли стрелка на число двенадцать, они оба получали один и тот же ответ: «да, стрелка указывает на двенадцать» или «нет, стрелка указывает на шесть». Оба ответа были равновероятны, но Алиса и Боб всегда получали один и тот же ответ. Теперь посмотрим, что получится, если Алиса и Боб изменят направление измерения. Например, что получится, если они оба спросят, указывает ли стрелка на число четыре? Мы знаем, что ответ либо «да, стрелка указывает на четыре», либо «нет, стрелка указывает на десять», но получат ли Алиса с Бобом один и тот же ответ? Равновероятны ли эти два ответа?

Сначала приведем логичные рассуждения для двух кубитов в запутанном состоянии

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}+\frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}.$$

Это состояние может быть представлено двумя электронами. Допустим, что Алиса и Боб измеряют спин своих электронов в направлении 0°. Если Алиса получит *N*, тогда Боб получит *S*. Если Алиса получит *S*, тогда Боб получит *N*. Как упоминалось ранее, это состояние может быть представлено двумя электронами в атоме, которые взаимно компенсируют друг друга. Но мы предполагаем, что спины будут компенсироваться во всех направлениях, поэтому ожидается, что если Алиса и Боб выберут другой базис для измерений, они все равно получат противоположно ориентированные спины. Симметрия также предполагает, что оба направления должны быть равновероятными.

Это логичное рассуждение приводит нас к предположению, что если взять два кубита в запутанном состоянии

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}+\frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}$$

и переписать их состояния с использованием другого ортонормированного базиса $\left(|b_0\rangle,|b_1\rangle\right)$, мы должны получить $\frac{1}{\sqrt{2}}|b_0\rangle\otimes|b_0\rangle+\frac{1}{\sqrt{2}}|b_1\rangle\otimes|b_1\rangle$. Наше рассуждение логично, но логичные рассуждения о чем-то столь же нелогичном, как квантовая механика, выглядят неубедительно. Но в данном случае мы правы и можем доказать нашу правоту.

Доказать, что $\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}+\frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}$ **равно** $\frac{1}{\sqrt{2}}|b_0\rangle\otimes|b_0\rangle+\frac{1}{\sqrt{2}}|b_1\rangle\otimes|b_1\rangle$.

Для начала запишем кеты $|b_0\rangle$ и $|b_1\rangle$ как векторы-столбцы. Пусть $|b_0\rangle=\begin{bmatrix}a\\b\end{bmatrix}$ и $|b_1\rangle=\begin{bmatrix}c\\d\end{bmatrix}$. Теперь выразим наши стандартные базисные векторы в виде линейных комбинаций новых базисных векторов. Используем для этого стандартный прием (второй в списке в конце главы 2). Начнем с $\begin{bmatrix}1\\0\end{bmatrix}$. Уравнение

$$\begin{bmatrix}a & b\\ c & d\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix}=\begin{bmatrix}a\\c\end{bmatrix}$$

дает нам

$$\begin{bmatrix}1\\0\end{bmatrix}=a\begin{bmatrix}a\\b\end{bmatrix}+\begin{bmatrix}c\\d\end{bmatrix}.$$

Следовательно,

$$\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}=\left(a\begin{bmatrix}a\\b\end{bmatrix}+c\begin{bmatrix}c\\d\end{bmatrix}\right)\otimes\begin{bmatrix}1\\0\end{bmatrix}.$$

Раскрыв скобки, получаем выражение

$$a\begin{bmatrix}a\\b\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}+c\begin{bmatrix}c\\d\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix},$$

которое можно переписать как

$$\begin{bmatrix}a\\b\end{bmatrix}\otimes\begin{bmatrix}a\\0\end{bmatrix}+\begin{bmatrix}c\\d\end{bmatrix}\otimes\begin{bmatrix}c\\0\end{bmatrix}.$$

То есть $\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}=\begin{bmatrix}a\\b\end{bmatrix}\otimes\begin{bmatrix}a\\0\end{bmatrix}+\begin{bmatrix}c\\d\end{bmatrix}\otimes\begin{bmatrix}c\\0\end{bmatrix}$.

Выполним аналогичные вычисления со вторым членом:

$$\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}=\begin{bmatrix}a\\b\end{bmatrix}\otimes\begin{bmatrix}0\\b\end{bmatrix}+\begin{bmatrix}c\\d\end{bmatrix}\otimes\begin{bmatrix}0\\d\end{bmatrix}.$$

Сложив эти два результата, получаем

$$\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}+\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}=\begin{bmatrix}a\\b\end{bmatrix}\otimes\left(\begin{bmatrix}a\\0\end{bmatrix}+\begin{bmatrix}0\\b\end{bmatrix}\right)+\begin{bmatrix}c\\d\end{bmatrix}\otimes\left(\begin{bmatrix}c\\0\end{bmatrix}+\begin{bmatrix}0\\d\end{bmatrix}\right).$$

Это выражение можно упростить до

$$\begin{bmatrix}a\\b\end{bmatrix}\otimes\begin{bmatrix}a\\b\end{bmatrix}+\begin{bmatrix}c\\d\end{bmatrix}\otimes\begin{bmatrix}c\\d\end{bmatrix},$$

то есть просто

$$|b_0\rangle\otimes|b_0\rangle+|b_1\rangle\otimes|b_1\rangle.$$

Итак, мы доказали, что

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}+\frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}$$

равно $\frac{1}{\sqrt{2}}|b_0\rangle \otimes |b_0\rangle + \frac{1}{\sqrt{2}}|b_1\rangle \otimes |b_1\rangle$.

То есть если Алиса и Боб владеют запутанными кубитами в состоянии

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} + \frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix}$$

и оба выберут для измерения своих кубитов ортонормированный базис $\left(|b_0\rangle, |b_1\rangle\right)$, запутанное состояние можно переписать как

$$\frac{1}{\sqrt{2}}|b_0\rangle|b_0\rangle + \frac{1}{\sqrt{2}}|b_1\rangle|b_1\rangle.$$

После первого измерения состояние изменится на $|b_0\rangle|b_0\rangle$ или на $|b_1\rangle|b_1\rangle$, причем оба этих, теперь уже незапутанных, состояния будут равновероятны. Как следствие, когда Алиса и Боб измерят свои кубиты, они оба получат один и тот же результат, 0 или 1, и оба исхода равновероятны.

Чтобы получить тот же результат, который получил Белл, мы должны измерить связанные кубиты с использованием трех разных базисов. Эти базисы соответствуют повороту измерительной установки на 0°, 120° и 240°. Если провести аналогию с запутанными квантовыми часами — мы зададим три вопроса, указывает ли стрелка на двенадцать, на четыре и на восемь. Если обозначить эти базисы как $\left(|\uparrow\rangle, |\downarrow\rangle\right)$, $\left(|\searrow\rangle, |\nwarrow\rangle\right)$ и $\left(|\swarrow\rangle, |\nearrow\rangle\right)$, эти три запутанных состояния можно записать так:

$$\frac{1}{\sqrt{2}}|\uparrow\rangle|\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\rangle|\downarrow\rangle \quad \frac{1}{\sqrt{2}}|\searrow\rangle|\searrow\rangle + \frac{1}{\sqrt{2}}|\nwarrow\rangle|\nwarrow\rangle \quad \frac{1}{\sqrt{2}}|\swarrow\rangle|\swarrow\rangle + \frac{1}{\sqrt{2}}|\nearrow\rangle|\nearrow\rangle.$$

Теперь обратимся к Эйнштейну и посмотрим, как он видел эти запутанные состояния.

Эйнштейн и локальный реализм

Хорошим примером для объяснения локального реализма может служить гравитация. Закон тяготения Ньютона дает формулу силы притяжения между двумя массами. Если подставить в нее размеры масс, расстояние

между ними и гравитационную постоянную, можно получить величину силы притяжения. Закон Ньютона изменил физику. С его помощью, например, можно доказать, что планета вращается вокруг звезды по эллиптической орбите. Однако несмотря на то, что закон описывает величину силы, он ничего не говорит нам о природе этой силы.

Закон тяготения Ньютона можно использовать для расчетов, но он не объясняет, как работает гравитация. Сам Ньютон тоже был этим обеспокоен. Все думали, что должна быть какая-то более глубокая теория, объясняющая действие гравитации. Делалось множество разных предположений, часто с привлечением «эфира», который должен быть неотъемлемой частью Вселенной. И хотя не было единого мнения о механизме работы гравитации, никто не считал гравитацию сверхъестественным действием на расстоянии, и все верили, что можно найти какое-то естественное объяснение. Была вера в то, что сейчас мы называем локальным реализмом.

На смену закону тяготения Ньютона пришла теория гравитации Эйнштейна. Она не только усовершенствовала теорию Ньютона с точки зрения точности предсказания астрономических наблюдений, которые нельзя вывести с помощью теории Ньютона, но также объяснила, как работает гравитация. Она описала искажение пространства-времени. Согласно ей, планета движется в соответствии с формой пространства-времени, в котором она находится. Никаких сверхъестественных действий на расстоянии. Теория Эйнштейна была не только более точной, но также описала, как работает гравитация, и это описание было локальным. Планета движется в соответствии с формой пространства в ее окрестностях.

Копенгагенская интерпретация в квантовой механике повторно ввела идею о сверхъестественном действии на расстоянии. При измерении пары запутанных кубитов их состояние изменяется немедленно, даже если они физически удалены друг от друга. Рассуждения Эйнштейна кажутся вполне естественными. Он только что исключил сверхъестественное действие из теории гравитации и теперь снова столкнулся с ним. В отличие от него, Бор не верил в существование более глубокой теории, способной объяснить механизм этого действия. Эйнштейн был не согласен с ним.

Эйнштейн верил, что сможет доказать ошибочность позиции Бора. В соавторстве с Борисом Подольским (Boris Podolsky) и Натаном Розеном

(Nathan Rosen) он написал статью, в которой указывал, что его специальная теория относительности подразумевает невозможность распространения информации быстрее скорости света, но мгновенные действия на расстоянии означают, что информация от Алисы к Бобу может доставляться мгновенно. Эта проблема получила название *ЭПР-парадокс*, то есть парадокс Эйнштейна—Подольского—Розена.

В наше время ЭПР-парадокс обычно описывается с позиции спина, и именно так мы и сделаем, хотя Эйнштейн с соавторами описывал проблему иначе. Они рассматривали местоположение и импульс двух запутанных частиц. А формулировку с позиции спина предложил Дэвид Бом (David Bohm). Именно формулировка Бома используется в настоящее время, и именно ее использовал Джон Сюарт Белл для вычисления своего важного неравенства. Несмотря на то что Бом сыграл важную роль в описании и формулировании парадокса, его имя обычно опускается.

В предыдущей главе указывалось, что копенгагенская интерпретация не допускает возможности передачи информации быстрее скорости света, и поэтому, хотя ЭПР-парадокс на самом деле не является парадоксом, все еще стоит вопрос о наличии объяснения, устраняющего сверхъестественность действия.

Эйнштейн и скрытые переменные

С классической точки зрения физика является детерминированной — если начальные условия известны с бесконечной точностью, можно предсказать точный результат. Конечно, начальные условия могут быть известны только с некоторой конечной точностью, в том смысле, что измерения всегда имеют некоторую погрешность — небольшую разность между измеренным и истинным значением. С течением времени эта ошибка может увеличиваться до значения, которое уже не позволит получить адекватный прогноз. Эта идея лежит в основе так называемой чувствительной зависимости от начальных условий. Она объясняет, почему прогноз погоды дальше чем на неделю крайне ненадежен. Однако важно помнить, что основополагающая теория детерминирована. Погода выглядит непредсказуемой, но это не связано с какой-то присущей ей случайностью, просто мы не можем выполнить измерения с достаточно высокой точностью.

Другая область, где вероятность вторгается в классическую физику, — законы, касающиеся газов, то есть законы термодинамики, но сама теория снова является детерминированной. Если точно знать скорость и массу каждой молекулы в газе, теоретически можно точно предсказать, что произойдет с каждой молекулой в будущем. На практике же молекул оказывается слишком много, чтобы можно было учесть каждую из них, поэтому мы берем средние значения и рассматриваем газ со статистической точки зрения.

Именно на этот классический детерминистский взгляд ссылался Эйнштейн, когда очень здорово высказался, что Бог не играет в кости со Вселенной. Он чувствовал, что использование вероятности в квантовой механике демонстрирует неполноту теории. Должна существовать более глубокая теория, возможно, включающая новые переменные, которая является детерминированной, но выглядит вероятностной, если не принимать во внимание все эти пока неизвестные переменные. Эти неизвестные переменные стали называть скрытыми переменными.

Классическое объяснение запутанности

Начнем с наших квантовых часов, находящихся в состоянии

$$\frac{1}{\sqrt{2}}|\uparrow\rangle|\uparrow\rangle+\frac{1}{\sqrt{2}}|\downarrow\rangle|\downarrow\rangle.$$

Алиса и Боб задают вопрос: указывает ли стрелка на двенадцать? Квантовая модель утверждает, что они оба получат один и тот же ответ: «да, стрелка указывает на двенадцать» или «нет, стрелка указывает на шесть». Оба ответа равновероятны. На самом деле мы можем провести эксперименты со спинами запутанных электронов. Результаты этих экспериментов будут в точности соответствовать тому, что предсказывает квантовая модель. Но как эти результаты объясняет классическая модель?

Классическая интерпретация описанной ситуации выглядит довольно просто. Электроны имеют определенный спин в любом направлении. Запутанные электроны запутываются в результате некоторого локального воздействия. И снова мы обращаемся к скрытым переменным и более глубокой теории. Мы не знаем точно, что происходит, но есть некоторый

локальный процесс, который переводит электроны в одно и то же состояние спина. Когда они запутаны, направление спина выбирается сразу для обоих электронов.

Это можно сравнить с ситуацией, когда у нас есть колода карт, которую мы сначала перемешиваем, затем не глядя извлекаем одну карту, разрезаем ее на две половины и вкладываем в два конверта, все это время не зная, какая карта была извлечена из колоды. Затем мы посылаем конверты Бобу и Алисе, живущим в противоположных концах Вселенной. Ни Алиса, ни Боб не подозревают, какую карту они получили. Это может быть любая карта из пятидесяти двух, но как только Алиса вскроет свой конверт и увидит бубнового валета, она будет точно знать, что Боб тоже получил половинку карты бубнового валета. Нет никакого действия на расстоянии и ничего сверхъестественного.

Чтобы прийти к результатам, полученным Беллом, мы должны измерить наши запутанные кубиты в трех разных направлениях. Теперь вернемся к аналогии запутанных часов и будем задавать три вопроса: указывает ли стрелка на двенадцать, на четыре и на восемь. Теоретическая квантовая модель утверждает, что на каждый вопрос будет получен ответ либо «да, указывает», либо «нет, она указывает в противоположном направлении». Оба ответа на каждый вопрос равновероятны. Но когда Алиса и Боб зададут один и тот же вопрос, они получат один и тот же ответ. Описать это с классической точки зрения можно точно так же, как и раньше.

Существует некоторый локальный процесс, который запутывает часы. Мы не пытаемся описать, как именно это делается, а просто ссылаемся на скрытые переменные — есть какая-то более глубокая теория, которая объясняет все это. Но когда часы запутаны, на три вопроса выбираются вполне определенные ответы. Это можно сравнить с ситуацией, когда имеется три колоды карт с рубашками разного цвета. Мы извлекаем по одной карте из колоды с синей, красной и зеленой рубашкой. Разрезаем каждую пополам и посылаем три половинки Алисе и три половинки Бобу. Если Алиса увидит половинку карты бубнового валета с зеленой рубашкой, она будет точно знать, что Боб получит половинку карты с зеленой рубашкой, которая является бубновым валетом.

В отношении наших квантовых часов классическая теория гласит, что на каждый вопрос имеется определенный ответ, который предопределен еще

до того, как будет задан вопрос. Квантовая теория, напротив, гласит, что ответ на вопрос не определен, пока он не задан.

Неравенство Белла

Представьте, что мы сгенерировали поток пар кубитов и послали их Алисе и Бобу. Каждая пара кубитов находится в запутанном состоянии

$$\frac{1}{\sqrt{2}}|\uparrow\rangle|\uparrow\rangle+\frac{1}{\sqrt{2}}|\downarrow\rangle|\downarrow\rangle.$$

Алиса случайным образом выбирает направление 0°, 120° или 240° для измерения своего кубита. Каждое из этих направлений выбирается случайно, с вероятностью 1/3. Алиса не запоминает выбираемые направления, но записывает получаемый результат, 0 или 1. (Напомню, что 0 соответствует первому базисному вектору, а 1 — второму.) После того как Алиса измерит свой кубит, Боб случайно, с вероятностью 1/3, выбирает одно из тех же трех направлений и измеряет свой кубит. Так же как Алиса, он не запоминает направление измерения, но записывает полученный результат, 0 или 1.

В итоге Алиса и Боб получают по длинной строке из 0 и 1. Затем они сравнивают свои строки, символ за символом. Если первые символы совпадают, они записывают букву *A*, если не совпадают — букву *D*. Затем переходят ко второму символу и также записывают *A* или *D*, в зависимости от совпадения или несовпадения. Так они сравнивают все символы в своих строках.

В результате получается новая строка, состоящая из букв *A* и *D*. Какая доля строки придется на символ *A*? Белл заметил, что модель квантовой механики и классическая модель дают разные ответы.

Ответ модели квантовой механики

Кубиты находятся в запутанном состоянии

$$\frac{1}{\sqrt{2}}|\uparrow\rangle|\uparrow\rangle+\frac{1}{\sqrt{2}}|\downarrow\rangle|\downarrow\rangle.$$

Мы уже видели, что если Алиса и Боб оба выберут одно и то же направление для измерения, они получат один и тот же ответ. Теперь посмотрим, что случится, если они выберут разные базисы.

Начнем со случая, когда Алиса выбирает $\left(|\searrow\rangle,|\nwarrow\rangle\right)$, а Боб выбирает $\left(|\swarrow\rangle,|\nearrow\rangle\right)$. Запутанное состояние

$$\frac{1}{\sqrt{2}}|\uparrow\rangle|\uparrow\rangle+\frac{1}{\sqrt{2}}|\downarrow\rangle|\downarrow\rangle$$

можно записать, используя базис Алисы, как

$$\frac{1}{\sqrt{2}}|\searrow\rangle|\searrow\rangle+\frac{1}{\sqrt{2}}|\nwarrow\rangle|\nwarrow\rangle.$$

Когда Алиса выполняет свое измерение, происходит переход в состояние $|\searrow\rangle|\searrow\rangle$ или $|\nwarrow\rangle|\nwarrow\rangle$, каждое из которых равновероятно. Если произошел переход в состояние $|\searrow\rangle|\searrow\rangle$, она запишет 0. Если произошел переход в состояние $|\nwarrow\rangle|\nwarrow\rangle$, она запишет 1.

Теперь измерение должен выполнить Боб. Допустим, что после измерения Алисой кубиты находятся в состоянии $|\searrow\rangle|\searrow\rangle$, то есть кубит Боба находится в состоянии $|\searrow\rangle$. Чтобы вычислить результат измерения Бобом, нужно переписать это состояние, использовав базис Боба. (Похожие вычисления мы уже делали в разделе «Алиса, Боб и Ева» главы 3.)

Записав решение с использованием двумерных кетов, получаем:

$$|\searrow\rangle=\begin{bmatrix}1/2\\-\sqrt{3}/2\end{bmatrix}\qquad|\swarrow\rangle=\begin{bmatrix}-1/2\\-\sqrt{3}/2\end{bmatrix}\qquad|\nearrow\rangle=\begin{bmatrix}\frac{\sqrt{3}}{2}\\-1/2\end{bmatrix}.$$

Умножим $|\searrow\rangle$ на матрицу со строками, соответствующими бра из базиса Боба.

$$\begin{bmatrix}-1/2 & -\sqrt{3}/2\\ \frac{\sqrt{3}}{2} & -1/2\end{bmatrix}\begin{bmatrix}1/2\\-\sqrt{3}/2\end{bmatrix}=\begin{bmatrix}1/2\\\sqrt{3}/2\end{bmatrix}.$$

В результате получаем $|\searrow\rangle = \frac{1}{2}|\swarrow\rangle + \frac{\sqrt{3}}{2}|\nearrow\rangle$. Выполнив измерение, Боб получит 0 с вероятностью 1/4 и 1 с вероятностью 3/4. То есть когда Алиса получит 0, Боб получит 0 с вероятностью 1/4. Легко проверить другой случай. Если Алиса получит 1, Боб также получит 1 с вероятностью 1/4.

Другие случаи дают аналогичные результаты: если Боб и Алиса производят измерения в разных направлениях, их результаты совпадут в 1/4 случаев и не совпадут в 3/4 случаев.

В итоге в 1/3 случаев они выполняют измерения в одном направлении и всегда получают совпадения; в 2/3 случаев они выполняют измерения в разных направлениях и получают совпадения в 1/4 случаев. Соответственно, доля символов *A* в строке из *A* и *D* составляет

$$\frac{1}{3}\times 1 + \frac{2}{3}\times\frac{1}{4} = \frac{1}{2}.$$

Таким образом, согласно модели квантовой механики, при достаточно большом числе испытаний доля символов *A* должна составлять половину.

Теперь рассмотрим классическую модель.

Ответ классической модели

Классическая модель утверждает, что результаты измерений во всех направлениях предопределены. Всего имеется три направления измерений. Измерение в каждом направлении может дать 0 или 1. То есть всего возможно восемь конфигураций: 000, 001, 010, 011, 100, 101, 110 и 111, где левая цифра определяет ответ при измерении в базисе $\left(|\uparrow\rangle, |\downarrow\rangle\right)$, средняя цифра — при измерении в базисе $\left(|\searrow\rangle, |\nwarrow\rangle\right)$ и правая цифра — в базисе $\left(|\swarrow\rangle, |\nearrow\rangle\right)$.

Запутанность просто означает, что конфигурации кубитов Алисы и Боба идентичны — если кубит Алисы имеет конфигурацию 001, такую же конфигурацию должен иметь кубит Боба. Теперь выясним, что получается, когда Алиса и Боб выбирают направление. Например, если их электроны имеют конфигурацию 001 и Алиса выполняет измерение в базисе $\left(|\uparrow\rangle, |\downarrow\rangle\right)$,

а Боб выполняет измерения в базисе $\left(|\swarrow\rangle,|\nearrow\rangle\right)$, Алиса получит в результате 0, а Боб получит 1, и их результаты не совпадут.

В таблице ниже перечислены все возможные варианты. В левом столбце перечисляются все конфигурации, а в верхней строке перечисляются возможные сочетания базисов, в которых производились измерения Алисой и Бобом. Для представления базисов используются буквы. Базис $\left(|\uparrow\rangle,|\downarrow\rangle\right)$ обозначается буквой *a*, базис $\left(|\searrow\rangle,|\nwarrow\rangle\right)$ — буквой *b* и базис $\left(|\swarrow\rangle,|\nearrow\rangle\right)$ — буквой *c*. Первым в каждой паре следует базис Алисы, а затем Боба. Например, (*b*, *c*) означает, что Алиса выбрала базис $\left(|\searrow\rangle,|\nwarrow\rangle\right)$, а Боб выбрал базис $\left(|\swarrow\rangle,|\nearrow\rangle\right)$. Буквы в остальных ячейках обозначают совпадение (*A* — agree, совпадение) или несовпадение (*D* — disagree, несовпадение).

Конфигурация	**Направления измерений**								
	(*a*, *a*)	(*a*, *u*)	(*a*, *c*)	(*b*, *a*)	(*b*, *b*)	(*b*, *c*)	(*c*, *a*)	(*c*, *b*)	(*c*, *c*)
000	*A*	*A*	*A*	*A*	*A*	*A*	*A*	*A*	*A*
001	*A*	*A*	*D*	*A*	*A*	*D*	*D*	*D*	*A*
010	*A*	*D*	*A*	*D*	*A*	*D*	*A*	*D*	*A*
011	*A*	*D*	*D*	*D*	*A*	*A*	*D*	*A*	*A*
100	*A*	*D*	*D*	*D*	*A*	*A*	*D*	*A*	*A*
101	*A*	*D*	*A*	*D*	*A*	*D*	*A*	*D*	*A*
110	*A*	*A*	*D*	*A*	*A*	*D*	*D*	*D*	*A*
111	*A*	*A*	*A*	*A*	*A*	*A*	*A*	*A*	*A*

Мы не знаем вероятностей разных конфигураций. Всего их восемь, поэтому логично предположить, что каждая из них встречается с вероятностью 1/8, но возможно, что они не все равны. Наш математический анализ не делает никаких предположений о величинах вероятностей выбора направлений. Однако мы можем сами определить их. Алиса и Боб выбирают каждый из трех базисов с равной вероятностью, поэтому каждая из девяти пар выбирается с вероятностью 1/9.

Обратите внимание, что в каждой строке содержится не менее пяти символов *A*, то есть для любой пары кубитов с любой конфигурацией вероятность получить *A* никак не меньше 5/9. Поскольку вероятность получить

A не меньше 5/9 для любой конфигурации спинов, можно сделать вывод, что и общая вероятность будет не меньше 5/9, независимо от доли, принадлежащей каждой конкретной конфигурации.

Теперь мы знаем, к каким результатам пришел Белл. Модель квантовой теории утверждает, что последовательности, полученные Алисой и Бобом, будут совпадать точно в половине случаев. Классическая модель утверждает, что символы в последовательностях Алисы и Боба будут совпадать по меньшей мере в пяти случаях из девяти. Таким образом, мы получаем тест, различающий эти две теории.

Белл опубликовал свою находку в 1964 году. К сожалению, это произошло уже после смерти Эйнштейна и Бора, поэтому ни один из них так и не узнал о существовании экспериментального способа, способного разрешить их спор.

На самом деле провести такой эксперимент очень сложно. Впервые он был выполнен Джоном Клаузером (John Clauser) и Стюартом Фридманом (Stuart Freedman) в 1972 году. Его результаты показали, что прогноз квантовой механики был верен. Однако экспериментаторы должны были сделать некоторые предположения, которые нельзя было проверить, и это оставляло некоторый шанс правильности классической точки зрения. С тех пор эксперимент неоднократно повторялся с увеличением сложности. И всякий раз он подтверждал точку зрения квантовой механики, поэтому теперь почти нет сомнений, что классическая модель ошибочна.

В ранних экспериментах имели место три проблемы. Во-первых, Алиса и Боб были слишком близки друг к другу. Во-вторых, в их измерениях участвовало слишком мало запутанных частиц. В-третьих, выбор направлений Алисой и Бобом не был случайным. Когда экспериментаторы находятся близко друг к другу, теоретически возможно, что на результаты измерений влияет какой-то другой механизм. Например, после первого измерения фотон продолжает перемещаться и может повлиять на второе измерение. Чтобы этого не происходило, измерительные установки должны находиться достаточно далеко друг от друга, чтобы интервал между измерениями был меньше времени, необходимого для перемещения фотона между ними. Чтобы предотвратить такое влияние, можно использовать запутанные фотоны. В отличие от запутанных электронов, запутанные

фотоны могут преодолевать большие расстояния, не взаимодействуя с окружающим миром.

К сожалению, это свойство фотонов не взаимодействовать с окружающим миром затрудняет их измерение. В экспериментах с запутанными фотонами многие из таких фотонов не участвуют в измерениях, поэтому теоретически может иметь место систематическая ошибка отбора — результаты отражают свойства нерепрезентативной выборки. Чтобы предотвратить систематическую ошибку отбора, можно использовать электроны. Но если использовать электроны, как тогда получить электроны, отстоящие далеко друг от друга перед измерением?

Это та самая проблема, которую решил коллектив ученых из Делфта за счет использования электронов, пойманных в ловушки в алмазах и запутанных с фотонами. Их эксперимент, похоже, закрыл обе лазейки сразу.[1]

Проблема случайности сложнее. Если копенгагенская интерпретация верна, легко можно создать поток случайных чисел. Так как эта интерпретация имеет отношение к случайности, чтобы убедиться в ее верности или ошибочности, нужно проверить последовательность чисел и убедиться в их случайности. Существует много способов, позволяющих проверить наличие закономерностей в числах. К сожалению, эти проверки могут подтвердить только неслучайность. Если последовательность не проходит проверку, можно утверждать, что она не случайна. Если последовательность проходит проверку, это хороший знак, но не доказательство случайности. Все, что можно сказать: пока ни одна из квантово-механических последовательностей не провалила проверку на случайность.

Чтобы гарантировать отсутствие корреляции между направлениями для измерения, выбираемыми Алисой и Бобом, использовались разные изощренные способы. Но опять же, нельзя исключить возможность, что то, что, по нашему мнению, является некоррелированным случайным результатом, не определяется некоторой теорией скрытых переменных.

---

[1] Статья «Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres» Б. Хенсена (B. Hensen) с соавторами, опубликованная в журнале *Nature* в 2015 году.

Большинство ученых считает, что Эйнштейн ошибался, но его теория была не лишена смысла. Белл, в частности, полагал, что классическая теория была лучшей из этих двух теорий, пока не увидел результаты экспериментов, после чего заявил: «Это так разумно. Я думаю, что когда Эйнштейн увидел это, а другие отказались это увидеть, рациональным был Эйнштейн. Другие же, хотя история оправдала их, прятали голову в песок. <...> Мне жаль, что идея Эйнштейна не подтвердилась. Разумные выводы просто не нашли подтверждения».[1]

Я сам полностью согласен с Беллом. Точка зрения Эйнштейна кажется естественной и разумной. И я удивлен, что Бор был уверен в ее ошибочности. Результат Белла, часто называемый теоремой Белла, привел к тому, что Белла номинировали на Нобелевскую премию по физике. Многие думают, что если бы он не умер от инсульта в сравнительно молодом возрасте шестидесяти одного года, то наверняка получил бы ее. Интересно, что в Белфасте есть улица, названная в честь теоремы Белла, — это, возможно, единственная теорема, название которой можно ввести в строку поиска в Google Maps и получить точный адрес.

Мы должны отказаться от стандартного предположения о локальной реальности. Когда запутанные частицы находятся далеко друг от друга, мы не должны думать о спине как о локальном свойстве, связанном с каждой частицей в отдельности; это глобальное свойство, которое следует рассматривать в терминах пары частиц.

Прежде чем завершить обзор квантовой механики, мы должны также рассмотреть еще один необычный аспект теории.

Измерение

Описывая квантовую механику, мы говорили, что вектор состояния переходит в базисный вектор, когда производится измерение. Все остается детерминированным до момента измерения, а потом происходит переход к одному из базисных векторов. Вероятности перехода к каждому из

[1] Дж. Бернштейн (J. Bernstein), *Quantum Profiles* (Princeton: Princeton University Press, 1991), 84.

базисных векторов точно известны, но они остаются всего лишь вероятностями. Детерминистская теория меняется на вероятностную, когда мы делаем измерение.

В общей теории квантовой механики так выглядит решение волнового уравнения Шредингера, которое схлопывается в момент выполнения измерения. Эрвину Шредингеру, давшему свое имя уравнению, очень не нравилась эта идея коллапса волновой функции в состояния, определяемые вероятностями.

Главная проблема заключается в отсутствии четкого определения, что именно подразумевается под измерением. Этот аспект не является частью квантовой механики. Измерения вызывают переходы, но что подразумевается под измерениями? Иногда вместо слова *измерение* использовалось слово *наблюдение*, и это заставляло некоторых говорить о сознании, вызывающем переход, но это маловероятно. Стандартно под измерением подразумевают взаимодействие с макроскопическим устройством. Измерительное устройство достаточно велико, чтобы его можно было описать с использованием классической физики, и его не нужно включать в квантово-теоретический анализ — всякий раз, когда производится измерение, мы физически взаимодействуем с измеряемым объектом, и это взаимодействие вызывает переход. Но такое объяснение выглядит недостаточно удовлетворительным. Оно выглядит правдоподобно, но ему не хватает математической точности.

Было предложено несколько разных интерпретаций квантовой механики, каждая из которых пытается устранить проблематичные аспекты, имеющие место в копенгагенской интерпретации.

Теория о *множественности миров* пытается решить проблему измерения, утверждая, что это лишь кажется, что происходит переход вектора состояния к одной из возможностей, на самом же деле существуют разные вселенные и каждая из возможностей является действительным явлением в одной из них. Вы в этой Вселенной видите один результат, а в других вселенных есть ваши двойники, которые видят другие результаты.

Бомовская механика пытается решить проблему вероятностного характера квантовой механики. Это детерминистская теория, согласно которой частицы ведут себя подобно классическим частицам. Она утверждает,

что есть еще одна новая сущность, называемая волной-пилотом, которая объясняет свойства нелокальности.

Каждая теория имеет много сторонников. Например, Дэвид Дойч (David Deutsch), с которым мы еще встретимся, уверен в правоте теории о множественности миров. Но до настоящего времени не было приведено никаких научных аргументов в пользу того или иного набора убеждений, в отличие от проверки Белла, экспериментально доказавшей ошибочность теории локальных скрытых переменных. Все интерпретации согласуются с нашей математической теорией. Каждая интерпретация — это попытка объяснить, как математическая теория связана с реальностью. Возможно, в какой-то момент найдется проницательный гений, как Белл, кто сможет показать, что разные интерпретации приводят к разным выводам, которые можно экспериментально различить, и эти эксперименты тогда дадут нам основу для выбора одной интерпретации из множества. А пока большинство физиков согласны с копенгагенской интерпретацией. Нет убедительных причин не использовать эту интерпретацию, поэтому мы и дальше будем придерживаться ее без дополнительных замечаний.

Последний раздел в этой главе показывает, что теорема Белла представляет не только академический интерес. На самом деле ее можно использовать для получения безопасного способа обмена ключами, которые потом будут использоваться для шифрования.

Протокол Экерта для квантового распределения ключей

В 1991 году Артур Экерт предложил метод, основанный на запутанных кубитах, используемых в проверке неравенства Белла. Всего есть несколько вариантов метода. Мы рассмотрим версию, которая использовалась в нашей презентации теоремы Белла.

Алиса и Боб получают поток пар кубитов. Алиса получает один кубит из каждой пары, а Боб — другой. Спины состояний запутаны. Они всегда находятся в состоянии

$$\frac{1}{\sqrt{2}}|\uparrow\rangle|\uparrow\rangle+\frac{1}{\sqrt{2}}|\downarrow\rangle|\downarrow\rangle.$$

Если Алиса и Боб измерят свои парные кубиты, используя один и тот же ортонормированный базис, они с равной вероятностью получат 0 или 1, при этом оба получат одинаковый результат.

Теперь представим протокол, следуя которому Алиса и Боб каждый раз выбирают для измерения кубитов стандартный базис. В итоге они получат одинаковую последовательность битов, и эта последовательность будет случайной последовательностью 0 и 1, что выглядит как отличный способ выбора и передачи ключа. Проблема, однако, в том, что он не совсем безопасен. Если Ева перехватит кубиты Боба, она сможет измерить их в стандартном базисе и послать соответствующие незапутанные кубиты Бобу. В результате Алиса, Боб и Ева получат идентичные последовательности битов.

Решение состоит в том, чтобы измерять кубиты с использованием базиса, случайно выбираемого из трех, — точно так же, как это делается в проверке Белла. Как и в протоколе BB84, по результатам каждого измерения Алиса и Боб записывают результат и базис, в котором он получен. Выполнив $3n$ измерений, они сравнивают последовательности выбранных базисов. Это можно делать по небезопасному каналу, потому что в этом случае посторонним будут доступны только базисы, но не результаты. Они совпадут примерно в n случаях. В каждой позиции, где выбран один и тот же базис, они получат одинаковые результаты измерений. В таких позициях они оба будут иметь 0 или оба будут иметь 1. Оставив только эти n позиции, они получат строку из 0 и 1, которая может служить ключом, если Ева их не подслушивала.

Теперь они должны проверить, не подслушала ли их Ева. Чтобы подслушать, Ева должна выполнять измерения. Всякий раз, когда она это делает, запутанное состояние перестает быть запутанным. Алиса и Боб проверяют свои строки из 0 и 1, полученные из позиций, в которых они выбирали разные базисы. Это даст им две последовательности из 0 и 1 с длиной, примерно равной $2n$. Из расчетов неравенства Белла они знают, что если состояния их кубитов запутаны, совпадения должны иметь место только в $1/4$ случаев. Но если Ева перехватывала и измеряла кубиты, пропорция совпадающих кубитов изменится. Например, если Ева измерила кубит до того, как Алиса и Боб выполнили свои измерения, легко проверить все возможные варианты, чтобы показать, что доля совпадений у Алисы

и Боба увеличится до 3/8. Это позволит им судить о присутствии Евы. Они вычисляют долю совпадений, и если она равна 1/4, они могут заключить, что их никто не подслушивал и можно использовать получившийся ключ.

Протокол Экерта имеет полезное свойство, которое заключается в том, что в процессе его выполнения генерируется ключ. Никакие цифр генерировать и сохранять заранее не требуется, благодаря чему устраняется одна из основных угроз при шифровании. Этот протокол был успешно опробован в лабораторных условиях с использованием запутанных фотонов.

На этом мы завершаем введение в понятия квантовой механики, и теперь нам предстоит познакомиться с классическими вычислениями. Это станет темой следующей главы.

6 Классическая логика, вентили и цепи

В этой главе мы кратко рассмотрим классические вычисления, знакомясь с идеями в хронологическом порядке их появления. Начнем с логических функций и логики, введенной Джорджем Булем в конце XIX века. В 1930-х годах Клод Шеннон изучал булеву алгебру (алгебру логики) и заметил, что булевы функции можно описать с использованием аналогии электрических выключателей. Электрические компоненты, соответствующие булевым функциям, называют логическими вентилями. При использовании такой аналогии составление булевых функций превращается в составление цепей с применением этих вентилей. Сначала мы исследуем булевы функции с позиции логики; затем посмотрим, как преобразовать их в цепи и вентили. Все эти сведения в настоящее время считаются стандартными и приводятся в каждом вводном курсе информатики. Но после знакомства с этим вводным материалом мы рассмотрим несколько идей, которые редко можно встретить в стандартных введениях.

В 1970-х годах лауреат Нобелевской премии по физике Ричард Фейнман заинтересовался вычислительной техникой и в течение нескольких лет в начале 1980-х читал курс по вычислительной технике в Калифорнийском технологическом институте. В конечном итоге его лекции были опубликованы под названием *Feynman Lectures on Computation* (Фейнмановские лекции по вычислениям). Интерес Фейнмана к вычислительной технике отчасти был обусловлен его общением с Эдвардом Фредкиным и знакомством с уникальными взглядами Фредкина на физику и вычисления. Фредкин считал, что Вселенная — это своеобразный компьютер,

и поскольку физические законы обратимы, мы должны изучать обратимые вычисления и обратимые вентили. Но несмотря на то что тезис Фредкина не получил широкой поддержки в сообществе физиков, он получил известность благодаря своим блестящим и нестандартным идеям. Одной из них является бильярдный компьютер. Книга Фейнмана включает рассмотрение обратимых вентилей и демонстрирует, что любое вычисление можно представить в виде сталкивающихся бильярдных шаров.

Мы воспользуемся подходом Фейнмана. Как оказывается, обратимые вентили — это как раз то, что нужно для квантовых вычислений. Бильярдный компьютер навел Фейнмана на идею заменить бильярдные шары частицами. Это вдохновило его на работу в области квантовых вычислений, но мы включили описание этой идеи в книгу в основном из-за ее простоты и оригинальности.

Логика

В конце XIX века Джордж Буль заметил, что некоторые элементы логики можно рассматривать с точки зрения алгебры, то есть существующие законы логики можно выразить в алгебраических терминах. В настоящее время мы используем стандартный способ введения в булеву логику с помощью таблиц истинности для трех основных операций *not* (*НЕ*), *and* (*И*) и *or* (*ИЛИ*).

Отрицание

Если утверждение истинно, тогда его отрицание ложно, и наоборот, если утверждение ложно, тогда его отрицание истинно. Например, утверждение $2 + 2 = 4$ истинно, а его отрицание $2 + 2 \neq 4$ ложно. Часто конкретные примеры мы заменяем символами *P*, *Q* и *R*. Например, утверждение $2 + 2 = 4$ можно представить символом *P*. Символ ¬ обозначает отрицание — *НЕ*; если *P* представляет утверждение $2 + 2 = 4$, тогда $\neg P$ обозначает обратное утверждение $2 + 2 \neq 4$. Теперь можно обобщить некоторые базовые свойства отрицания с использованием наших символов: если *P* истинно, тогда $\neg P$ ложно. Если *P* ложно, тогда $\neg P$ истинно.

Чтобы еще больше сократить объяснения, можно использовать символы *T* и *F* для обозначения *истинности* (true) и *ложности* (false) соответственно. Теперь можно определить свойства в виде таблицы.

P	**¬P**
T	F
F	T

И

Операция *И* (*and*) обозначается символом ∧. Два утверждения, *P* и *Q*, можно объединить в выражение $P \wedge Q$. Утверждение $P \wedge Q$ истинно, только если оба составляющих его утверждения, *P* и *Q*, истинны. Свойства операции *И* определяются следующей таблицей, где в первых двух столбцах перечисляются возможные комбинации истинности *P* и *Q*, а в третьем столбце приводится соответствующее значение истинности операции $P \wedge Q$.

P	**Q**	**P ∧ Q**
T	T	T
T	F	F
F	T	F
F	F	F

ИЛИ

Операция *ИЛИ* (*or*) обозначается символом ∨ и определяется следующей таблицей.

P	**Q**	**P ∨ Q**
T	T	T
T	F	T
F	T	T
F	F	F

Обратите внимание, что $P \vee Q$ истинно, если одно из утверждений, P или Q, истинно, то есть $P \vee Q$ истинно, если истинно хотя бы одно из утверждений, P или Q, а также если истинны оба этих утверждения. В математике операция ИЛИ часто называется *включающим ИЛИ*. *Исключающее ИЛИ* дает истину, только когда какое-то одно из утверждений, P или Q, истинно, но не оба. Оно дает ложь, если оба утверждения ложны, а также если оба утверждения истинны. Операция *исключающего ИЛИ* обозначается символом $\oplus$. Соответствующая таблица истинности показана ниже.

P	**Q**	**P ⊕ Q**
T	T	F
T	F	T
F	T	T
F	F	F

(Позже вы узнаете, почему для обозначения *исключающего ИЛИ* используется символ, напоминающий знак «плюс», — он соответствует сложению по модулю два.)

Булева алгебра

Начнем с того, что посмотрим, как конструировать таблицу истинности для любого выражения с двумя членами. Чтобы говорить предметно, сконструируем таблицу истинности для выражения $\neg(\neg P \wedge \neg Q)$. Для этого нужно выполнить несколько шагов. Сначала запишем в таблицу все возможные значения для P и Q.

P	**Q**
T	T
T	F
F	T
F	F

Затем присоединим столбцы для $\neg P$ и $\neg Q$, и запишем в них соответствующие значения истинности.

P	Q	¬P	¬Q
T	T	F	F
T	F	F	T
F	T	T	F
F	F	T	T

Затем добавим столбец для $\neg P \wedge \neg Q$. Это выражение истинно, только когда оба утверждения, $\neg P$ и $\neg Q$, истинны.

P	Q	¬P	¬Q	¬P ∧ ¬Q
T	T	F	F	F
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

Наконец, добавим столбец для $\neg(\neg P \wedge \neg Q)$. Это утверждение истинно, только если $\neg P \wedge \neg Q$ ложно.

P	Q	¬P	¬Q	¬P ∧ ¬Q	¬(¬P ∧ ¬Q)
T	T	F	F	F	T
T	F	F	T	F	T
F	T	T	F	F	T
F	F	T	T	T	F

Опустив столбцы, соответствующие промежуточным шагам, получаем следующую таблицу.

P	Q	¬(¬P ∧ ¬Q)
T	T	T
T	F	T
F	T	T
F	F	F

Логическая эквивалентность

Обратите внимание, что значения истинности в таблице для $\neg(\neg P \wedge Q)$ идентичны значениям истинности в таблице для $P \vee Q$. Они абсолютно одинаковы во всех случаях. В таких случаях мы говорим, что утверждения $P \vee Q$ и $\neg(\neg P \wedge Q)$ *логически эквивалентны*. Записывается это так:

$$P \vee Q \equiv \neg(\neg P \wedge \neg Q).$$

Отсюда следует, что операцию *ИЛИ* можно вообще никогда не использовать. Если в выражении присутствует *ИЛИ*, такое выражение можно переписать с использованием $\neg$ и $\wedge$.

А можно ли точно так же избавиться от *исключающего ИЛИ*, которое обозначается символом $\oplus$? Можно ли заменить его выражением, в котором используются только $\neg$ и $\wedge$? Да, можно, и сейчас мы убедимся в этом.

Рассмотрим таблицу истинности для $\oplus$.

P	**Q**	**P $\oplus$ Q**
T	T	F
T	F	T
F	T	T
F	F	F

Найдем записи с символом *T* в третьем столбце. Первый встречается в строке, где *P* имеет значение *T* и *Q* имеет значение *F*. Значение *T* только для этой комбинации значений истинности *P* и *Q* нам дает выражение $P \wedge \neg Q$. Следующее значение *T* в третьем столбце встречается в строке, где *P* имеет значение *F* и *Q* имеет значение *T*. Значение *T* только для этой комбинации значений истинности *P* и *Q* нам дает выражение $\neg P \wedge Q$.

Символ *T* встречается в третьем столбце только в этих строках. Чтобы получить выражение, эквивалентное заданному, теперь нужно объединить все сконструированные выражения с использованием $\vee$, то есть

$$P \oplus Q = (P \wedge \neg Q) \vee (\neg P \wedge Q).$$

Мы знаем, что

$$P \vee Q \equiv \neg\left(\neg P \wedge \neg Q\right).$$

Использовав его для замены $\vee$, получаем

$$P \oplus Q \equiv \neg\left(\neg\left(P \wedge \neg Q\right) \wedge \left(\neg\left(\neg P \wedge Q\right)\right)\right).$$

Как видите, мы можем полностью отказаться от $\oplus$. Если в выражении присутствует $\oplus$, такое выражение можно переписать с использованием $\neg$ и $\wedge$. Метод, который мы только что использовали для замены $\oplus$ операциями $\neg$ и $\wedge$, довольно универсален.

Функциональная полнота

Только что представленные логические операторы можно рассматривать как функции. Например, $\wedge$ — это функция с двумя аргументами, P и Q, и одним возвращаемым значением; $\neg$ — имеет один аргумент и одно возвращаемое значение.

Мы могли бы сконструировать свою функцию, принимающую несколько аргументов, которые могут иметь значения T и F, и для каждого случая возвращающую значение T или F. Такие функции называют *булевыми функциями*. Для предметного рассмотрения сконструируем функцию, принимающую три аргумента — P, Q и R. Назовем ее $f\left(P,Q,R\right)$. Чтобы определить функцию, нам нужно заполнить четвертый столбец в следующей таблице.

P	Q	R	f(P, Q, R)
T	T	T	
T	T	F	
T	F	T	
T	F	F	
F	T	T	
F	T	F	
F	F	T	
F	F	F	

Всего мы должны записать восемь значений. Для каждого значения на выбор есть два варианта, то есть всего существует 2^8 возможные функции. Далее вы увидите, что независимо от выбора функции всегда можно найти эквивалентное выражение, в котором используются только функции $\neg$ и $\wedge$.

Для этого используем тот же метод, с помощью которого преобразовывали выражение

$$P \oplus Q \equiv (P \wedge \neg Q) \vee (\neg P \wedge Q).$$

Начнем с поиска значений *T* в последнем столбце. Чтобы вам было проще, используем конкретную функцию, заданную следующей таблицей, но вообще этот метод применим к любой булевой функции.

P	Q	R	f(P, Q, R)
T	T	T	F
T	T	F	F
T	F	T	T
T	F	F	F
F	T	T	F
F	T	F	T
F	F	T	F
F	F	F	T

Первый символ *T* встречается в строке, где *P* и *R* имеют значение *T*, а *Q* — значение *F*. Значение *T* только для этой комбинации значений истинности *P*, *Q* и *R* дает выражение $P \wedge \neg Q \wedge R$. Следующий символ *T* встречается в строке, где *P* и *R* имеют значение *F*, а *Q* — значение *T*. Значение *T* только для этой комбинации значений истинности дает выражение $\neg P \wedge Q \wedge \neg R$. Последний символ *T* встречается в строке, где все три компонента — *P*, *Q* и *R* — имеют значение *F*. Значение *T* только для этой комбинации значений истинности дает выражение $\neg P \wedge \neg Q \wedge \neg R$.

Выражение, которое дает значение *T*, только в этих трех случаях имеет вид

$$(P \wedge \neg Q \wedge R) \vee (\neg P \wedge Q \wedge \neg R) \vee (\neg P \wedge \neg Q \wedge \neg R),$$

то есть

$$f(P,Q,R) \equiv (P \wedge \neg Q \wedge R) \vee (\neg P \wedge Q \wedge \neg R) \vee (\neg P \wedge \neg Q \wedge \neg R).$$

Заключительный шаг — замена оператора $\vee$ с использованием того факта, что

$$P \vee Q \equiv \neg(\neg P \wedge \neg Q).$$

В результате замены первого оператора получаем:

$$f(P,Q,R) \equiv \neg(\neg P \wedge \neg Q \wedge R) \wedge \neg(\neg P \wedge Q \wedge \neg R) \vee (\neg P \wedge \neg Q \wedge \neg R).$$

Заменив второй оператор, получаем выражение, логически эквивалентное *f*(*P*, *Q*, *R*)

$$\neg\Big(\neg\Big[\neg\big(\neg(P \wedge \neg Q \wedge R) \wedge \neg(\neg P \wedge Q \wedge \neg R)\big)\Big] \wedge \neg[\neg P \wedge \neg Q \wedge \neg R]\Big).$$

Это универсальный метод. Если есть некоторая функция *f*, заданная таблицей истинности, тогда можно найти выражение, которое будет логически эквивалентно функции *f* и будет содержать только операторы ¬ и ∧. Поскольку любую булеву функцию можно выразить с использованием только этих двух функций, мы говорим, что $\{\neg, \wedge\}$ — это *функционально полное* множество булевых операторов.

Возможность выразить любую функцию, определенную таблицей истинности, только с использованием ¬ и ∧ кажется удивительной, но еще более удивительной выглядит другая, более удобная возможность. Существует двухместный оператор, который называется *Nand* (*И-НЕ*), и для любой булевой функции существует логически эквивалентное выражение, использующее только оператор *Nand* (*И-НЕ*).

И-НЕ

Nand — это составное слово, сформированное из слов *not* (НЕ) и *and* (И). Этот оператор обозначается символом ↑. Его можно определить как $P \uparrow Q = \neg(P \wedge Q)$ или с помощью следующей таблицы истинности:

P	Q	P ↑ Q
T	T	F
T	F	T
F	T	T
F	F	T

Мы знаем, что $\{\neg,\wedge\}$ — это функционально полное множество операторов, поэтому, чтобы показать, что оператор *И-НЕ* сам является функционально полным множеством — и с его помощью можно записать выражение, эквивалентное любой булевой функции, — нам просто нужно показать, что оба оператора, *И* и *НЕ*, можно заменить единственным оператором *И-НЕ*.

Взгляните на следующую таблицу истинности, в которой перечислены значения истинности только для утверждения *P*, затем для $P \wedge P$ и, наконец, для $\neg(P \wedge P)$.

P	P ∧ P	¬(P ∧ Q)
T	T	F
F	F	T

Обратите внимание, что значения истинности в последнем столбце совпадают со значениями истинности для $\neg P$, то есть

$$\neg(P \wedge P) \equiv \neg P,$$

но $\neg(P \wedge P)$ эквивалентно выражению $P \uparrow P$, то есть

$$P \uparrow P \equiv \neg P.$$

Это показывает, что все вхождения *НЕ* можно заменить на *И-НЕ*. Теперь обратим внимание на оператор *И*.

Мы уже видели, что

$$P \wedge Q \equiv \neg\neg(P \wedge Q).$$

Соответственно, $\neg(P \wedge Q) \equiv P \uparrow Q$, то есть

$$P \wedge Q \equiv \neg(P \uparrow Q).$$

Заменим оператор *НЕ* в предыдущем выражении, используя предыдущее равенство, и получим

$$P \wedge Q \equiv (P \uparrow Q) \uparrow (P \uparrow Q).$$

Впервые функциональная полнота оператора *И-НЕ* была официально отмечена в работе Генри М. Шеффера (Henry M. Sheffer) в 1913 году. Чарльз Сандерс Пирс (Charles Sanders Peirce) узнал об этом факте еще в конце XIX века, но этот труд, как и большая часть его оригинальных работ, был опубликован намного позже. (Для обозначения оператора *И-НЕ* Шеффер использовал символ |. Многие авторы используют или использовали его вместо ↑. Он называется *штрих Шеффера*.)

Булевы переменные принимают одно из двух значений. В примерах выше мы использовали *T* и *F*, но точно так же можно использовать любую другую пару символов. Например, можно использовать цифры 0 и 1. Такая замена *T* и *F* на 0 и 1 позволяет нам рассуждать о булевых функциях как о функциях, оперирующих битами. Так мы и будем поступать, начиная с этого момента.

Замену можно осуществить двумя способами. Мы будем использовать вариант, когда 0 заменяет *F*, а 1 заменяет *T*. Обратите внимание, что условно мы перечисляем *T* перед F, но 0 перед 1. Соответственно, при использовании 0 и 1 строки в таблицах истинности перечисляются в порядке, обратном по отношению к таблицам, записанным с использованием *T* и *F*. Это не должно вызывать никакой путаницы, но чтобы было понятнее, ниже приводятся две таблицы для $P \vee Q$.

P	Q	P ∨ Q
T	T	T
T	F	T
F	T	T
F	F	F

P	Q	P ∨ Q
0	0	0
0	1	1
1	0	1
1	1	1

Вентили

Многие исследователи заметили, что если логику выразить в терминах алгебры, то можно спроектировать машины, выполняющие логические операции. Самым известным исследователем является Клод Шеннон, который показал, что всю булеву алгебру можно выразить с использованием электрических выключателей. Это одна из фундаментальных идей, лежащих в основе схемотехники всех современных компьютеров. Самое интересное, что он сделал это, еще будучи студентом MIT.

В дискретные интервалы времени электрический импульс или передается, или нет. Если в соответствующий интервал времени мы получаем импульс, то представляем его как значение истинности *T* или эквивалентное битовое значение 1. Если в соответствующий интервал времени мы не получаем импульс, то представляем его как значение истинности *F* или эквивалентное битовое значение 0.

Комбинации выключателей, соответствующие нашим двухместным операторам, называют *вентилями*. Распространенные вентили имеют соответствующие им диаграммы. Рассмотрим некоторые из них.

Вентиль НЕ

На рис. 6.1 показан значок, изображающий вентиль *НЕ*. Его можно представить как устройство, в которое импульс входит слева и выходит справа. Если на вход подать 1, на выходе получится 0. Если на вход подать 0, на выходе получится 1.

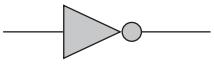


Рис. 6.1. Вентиль НЕ

Вентиль И

На рис. 6.2 показан значок, изображающий вентиль *И*. И снова читать его нужно слева направо. Он имеет два входа, которые могут принимать значение 0 или 1, и один выход. На рис. 6.3 изображены четыре возможные комбинации.

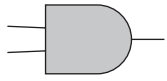


Рис. 6.2. Вентиль И

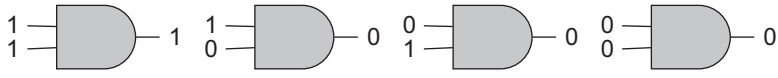


Рис. 6.3. Четыре возможные комбинации входов вентиля И

Вентиль ИЛИ

На рис. 6.4 показан значок, изображающий вентиль *ИЛИ*, а также четыре возможные комбинации его входов и выхода.

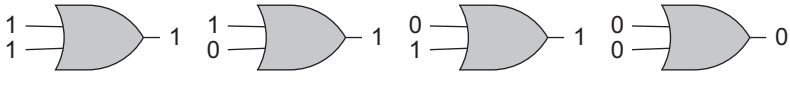


Рис. 6.4. Вентиль ИЛИ

Вентиль И-НЕ

На рис. 6.5 показан значок, изображающий вентиль *И-НЕ*, а также четыре возможные комбинации его входов и выхода.

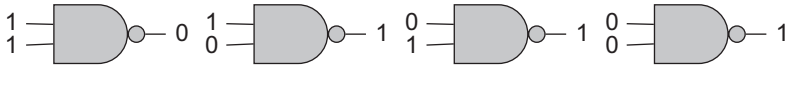


Рис. 6.5. Вентиль И-НЕ

Цепи

Вентили можно соединять и формировать из них цепи. Эти цепи не замкнуты — они линейны и читаются слева направо. Мы подаем наши биты на входы слева и читаем выходы справа. Рассмотрим несколько

примеров, соответствующих булевым функциям, представленным выше.

Начнем с булева выражения $\neg(\neg P \wedge \neg Q)$. Используя вентили, мы можем собрать соответствующую цепь. Такая цепь изображена на рис. 6.6, где входные и выходные выводы вентилей подписаны соответствующими выражениями. Напомню, что $P \vee Q \equiv \neg(\neg P \wedge \neg Q)$, поэтому цепь на рис. 6.6 эквивалентна вентилю ИЛИ.

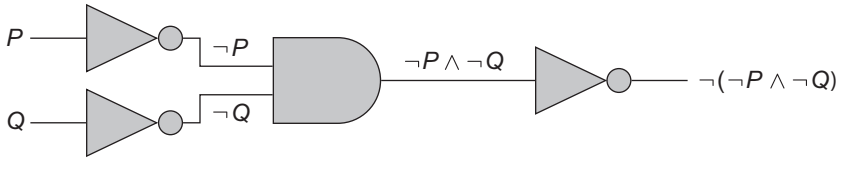


Рис. 6.6. Цепь для ¬(¬P ∧ ¬Q)

Следующий пример — выражение $P \uparrow P$. На оба входа вентиля И-НЕ подается одно и то же значение *P*. Такого разбиения сигнала на два можно добиться подключением дополнительного провода. Процесс разбиения сигнала на несколько копий называют *разветвлением*. Соответствующая цепь изображена на рис. 6.7.

Мы знаем, что $P \uparrow P \equiv \neg P$, поэтому цепь на рис. 6.7 эквивалентна вентилю *НЕ*.

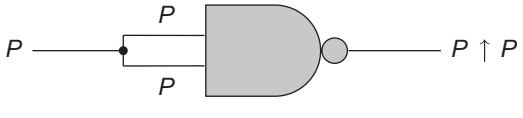


Рис. 6.7. Цепь для P ↑ P

И последний пример — выражение с двумя членами $(P \uparrow Q) \uparrow (P \uparrow Q)$. Чтобы получить две копии $P \uparrow Q$, снова используется разветвление. Соответствующая цепь изображена на рис. 6.8.

Мы также знаем, что $P \wedge Q \equiv (P \uparrow Q) \uparrow (P \uparrow Q)$, поэтому цепь на рис. 6.8 также эквивалентна вентилю *И*.

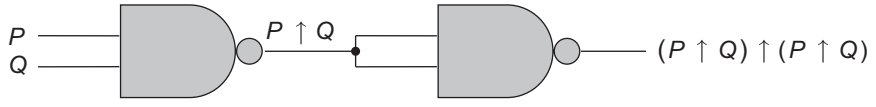


Рис. 6.8. Цепь для (P ↑ Q) ↑ (P ↑ Q)

И-НЕ — универсальный вентиль

Выше мы показали, что булева функция *И-НЕ* является функционально полной. В этом разделе мы повторно докажем это, но уже с использованием вентилей.

В прошлый раз мы сначала показали, что любое вхождение оператора *ИЛИ* можно заменить, используя следующее тождество:

$$P \vee Q \equiv \neg\left(\neg P \wedge \neg Q\right).$$

Соответствующая цепь, изображенная на рис. 6.6, показывает, что мы вообще можем не использовать вентиль *ИЛИ*.

Затем мы показали, что любую булеву функцию можно сконструировать, используя только комбинацию операторов *НЕ* и *И*. Следовательно, для любой булевой функции можно собрать цепь, используя только вентили *НЕ* и *И*.

Затем мы показали, что оба оператора, *НЕ* и *И*, можно заменить оператором *И-НЕ*, доказав тем самым, что *И-НЕ* сам является функционально полным. То же верно в отношении вентиля *И-НЕ*. Для любой булевой функции можно собрать цепь, используя только вентили *И-НЕ*. Вместо определения *функционально полный* к вентилям применяется определение *универсальный*, то есть *И-НЕ* — универсальный вентиль. Но давайте рассмотрим сложившуюся ситуацию немного под другим углом.

Схемы на рис. 6.7 и 6.8 демонстрируют, как избавиться от вентилей *НЕ* и *И*, заменив их вентилями *И-НЕ*. Но обратите внимание, что при этом мы вынуждены прибегнуть к разветвлению сигналов. Эта операция получает один бит информации и возвращает два бита, идентичных входному биту. Как может показаться, в этом нет ничего особенного; просто нужно

добавить еще кусок провода, но позже мы увидим, что эта операция невозможна применительно к квантовым битам.

Вентили и вычисления

Вентили — основные строительные блоки, из которых создаются современные компьютеры. Вентили можно использовать для выполнения не только логических операций, но и вычислений. Мы не будем подробно изучать, как это делается. (Если вам интересно, отыщите книгу *Code* Чарльза Петцольда (Charles Petzold),[1] где он начинает описание с выключателей и затем показывает, как конструируются компьютеры.) Но рассмотрим пример, иллюстрирующий идеи, лежащие в основе реализации операции сложения.

Напомню, что оператор *исключающее ИЛИ* обозначается символом $\oplus$. Он определяется так:

$$0 \oplus 0 = 0 \qquad 0 \oplus 1 = 1 \qquad 1 \oplus 0 = 1 \qquad 1 \oplus 1 = 0$$

Это можно сравнить со сложением четных и нечетных чисел. Мы знаем, что:

чет+чет=чет, чет+нечет=нечет, нечет+чет=нечет, нечет+нечет=чет.

Такое сложение «чет» и «нечет» часто называют *сложением по модулю 2*. Если «чет» обозначить как 0, а «нечет» как 1, то сложение по модулю 2 обозначается как $\oplus$. Именно поэтому для обозначения оператора *исключающего ИЛИ* используется символ, похожий на знак «плюс». (Часто проще выполнять вычисления с $\oplus$, интерпретируя его как сложение, а не как *исключающее ИЛИ*.)

Шлюз *исключающее ИЛИ* также часто называют *XOR* и обозначают значком, изображенным на рис. 6.9.

---

[1] Чарльз Петцольд. *Код. Тайный язык информатики*. Русская Редакция (2001). — *Примеч. пер.*

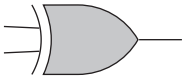


Рис. 6.9. Вентиль исключающее ИЛИ

Мы будем использовать этот вентиль для конструирования так называемого полусумматора (одноразрядного сумматора). Эта цепь складывает две двоичные цифры. Чтобы было понятнее, сравним его с десятичным полусумматором. Если имеются две десятичные цифры, сумма которых меньше десяти, мы просто складываем их. Например, 2 + 4 = 6, 3 + 5 = 8.

Но если сумма цифр больше десяти, мы записываем соответствующую цифру из младшего разряда результата и запоминаем перенос единицы в старший разряд для следующего шага в вычислениях. Например, 7 + 5 = 2, и мы запоминаем 1.

Двоичный полусумматор действует аналогично. Мы можем сконструировать его с использованием вентилей *исключающее ИЛИ* (*XOR*) и *И*. Вентиль *исключающее ИЛИ* вычисляет цифру младшего разряда, а вентиль *И* запоминает перенос единицы в старший разряд.

$$0+0=0,\ \textit{с переносом}\ =\ 0;$$
$$0+1=1,\ \textit{с переносом}\ =\ 0;$$
$$1+0=1,\ \textit{с переносом}\ =\ 0;$$
$$1+1=0,\ \textit{с переносом}\ =\ 1.$$

Такая цепь изображена на рис. 6.10. (Пересечения проводов с точками на этом рисунке изображают операции разветвления. Пересечения без точек означают простое перекрещивание проводов, без контакта между ними.)

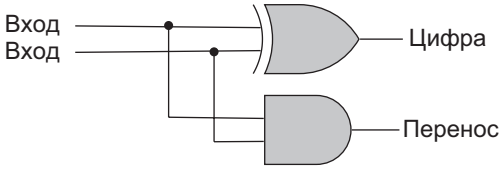


Рис. 6.10. Схема полусумматора

Эта цепь называется полусумматором, а не просто сумматором, потому что не предусматривает учета сигнала переноса, который мог быть получен на

предыдущем шаге. Рассмотрим пример сложения обычных десятичных чисел. Допустим, что нам требуется сложить следующие четырехзначные числа (звездочками изображены неизвестные цифры).

```
  **6*
+ **5*
------
```

Сложив 6 и 5, мы получаем цифру 1, и еще одна единица переносится в старший разряд, но вполне возможно, что перенос также будет получен при сложении цифр в предыдущем разряде, тогда мы получим цифру 2 и признак переноса единицы в следующий разряд. Полный сумматор учитывает возможность получения признака переноса из предыдущего шага.

Мы не будем рисовать схему полного двоичного сумматора, но легко могли бы сделать это. Так как схему на любых вентилях можно заменить эквивалентной схемой, состоящей только из вентилей *И-НЕ*, мы можем сконструировать сумматор, используя только вентили *И-НЕ* и ветвления. Фактически, используя только эти два компонента, можно собрать целый компьютер.

Память

Выше мы видели, как использовать вентили для выполнения логических и арифметических операций, но чтобы сконструировать настоящий компьютер, еще необходимо каким-то способом реализовать хранение данных. Это тоже можно сделать с помощью вентилей. Если подробно описывать этот вопрос, можно уйти слишком далеко в сторону, поэтому просто отмечу, что ключевой идеей является создание триггера. Триггер можно создать на вентилях с обратной связью. Выходы вентилей в этом случае поступают обратно на входы. Пример триггера на двух вентилях *И-НЕ* показан на рис. 6.11. Мы не будем вдаваться в подробное описание реализации, но отметим, что при использовании обратной связи важно правильно синхронизировать входы и выходы. Это то место, где в игру вступают часы, посылающие электрические импульсы с постоянными интервалами времени.

Обратимые вычисления

Теперь, получив некоторое представление о том, как собрать компьютер на классических вентилях, перейдем к обзору обратимых вентилей.

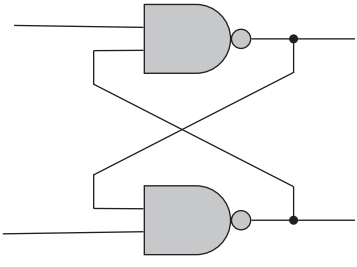


Рис. 6.11. Триггер на двух вентилях И-НЕ

Вентили можно рассматривать как булевы функции. Например, вентиль *И* принимает на входе два булева значения и выводит одно булево значение. Часто работу вентиля проще представить в виде таблицы. (Это та же самая таблица, которую мы называли таблицей истинности.)

И	
Входы	**Выход**
0 0	0
0 1	0
1 0	0
1 1	1

С помощью такой же таблицы можно описать работу полусумматора. Но на этот раз у нас имеются два входа и два выхода.

Полусумматор		
Входы	**Выход**	
	цифра	**перенос**
0 0	0	0
0 1	1	0
1 0	1	0
1 1	0	1

В этом разделе мы рассмотрим обратимые вентили. Они соответствуют обратимым функциям. Можно ли по результату на выходе определить входные значения? Если да, значит, функция обратима — вентиль обратим.

Если на выходе вентиля *И* получилась 1, можно утверждать, что на вход были поданы две 1, но 0 на выходе может получиться из трех разных пар входных значений, и, не имея никакой дополнительной информации, нельзя точно сказать, какая из трех комбинаций имелась на входе. То есть вентиль *И* не является обратимым.

Полусумматор тоже необратим. Цифру а и перенос 0 на выходе дают две комбинации входных значений. В обоих этих случаях у нас есть два бита на входе, но мы не получаем двух битов на выходе. То есть в процессе вычислений часть информации теряется.

Изучение обратимых вентилей и обратимых вычислений начиналось с исследования термодинамики вычислений. Шеннон определил понятие энтропии для информации. Понятие энтропии также существует в термодинамике. Именно этот факт натолкнул Шеннона на мысль. Насколько тесно эти две энтропии связаны друг с другом? Можно ли выразить теорию вычислений с точки зрения термодинамики? В частности, можно ли говорить о минимальной энергии, необходимой для выполнения вычислений? Джон фон Нейман предположил, что с потерей информации расходуется энергия — она рассеивается в виде тепла. Рольф Ландауэр (Rolf Landauer) доказал это предположение и рассчитал количество энергии, минимально необходимое, чтобы стереть один бит информации. Это количество энергии получило название *предел Ландауэра*.

Однако в обратимых вычислениях информация не теряется, и теоретически такие вычисления могут выполняться без потери энергии.

Далее мы рассмотрим три обратимых вентиля: *CNOT* (*управляемое НЕ*), *Тоффоли* и *Фредкин*.

Управляемое НЕ

Вентиль *управляемое НЕ* (*controlled not*, или *CNOT*) имеет два входа и два выхода. Первый вход называется управляющим битом. Если он

равен 0, тогда вентиль пропускает второй входной бит без изменения. Если управляющий бит равен 1, тогда вентиль преобразует второй входной бит как вентиль *НЕ*. Управляющий бит является первым входным битом и обозначается как x. Этот бит передается на первый выход без изменений. Второй выход равен второму входу, если управляющий бит равен 0, и получает противоположное значение, если управляющий бит равен 1. Эта функция задается выражением $f(x, y) = (x, x \oplus y)$ или следующей таблицей.

Управляемое НЕ			
Вход		**Выход**	
x	**y**	**x**	**x ⊕ y**
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Обратите внимание, что эта операция обратима. Любой паре выходных значений соответствует точно одна пара входных значений.

Цепь, реализующую эту операцию, можно сконструировать с использованием разветвления и вентиля *исключающее ИЛИ*. Она изображена на рис. 6.12.

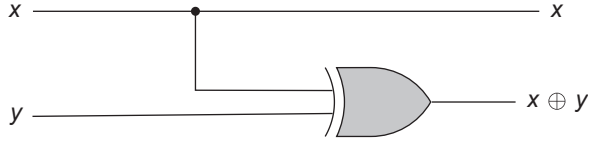


Рис. 6.12. Схема вентиля управляемое НЕ

Однако такая схема редко изображается на практике. Обычно используется более упрощенный ее вариант, как показано на рис. 6.13.

Вентиль *управляемое НЕ* не только обратим, но также обладает замечательным свойством инверсии самого себя. То есть если соединить в цепь

два вентиля *управляемое НЕ* друг за другом, соединив выход первого вентиля со входом второго, выход второго вентиля будет идентичен входу первого. Второй вентиль отменяет действие первого. Чтобы убедиться в этом, вспомним, что действие вентиля *управляемое НЕ* определяется формулой

$$f(x,y)=(x,x\oplus y).$$

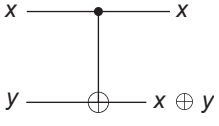


Рис. 6.13. Типичная схема для изображения вентиля управляемое НЕ

Подставив вывод первого вентиля в формулу для второго, получим

$$f(x,x\oplus y)=(x,x\oplus x\oplus y)=(x,y).$$

Здесь мы использовали тот факт, что $x\oplus x=0$ и $0\oplus y=y$.

Вначале мы имеем на входе (x, y) и после прохождения двух вентилей снова получаем пару (x, y), с которой начали.

Вентиль Тоффоли

Вентиль *Тоффоли*, предложенный Томасом Тоффоли (Tommaso Toffoli), имеет три входа и три выхода. Первые два — управляющие биты. Они инвертируют третий входной бит, если оба равны 1, иначе третий бит передается на выход без изменений. Так как этот вентиль подобен вентилю *управляемое НЕ* (*CNOT*), но имеет два управляющих бита, иногда его называют *управляемое НЕ* (*CCNOT*). Действие этого вентиля описывается функцией:

$$T(x,y,z)=(x,y,(x\wedge y)\oplus z).$$

В табличной форме он задается, как показано ниже.

Вентиль Тоффоли					
Вход			**Выход**		
x	y	z	x	y	$(x \wedge y) \oplus z$
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Стандартная схема этого вентиля является расширением диаграммы вентиля *управляемое НЕ* (рис. 6.14).

Из таблицы видно, что вентиль *Тоффоли* обратим — каждой тройке выходных значений соответствует точно одна строка входных значений. Подобно вентилю *управляемое НЕ*, этот вентиль обладает свойством инверсии самого себя.

Как мы уже знаем, $T(x, y, z) = (x, y, (x \wedge y) \oplus z)$. Если теперь выход первого вентиля подставить в формулу для второго вентиля, получим:

$$T(x, y, (x \wedge y) \oplus z) = (x, y, (x \wedge y) \oplus (x \wedge y) z) = (x, y, z).$$

Здесь мы использовали тот факт, что $(x \wedge y) \oplus (x \wedge y) = 0$ и $0 \oplus z = z$.

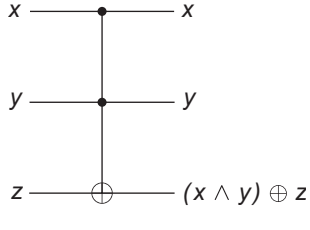


Рис. 6.14. Вентиль Тоффоли

Вентиль *Тоффоли* тоже универсален. Как мы уже знаем, любую булеву цепь можно сконструировать исключительно с использованием вентилей *И-НЕ* и разветвлений. Чтобы убедиться в универсальности вентиля *Тоффоли*, достаточно показать, что с его помощью можно сконструировать оба вентиля, *И* и *НЕ*.

Вентиль *И-НЕ* описывается формулой $f(x, y) = \neg(x \wedge y)$, поэтому мы должны подать на вход x и y и получить на выходе $\neg(x \wedge y)$. Но так как мы используем вентиль *Тоффоли*, будем подавать на вход три значения и получать на выходе тоже три значения. Выражение $\neg(x \wedge y)$ логически эквивалентно выражению $(x \wedge y) \oplus 1$. На третий вход мы можем всегда подавать 1 и игнорировать первые два выхода. Используем

$$T(x, y, 1) = (x, y, (x \wedge y) \oplus 1) = (x, y, \neg(x \wedge y)),$$

чтобы показать, что *управляемое НЕ* можно сымитировать, подавая на вход x и y и читая только третий выход.

Аналогично можно реализовать разветвление. Для этого нужно подать на вход только одно значение x и получить на выходе два значения x. И снова, так как вентиль *Тоффоли* имеет три входа и три выхода, мы можем зафиксировать два других входа, кроме x, и получать значения x на двух выходах, игнорируя третий. Реализовать это можно так:

$$T(x, 1, 0) = (x, 1, x).$$

То есть любую булеву цепь можно сконструировать, используя только вентили *Тоффоли*.

Эти конструкции иллюстрируют явление, часто возникающее при использовании обратимых вентилей. Число входов должно быть равно числу выходов, но часто бывает нужно вычислить что-то, когда число входов и выходов различается. Мы всегда можем реализовать такую схему, добавляя дополнительные входные биты, которые часто называются вспомогательными, или игнорируя некоторые выходные биты, которые иногда называют мусорными, или посторонними. В примере, где мы показали, как с помощью вентиля *Тоффоли* получить разветвление, использовалась формула $T(x, 1, 0) = (x, 1, x)$. Значения 1 и 0 на входе — это вспомогательные биты, а 1 на выходе — мусорный бит.

Вентиль Фредкина

Вентиль *Фредкина* также имеет три входа и три выхода. Первый вход — управляющий бит. Если он равен 0, второй и третий входные биты передаются на выход без изменений. Если управляющий бит равен 1, он меняет второй и третий входные биты местами — на второй выход подается третий вход, а на третий выход — второй вход. Этот вентиль определяется формулой

$$F(0, y, z) = (0, y, z),\ F(1, y, z) = (1, z, y).$$

В табличной форме он задается, как показано ниже.

Вентиль Фредкина					
Вход			**Выход**		
x	y	z	x		
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	1	1

Из таблицы видно, что вентиль *Фредкина* обратим и, так же как вентили *управляемое НЕ* и *Тоффоли*, обладает свойством инверсии самого себя. По таблице также можно заметить еще одно свойство — количество 1 на входах равно количеству 1 на выходах. Мы воспользуемся этим фактом позже, когда будем конструировать вентиль Фредкина с использованием бильярдных шаров. (Для вентилей бильярдных шаров должно соблюдаться свойство равенства числа бильярдных шаров на входе с числом бильярдных шаров на выходе.) На рис. 6.15 показана схема этого вентиля.

Обратите внимание, что $F(0,0,1)=(0,0,1)$ и $F(1,0,1)=(1,1,0)$, то есть для обоих возможных значений x

$$F(x,0,1)=(x,x,\neg x).$$

Как следствие — вентиль *Фредкина* можно использовать для моделирования разветвления и отрицания. Для случая с разветвлением $\neg x$ можно рассматривать как мусорный бит. Для случая с отрицанием мусорными можно считать оба бита x.

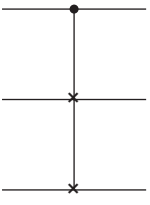


Рис. 6.15. Вентиль Фредкина

Если на вход z подать 0, мы получим:

$$F(0,0,0)=(0,0,0),\quad F(0,1,0)=(0,1,0),\quad F(1,0,0)=(1,0,0),\quad F(1,1,0)=(1,0,1).$$

Более компактно то же самое можно записать так:

$$F(x,y,0)=(x,\neg x\wedge y,x\wedge y).$$

То есть вентиль *Фредкина* можно использовать для конструирования вентиля *И* (0 — вспомогательный бит, а оба выхода, $\neg x\wedge y$ и $x\wedge y$, — мусорные биты).

Так как любую булеву цепь можно сконструировать, используя только вентили *НЕ* и *И* и разветвление, мы сможем сконструировать любую булеву цепь, используя только вентили *Фредкина*. Как и вентиль *Тоффоли*, вентиль *Фредкина* универсален.

Мы определили вентиль *Фредкина* как

$$F(0,y,z)=(0,y,z),\ F(1,y,z)=(1,z,y),$$

но можно дать другое, эквивалентное определение.

Этот вентиль выводит три числа. Первое число на выходе всегда равно числу x на первом входе. Второе число на выходе равно 1, если $x = 0$ и $y = 1$ или если $x = 1$ и $z = 1$, что можно выразить как $(\neg x \wedge y) \vee (x \wedge z)$. Третье число на выходе равно 1, если $x = 0$ и $z = 1$ или если $x = 1$ и $y = 1$, что можно выразить как $(\neg x \wedge z) \vee (x \wedge y)$. Следовательно, вентиль можно выразить так:

$$F(x,y,z) = (x,(\neg x \wedge y) \vee (x \wedge z),(\neg x \wedge z) \vee (x \wedge y)).$$

Это выражение выглядит намного сложнее и кажется более трудным для запоминания, чем словесное определение: «если $x = 0$, тогда оба входа, y и z, передаются на выходы без изменений; если $x = 1$, тогда y и z меняются местами». Однако есть одна ситуация, когда эта более сложная формула оказывается удобнее, но о ней мы поговорим в следующем разделе, где будем рассматривать конструирование этого вентиля с использованием бильярдных шаров.

Бильярдный компьютер

Мы пока не говорили о том, как фактически конструируются вентили. Их можно сконструировать с помощью выключателей и проводов с электрическим потенциалом или его отсутствием, представляющим биты 1 и 0 соответственно. Фредкин показал, что их также можно сконструировать с использованием бильярдных шаров, сталкивающихся друг с другом и с зеркалами, расположенными в важных местах. Зеркала — это просто твердые стенки, от которых отскакивают шары. (Мы назвали их зеркалами, потому что для них справедливо правило: «угол падения равен углу отражения».) Вентили на бильярдных шарах — это теоретические устройства; они предполагают, что все столкновения являются упругими, то есть происходят без потери энергии. Пример простого вентиля, который называется *переключателем*, показан на рис. 6.16. На этом рисунке сплошные линии представляют стенки; линии сетки нарисованы, чтобы помочь следить за перемещением центров шаров.

На рисунке слева шар только что вошел через Вход 1. Поскольку на Входе 2 шар отсутствует, он катится беспрепятственно и достигает Выхода 1.

На рисунке справа изображена аналогичная ситуация, когда шар входит через Вход 2 и беспрепятственно достигает Выхода 2A.

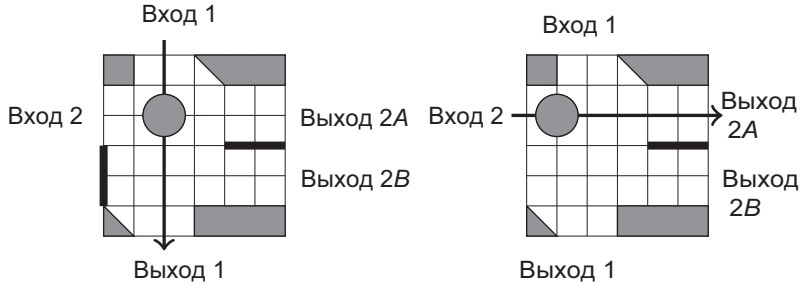


Рис. 6.16. Переключатель на бильярдных шарах

Возможны две другие ситуации посылки шаров через два входа. Неудивительно, что если не послать на входы ни одного шара, мы ничего не получим на выходе. Последний и самый сложный случай — когда через оба входа посылаются два шара. В данном случае предполагается, что шары имеют одинаковые массу, размеры, скорость и посылаются одновременно. На рис. 6.17 показано, что произойдет в этом случае.

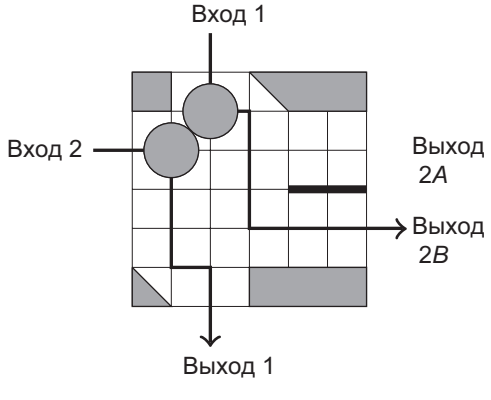


Рис. 6.17. Переключатель с двумя шарами на входе

Первый шар сталкивается со вторым, затем оба отскакивают от диагональных бортиков (или от зеркал), затем снова сталкиваются друг с другом. Наконец, они выкатываются через выходы: Один через Выход 1 и дру-

гой через Выход 2*B*. (Траектории центров шаров обозначены жирными стрелками.)

Присутствие и отсутствие шара можно обозначить соответственно 1 и 0 и представить полученный вентиль следующей таблицей.

Переключатель				
Вход		**Выход**		
1	**2**	**1**	**2A**	**2B**
0	0	0	0	0
0	1	0	1	0
1	0	1	0	0
1	1	1	0	1

Эту же таблицу можно получить, использовав утверждения $x, y, \neg x \wedge y$ и $x \wedge y$.

x	y	x	$\neg x \wedge y$	$x \wedge y$
0	0	0	0	0
0	1	0	1	0
1	0	1	0	0
1	1	1	0	1

Это позволяет нам изобразить переключатель в виде черного ящика со входами и выходами, подписанными, как показано на рис. 6.18.

Эта картинка сообщает нам, где шары входят в вентиль и где выходят. Если шар входит через x, он должен выйти через x. Если шар входит через y, он должен выйти через $\neg x \wedge y$, если на входе x отсутствовал второй шар, и через $x \wedge y$, если через вход x посылался второй шар. Вас может обеспокоить то обстоятельство, что когда на входы посылаются два шара, они меняются местами, потому что шар, выходящий через x, — это шар, который посылался через y, а шар, выходящий через $x \wedge y$, — это шар, который посылался через x. Но пусть вас это не беспокоит. Мы считаем

шары неразличимыми, и нас интересует только наличие или отсутствие шаров, но совершенно не интересует, откуда они появились и куда вышли.

Мы можем также послать шары в вентиль в обратном направлении, как показано на рис. 6.19. Но будьте осторожны, интерпретируя этот рисунок. Если послать только один шар через $\neg x \wedge y$, не посылая шар через x, он пройдет прямо. Если послать два шара через $x \wedge y$ и x, они столкнутся. В результате первый шар выйдет из вентиля вверх, а второй слева. Это означает, что на выходе слева шар появится, только если был послан шар через $\neg x \wedge y$ или $x \wedge y$, поэтому этот выход можно подписать как $(\neg x \wedge y) \vee (x \wedge y)$. Но выражение $(\neg x \wedge y) \vee (x \wedge y)$ логически эквивалентно y, а это означает, что при обращении вентиля просто меняются направления стрелок, а подписи остаются прежними.

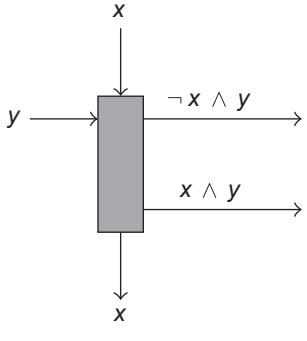


Рис. 6.18. Переключатель с подписанными входами и выходами

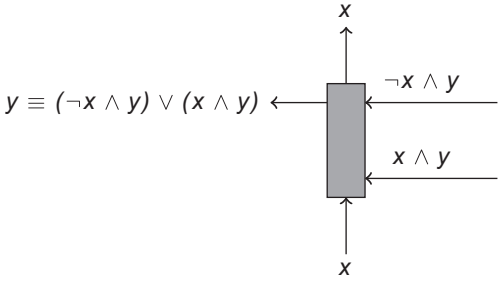


Рис. 6.19. Переключатель, в котором входы и выходы поменялись местами

Теперь можно сконструировать вентиль *Фредкина*. Напомню, что

$$F(x,y,z)=\big(x,(\neg x\wedge y)\vee(x\wedge z),(\neg x\wedge z)\vee(x\wedge y)\big).$$

Нам нужна конструкция со входами x, y и z и с выходами x, $(\neg x\wedge y)\vee(x\wedge z)$ и $(\neg x\wedge z)\vee(x\wedge y)$. Ее можно получить из четырех переключателей и значительной доли изобретательности. Она изображена на рис. 6.20.

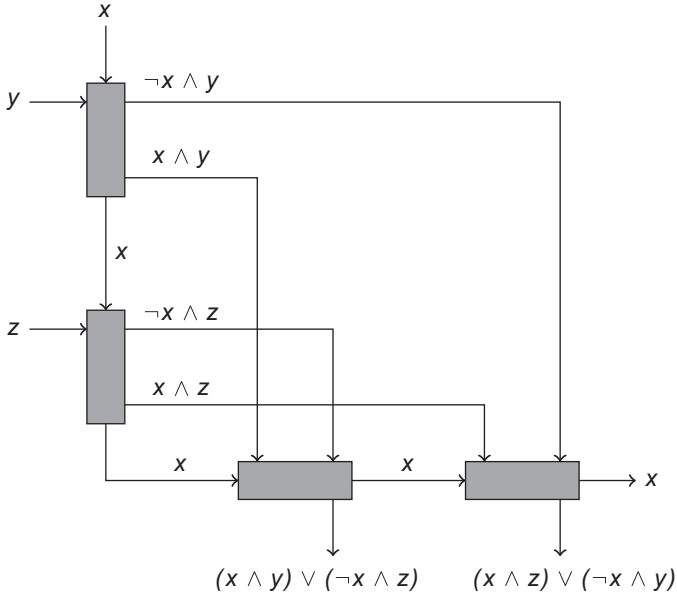


Рис. 6.20. Вентиль Фредкина, сконструированный из переключателей

Прямые углы в траекториях на этом рисунке получены в результате отскока от диагональных стенок. Это единственные другие взаимодействия, имеющие место в переключателях. Пересекающиеся траектории на рисунке не являются столкновениями шаров; шары проходят через точки пересечения в разное время. Чтобы обеспечить столкновение шаров только в определенных местах, мы всегда можем добавить задержки, формируя на их пути небольшие обходные траектории с использованием стенок. Например, добавить задержку можно, изменив прямую траекторию движения, как показано на рис. 6.21.

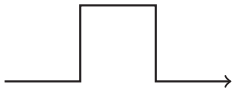


Рис. 6.21. Добавление задержки изменением траектории движения

Помещая отражающие стенки в нужных местах и добавляя задержки, вентиль можно сконструировать так, что выходы будут находиться на одной линии со входами и шары, посылаемые в вентиль одновременно, будут одновременно покидать его. (Это показано на рис. 6.22.) Теперь мы можем составлять схемы с несколькими вентилями *Фредкина*.[1] Благодаря их универсальности вентили *Фредкина* можно использовать для конструирования любых булевых цепей. Соответственно, любую булеву схему можно сконструировать с использованием только бильярдных шаров и отражающих стенок.

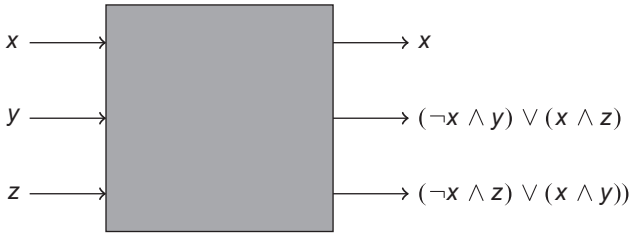


Рис. 6.22. Бильярдный вентиль Фредкина для использования в схемах

Эдвард Фредкин считает, что Вселенная — это компьютер. Ему не удалось в этом убедить Фейнмана, но компьютер на бильярдных шарах произвел на того большое впечатление. Оба поняли, что любая самая мелкая ошибка в местоположении или скорости шара будет усиливаться и распространяться дальше. В реальной жизни столкновения никогда не бывают идеально упругими; всегда имеется трение и потеря энергии с выделением тепла. Компьютер на бильярдных шарах — это исключительно теоретическая машина, его нельзя построить на практике. Но эта машина вызывает в воображении образы атомов, сталкивающихся друг с другом, что привело Фейнмана к идее вентилей, основанных не на классической, а на квантовой механике. Мы рассмотрим эту идею в следующей главе.

[1] Отличную наглядную демонстрацию этого вентиля с шарами можно найти на сайте: http://www.bubblycloud.com/billiard/fredkin-from-switches.html.

7 Квантовые вентили и цепи

Квантовые вентили и цепи являются естественным продолжением классических вентилей и цепей. Они также дают иное представление о математическом аппарате, описывающем отправку кубитов Алисой Бобу.

Я езжу на работу и обратно на поезде. Часто, когда мой поезд стоит на какой-то станции, рядом с ним оказывается другой поезд. Когда какой-то из поездов медленно начинает двигаться, наблюдая соседний поезд из окна, порой неясно, какой из поездов начал движение, и приходится поворачивать голову, чтобы посмотреть в окно с противоположной стороны вагона. Иногда оказывается, что движение начал мой поезд, иногда — соседний. То же верно в отношении измерений Боба. Можно считать, что Боб повернул свою измерительную установку или что положение установки Боба неизменно и совпадает с ориентацией установки Алисы, и этот кубит почему-то вращается, двигаясь от Алисы к Бобу. Когда Алиса и Боб находятся далеко друг от друга, часто предпочтительнее считать, что поворачивается измерительная установка Боба. Но далее мы будем посылать кубиты самим себе, и в этом случае предпочтительнее считать, что установка неподвижна и вращается сам кубит. Будем считать, что вращение имеет место, пока кубит преодолевает расстояние между местом его отправки и местом измерения. Это вращение задается отправкой кубита через вентиль. Выше мы говорили, что выбор направления измерения кубитов соответствует выбору ортогональной матрицы. Теперь мы будем считать направления измерений фиксированными, а ортогональную матрицу — соответствующей вентилю, через который проходят кубиты.

Прежде чем перейти к примерам, введем несколько новых названий, касающихся наших базисных кетов.

Кубиты

Итак, мы решили считать ориентацию измерительной установки неизменной, поэтому мы должны использовать единственный упорядоченный базис для отправки и приема кубитов. В этом случае естественно выбрать стандартный базис $\left(\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\right)$. Раньше мы обозначали его как $\left(|\uparrow\rangle, |\downarrow\rangle\right)$. Но кроме того, мы связали первый вектор в упорядоченном базисе с битом 0, а второй — с битом 1. Теперь, если мы решим использовать только этот базис, есть смысл дать нашим кетам новые имена, подчеркивающие их связь с битами. Пусть $|0\rangle$ будет обозначать $\begin{bmatrix}1\\0\end{bmatrix}$, а $|1\rangle$ будет обозначать $\begin{bmatrix}0\\1\end{bmatrix}$. В общем случае кубит будет иметь форму $a_0|0\rangle + a_1|1\rangle$, где $a_0^2 + a_1^2 = 1$. При измерении он будет переходить в состояние $|0\rangle$, и мы прочитаем 0, или в состояние $|1\rangle$, и мы прочитаем 1. Первое событие имеет вероятность a_0^2, а второе — вероятность a_1^2.

Обычно имеется система с несколькими кубитами, а это означает, что мы должны сформировать тензорные произведения. Для системы с двумя кубитами соответствующий упорядоченный базис имеет вид

$$\left(\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}\right).$$

Его можно записать как $\left(|0\rangle\otimes|0\rangle, |0\rangle\otimes|1\rangle, |1\rangle\otimes|0\rangle, |1\rangle\otimes|1\rangle\right)$. Как уже отмечалось ранее, символы, обозначающие тензорное умножение, обычно принято опускать, поэтому произведение можно записать еще компактнее: $\left(|0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle, |1\rangle|1\rangle\right)$. Наконец, договоримся обозначать $|a\rangle|b\rangle$ как $|ab\rangle$, соответственно тензорное произведение примет еще более компактный и простой для чтения вид: $\left(|00\rangle, |01\rangle, |10\rangle, |11\rangle\right)$.

Какое отношение все это имеет к вентилям? Мы ответим на этот вопрос далее. Начнем с вентиля *CNOT* (*управляемое НЕ*).

Управляемое НЕ

Как мы видели, классический вентиль *управляемое НЕ* (CNOT) имеет два входных бита и два выходных. Он определяется таблицей:

Управляемое НЕ			
Вход		**Выход**	
x	y	x	$x \oplus y$
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Преобразуем ее для случая с кубитами, заменив 0 на $|0\rangle$ и 1 на $|1\rangle$:

Управляемое НЕ			
Вход		**Выход**	
x	y	x	$x \oplus y$
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$

Эту таблицу можно переписать в более компактной форме, использовав тензорные произведения:

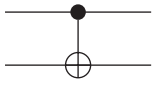
Управляемое НЕ	
Вход	**Выход**
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$
$\|11\rangle$	$\|10\rangle$

Таблица описывает происходящее с базисными векторами. Теперь расширим линейные комбинации базисных векторов.

$$CNOT\left(r|00\rangle + s|01\rangle + t|10\rangle + u|11\rangle\right) = r|00\rangle + s|01\rangle + u|10\rangle + t|11\rangle.$$

Здесь просто меняются местами амплитуды вероятностей для $|10\rangle$ и $|11\rangle$.

Мы продолжим использовать прежнюю диаграмму, изображающую вентиль *управляемое НЕ*, но будем осторожнее относиться к ее интерпретации. В классическом случае бит, попадающий в вентиль через верхний вход слева, покидает вентиль неизменным через верхний выход справа. Это также верно для кубитов, если верхний кубит имеет состояние $|0\rangle$ или $|1\rangle$, но неверно для других кубитов.



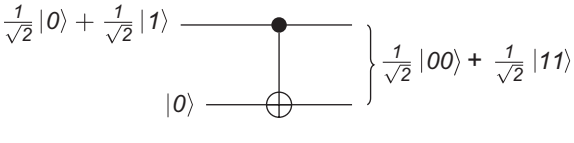
Например, пусть верхний кубит имеет состояние $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, а нижний — состояние $|0\rangle$.

То есть на входе мы получим состояние

$$\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \otimes |0\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle.$$

Оно будет преобразовано вентилем *управляемое НЕ* в $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$.

Это состояние, как мы узнаем из эксперимента *EPR*, является запутанным. Следовательно, мы не можем назначить отдельные состояния верхнему и нижнему выходам справа. Нарисуем такую диаграмму.



Провода здесь представляют наши электроны или фотоны. Это отдельные объекты, и они могут находиться далеко друг от друга. Мы часто будем

говорить о верхнем и нижнем кубитах, подразумевая, что они находятся далеко друг от друга. Но помните, что если они запутаны, то измерение одного будет влиять на измерение другого.

Этот пример иллюстрирует, насколько часто мы будем использовать этот вентиль. Мы можем ввести два незапутанных кубита и использовать вентиль, чтобы запутать их.

Квантовые вентили

Обратите внимание, что вентиль *управляемое НЕ* переставляет базисные векторы. Перестановка векторов в упорядоченном ортонормированном базисе дает другой упорядоченный ортонормированный базис, и мы знаем, что с любым из этих базисов связана ортогональная матрица. Следовательно, матрица, соответствующая вентилю *упорядоченное НЕ*, является ортогональной. Фактически все обратимые вентили, представленные в предыдущей главе, переставляют базисные векторы. Всем им соответствуют ортогональные матрицы, что дает нам определение квантовых вентилей. Они представляют операции, которые можно описать в терминах ортогональных матриц.

Так же как в случае с классическими вычислениями, нам нужно собрать небольшую коллекцию простых вентилей, которые можно соединить друг с другом, чтобы получить цепь. Для начала рассмотрим простейшие вентили, воздействующие на один кубит.

Квантовые вентили, воздействующие на один кубит

В классических обратимых вычислениях имеется только два булевых оператора, воздействующих на один бит: оператор тождественности, оставляющий бит неизменным, и оператор *НЕ* (*NOT*), инвертирующий значения 0 и 1. В случае с кубитами таких вентилей бесконечно много!

Сначала рассмотрим два квантовых вентиля, соответствующих классической тождественности и оставляющих кубиты $|0\rangle$ и $|1\rangle$ неизменными. Затем мы познакомимся с двумя квантовыми вентилями, инвертирующими кубиты $|0\rangle$ и $|1\rangle$. Эти четыре вентиля названы в честь Вольфганга Паули и называются *преобразованиями Паули*.

Вентили I и Z

Вентиль I — это единичная матрица $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Посмотрим, как I воздействует на произвольный кубит $a_0|0\rangle + a_1|1\rangle$.

$$I\left(a_0|0\rangle + a_1|1\rangle\right) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a_0 \\ a_1 \end{bmatrix} = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} = a_0|0\rangle + a_1|1\rangle.$$

Как и следовало ожидать, I действует как оператор тождественности и оставляет кубиты в неизменном состоянии.

Вентиль Z определяется матрицей $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

Посмотрим, как Z воздействует на произвольный кубит $a_0|0\rangle + a_1|1\rangle$.

$$Z\left(a_0|0\rangle + a_1|1\rangle\right) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} a_0 \\ a_1 \end{bmatrix} = \begin{bmatrix} a_0 \\ -a_1 \end{bmatrix} = a_0|0\rangle - a_1|1\rangle.$$

Вентиль Z оставляет амплитуду вероятности для $|0\rangle$ неизменной, но меняет знак амплитуды вероятности для $|1\rangle$. А теперь посмотрим на действие Z чуть внимательнее.

Сначала посмотрим, как он воздействует на базисные векторы. Мы имеем $Z\left(|0\rangle\right) = |0\rangle$ и $Z\left(|1\rangle\right) = -|1\rangle$. Но давайте вспомним, что вектор состояния эквивалентен вектору состояния, умноженному на -1, то есть $-|1\rangle$ эквивалентен вектору $|1\rangle$; иными словами Z сохраняет оба базисных вектора, но они не остаются тождественными. Если применить Z к кубиту

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle,$$

мы получим $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$, и, как было показано выше,

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

отличается от $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$, но эквивалентен ему.

Даже при том, что преобразование *Z* сохраняет оба базисных вектора, оно изменяет каждый второй кубит! Эту операцию изменения знака амплитуды вероятности иногда называют *изменением относительной фазы кубита*.

Вентили X и Y

Вентили *X* и *Y* задаются матрицами:[1]

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Y = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

Они обе соответствуют вентилю *HE* (NOT), инвертируя $|0\rangle$ и $|1\rangle$. Вентиль *X* выполняет простое инвертирование, а вентиль *Y* выполняет инвертирование и изменяет относительную фазу.

Вентиль Адамара

Последний из наиболее важных вентилей, воздействующих на единственный бит, — вентиль Адамара, *H*. Он определяется как

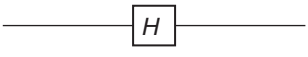
$$H = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

[1] Большинство авторов определяет матрицу *Y* как *–i*, умноженное на заданную матрицу. Мы решили не использовать комплексные числа. Наш выбор для *Y* избавит нас от лишних сложностей, когда мы будем рассматривать сверхплотное кодирование и квантовую телепортацию.

Этот вентиль часто используется, чтобы поместить базисные векторы в суперпозиции:

$$H\left(|0\rangle\right)=\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right) \qquad H\left(|1\rangle\right)=\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right).$$

На диаграммах вентили, воздействующие на один кубит, обозначаются квадратиком с соответствующей буквой в центре. Например, вентиль Адамара обозначается так:



Мы назвали пять вентилей, воздействующих на единственный кубит, но таких вентилей бесконечно много. Любой поворот даст нам ортогональную матрицу — их бесконечно много, и все они могут считаться вентилями.

Существуют ли универсальные квантовые вентили?

Знакомясь с классическими вычислениями, мы видели, что любую булеву функцию можно выразить в виде цепи, состоящей только из вентилей *Фредкина*, то есть вентиль *Фредкина* является универсальным. Мы также видели, что вентиль *И-НЕ* (NAND), вместе с разветвлением, тоже является универсальным. А существуют ли универсальные квантовые вентили?

В классическом случае существует конечное число булевых функций с данным числом переменных. Для одной переменной существуют только две булевы функции, для двух переменных — четыре. В общем случае для n переменных существует 2^n функций. Но ситуация с квантовыми вентилями в корне иная. Как мы уже видели, существует бесконечное множество вентилей, воздействующих на один кубит. Если взять конечное число вентилей и соединить их конечным числом способов, мы получим конечное число цепей. То есть невозможно из конечного числа вентилей получить бесконечное число цепей.

Таким образом, ответ на вопрос о существовании конечного числа квантовых вентилей, являющихся универсальными, — «нет». Однако даже

при том, что с помощью конечного числа вентилей невозможно получить все возможные квантовые цепи, исследователи показали, что существует конечное множество вентилей, которое можно использовать для аппроксимации всех возможных цепей, но мы не будем вдаваться в подробности доказательства. Все цепи, которые нам понадобятся, можно построить из вентилей, описанных выше: пяти, воздействующих на один кубит, и одного вентиля *управляемого HE*, воздействующего на два кубита.

Теорема о запрете клонирования

Впервые с операцией разветвления мы столкнулись, когда знакомились с классическими цепями. Один входной провод подключался к двум входам вентиля. Входной сигнал расщеплялся на две идентичные копии.

Затем мы рассмотрели обратимые вентили. Если обратимый вентиль имеет два выхода, он должен иметь два входа. Мы могли бы получить операцию ветвления с помощью вспомогательного бита — приняв второй вход всегда равным 0. Вот один из способов, как реализовать разветвление с помощью вентиля *управляемого HE*.

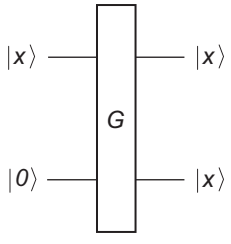
$CNOT(|0\rangle|0\rangle)=|0\rangle|0\rangle$, $CNOT(|1\rangle|0\rangle)=|1\rangle|1\rangle$, то есть $CNOT(|x\rangle|0\rangle)=|x\rangle|x\rangle$, если $|x\rangle$ — это $|0\rangle$ или $|1\rangle$. К сожалению, если $|x\rangle$ не является ни $|0\rangle$, ни $|1\rangle$, мы не получим две копии. Мы видели это, когда вводили

$$\left(\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle\right)|0\rangle$$

в вентиль *управляемого HE*. В результате мы получили два запутанных состояния, а не две копии исходного кубита. Мы можем использовать *управляемое HE* для копирования классических битов, но в общем случае этот вентиль не позволяет получить две копии кубита.

Понятие разветвления ограничивается классическими вычислениями. Аналогичное понятие в квантовых вычислениях называется *клонированием*. Клонирование подобно разветвлению, но только для кубитов. Нам нужна возможность создавать копии не только классических битов,

но также кубитов. Нам нужен вентиль, принимающий произвольный кубит $|x\rangle$ и второй фиксированный вход $|0\rangle$ (вспомогательный бит) и возвращающий две копии $|x\rangle$. Вот как выглядит диаграмма желаемого вентиля.



Вопрос клонирования превращается в вопрос возможности существования вентиля G. Мы покажем невозможность такого вентиля, доказав невозможность клонирования кубитов в принципе. Для этого предположим, что такой вентиль действительно существует, и покажем, что из этого предположения логически вытекают два противоречивых следствия. Поскольку доказательство логически обосновано и не должно иметь противоречий, мы приходим к выводу, что первоначальное предположение о существовании G ложно. Вот это доказательство.

Если G существует, тогда из свойства клонирования вытекает:

1. $G\big(|0\rangle|0\rangle\big)=|0\rangle|0\rangle$.
2. $G\big(|1\rangle|0\rangle\big)=|1\rangle|1\rangle$.
3. $G\left(\left(\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle\right)|0\rangle\right)=\left(\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle\right)$.

Переформулировав эти три утверждения, получаем:

1. $G\big(|00\rangle\big)=|00\rangle$.
2. $G\big(|00\rangle\big)=|11\rangle$.
3. $G\left(\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|10\rangle\right)=\frac{1}{2}\big(|00\rangle+|01\rangle+|10\rangle+|11\rangle\big)$.

Вентиль G, как и все матричные операторы, должен быть линейным, а это значит, что

$$G\left(\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|10\rangle\right)=\frac{1}{\sqrt{2}}G|00\rangle+\frac{1}{\sqrt{2}}G|10\rangle.$$

Заменив $G(|00\rangle)$ и $G(|10\rangle)$ утверждениями (1) и (2), получаем

$$G\left(\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|10\rangle\right)=\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|11\rangle.$$

Но утверждение (3) говорит, что

$$G\left(\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|10\rangle\right)=\frac{1}{2}|00\rangle+|01\rangle+|10\rangle+|11\rangle.$$

Однако

$$\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|11\rangle\neq\frac{1}{2}|00\rangle+|01\rangle+|10\rangle+|11\rangle.$$

Итак, мы показали, что если G существует, два неравных утверждения должны быть равны. Это противоречие. Единственный логический вывод — G не может существовать и невозможно сконструировать вентиль, клонирующий любые кубиты. В приведенном доказательстве использовался вспомогательный бит $|0\rangle$. В этом нет ничего особенного. Точно такое же доказательство можно привести для любого другого значения этого бита.

Невозможность клонирования кубита имеет множество важных следствий. Нам нужна возможность создавать резервные копии файлов и передавать их копии другим людям. Операция копирования вездесуща. Наши обычные компьютеры основаны на архитектуре фон Неймана, которая в значительной степени полагается на возможность копирования. Запуская программу, мы всегда копируем биты из одного места в другое. Проделать то же самое с кубитами в квантовых вычислениях невозможно. Поэтому программируемые квантовые компьютеры будут основаны на другой архитектуре.

На первый взгляд невозможность клонирования кубитов кажется серьезным недостатком, но есть пара важных замечаний, которые следует сделать.

Часто требуется предотвратить возможность копирования. Нам нужно защитить свои данные — никто из нас не хотел бы, чтобы его общение прослушивалось. В этом случае, как мы видели в примере с Евой, факт невозможности клонирования кубитов играет нам на руку, препятствуя созданию нежелательных копий.

Второе замечание настолько важно, что заслуживает отдельного рассмотрения.

Квантовые и классические вычисления

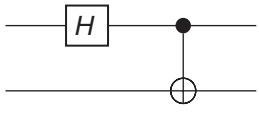
Кубиты $|0\rangle$ и $|1\rangle$ соответствуют битам 0 и 1. Если запустить наш квантовый вентиль *управляемое НЕ* только с использованием кубитов $|0\rangle$ и $|1\rangle$, а не каких-либо суперпозиций, вычисления будут выполнены точно так же, как в классическом вентиле *управляемое НЕ* с битами 0 и 1. То же верно в отношении квантовой версии вентиля *Фредкина*. Учитывая универсальность классического вентиля *Фредкина* и эквивалентность квантового вентиля *Фредкина* классическому, при использовании только кубитов $|0\rangle$ и $|1\rangle$ можно утверждать, что квантовая цепь будет давать тот же результат, что и классическая. Некоторое беспокойство может вызывать свойство, запрещающее клонирование, но оно никаким образом не препятствует выполнению классических вычислений.

Это важное наблюдение. Оно показывает, что, сравнивая классические и квантовые вычисления, не следует думать о них как о вычислениях разного типа. Квантовые вычисления являются надмножеством классических вычислений. Они представляют более общую форму вычислений. Кубит — вот базовая единица информации в вычислениях, а не бит.

Теперь, познакомившись с некоторыми основными вентилями, начнем соединять их и формировать цепи.

Цепь Белла

Следующая квантовая цепь называется цепью Белла.



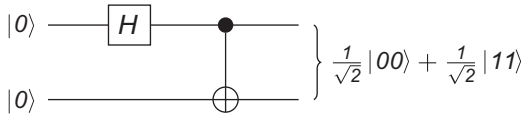
Чтобы понять, что она делает, подадим на ее входы четыре пары кубитов, образующих стандартный базис. Начнем с $|00\rangle = |0\rangle|0\rangle$. Первый кубит подвергается воздействию вентиля *Адамара*, который преобразует его в $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, то есть на этом этапе система из двух кубитов получает состояние

$$\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)|0\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle.$$

Далее следует вентиль *управляемое НЕ*. Он превратит $|10\rangle$ в $|11\rangle$, и мы получим окончательное состояние

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle.$$

Эту ситуацию можно представить, как показано на следующей диаграмме.



Обобщив, получаем

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

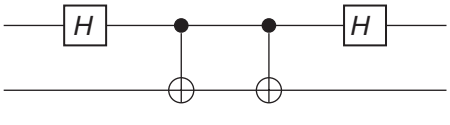
Остальные три пары проверьте сами и убедитесь, что

$$B(|01\rangle) = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle,$$
$$B(|10\rangle) = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle,$$
$$B(|11\rangle) = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle.$$

Все пары, получаемые в результате, запутаны. Поскольку входы образуют ортонормированный базис для $\mathbb{R}^4$, выходы тоже должны образовывать ортонормированный базис. Этот базис, состоящий из четырех запутанных кетов, называется базисом Белла.

Напомню, что проверить ортогональность квадратной матрицы A можно, вычислив A^TA, где A^T — транспонированная матрица, полученная взаимной заменой строк и столбцов в A. Если в результате получится единичная матрица I, значит, матрица A ортогональная и ее столбцы образуют ортонормированный базис. Если получится неединичная матрица, значит, матрица A не ортогональная. Мы определили наши вентили как ортогональные, поэтому все они обладают этим свойством. Фактически все вентили, представленные в этой главе, кроме матрицы Паули Y, обладают еще одним свойством — результат транспонирования является исходной матрицей.[1] Следовательно, для всех этих вентилей выполняется условие $AA = I$. То есть если применить вентиль два раза подряд, мы получим выход, не отличающийся от входа. Повторное применение вентиля отменяет первое применение.

Чуть ниже мы увидим пару примеров использования цепи Белла, но сначала исследуем свойство инверсии вентилей *Адамара* и *управляемого НЕ*. Рассмотрим следующую цепь:

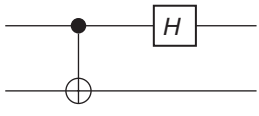


Если подать на вход цепи пару кубитов, сначала к ним применится вентиль *Адамара*, а затем вентиль *управляемого НЕ*. Затем последнее преоб-

[1] Матрицы, обладающие свойством $A^T = A$, называют *симметричными*. Осью симметрии в них служит главная диагональ.

разование будет немедленно отменено повторным применением вентиля *управляемого НЕ*. И наконец, повторное применение вентиля *Адамара* отменит применение первого вентиля *Адамара*. В конечном итоге эта цепь ничего не меняет. Кубиты на выходе идентичны кубитам на входе. Вторая половина цепи обращает все изменения, выполненные первой половиной.

Следующая цепь, которую мы назовем обратной цепью Белла, обращает действие цепи Белла.



Мы уже знаем, что если подать на вход векторы из базиса Белла, на выходе получатся векторы стандартного базиса.

Если ввести $\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|11\rangle$, на выходе получится $|00\rangle$.

Если ввести $\frac{1}{\sqrt{2}}|01\rangle+\frac{1}{\sqrt{2}}|10\rangle$, на выходе получится $|01\rangle$.

Если ввести $\frac{1}{\sqrt{2}}|00\rangle-\frac{1}{\sqrt{2}}|11\rangle$, на выходе получится $|10\rangle$.

Если ввести $\frac{1}{\sqrt{2}}|01\rangle-\frac{1}{\sqrt{2}}|10\rangle$, на выходе получится $|11\rangle$.

Теперь, после знакомства с основными свойствами цепи Белла, рассмотрим несколько интересных способов ее использования. Далее мы исследуем сверхплотное кодирование и квантовую телепортацию.

Сверхплотное кодирование

Исходные условия для сверхплотного кодирования и квантовой телепортации идентичны. Два электрона имеют спины в запутанном состоянии

$$\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|11\rangle.$$

Один из электронов передается Алисе, а другой Бобу. Затем они удаляются друг от друга подальше, стараясь не проводить никаких измерений своих электронов, чтобы сохранить их в запутанном состоянии.

В задаче сверхплотного кодирования Алиса хочет послать Бобу два классических бита информации, то есть одну из комбинаций: 00, 01, 10, 11. Сделать она это собирается, используя единственный кубит — свой электрон. Далее мы увидим полное описание процедуры, но сначала проанализируем задачу, чтобы понять, что нужно сделать.

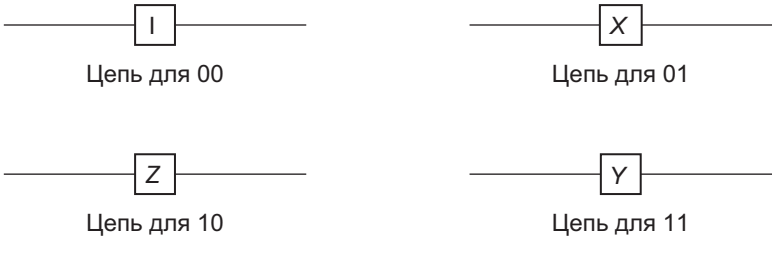
На первый взгляд кажется, что решение должно быть простым. Алиса собирается послать Бобу кубит $a_0|0\rangle + a_1|1\rangle$. Для кубита существует бесконечное множество вариантов, удовлетворяющих условию $a_0^2 + a_1^2 = 1$. Конечно, передача двух битов информации не должна вызывать сложностей — любой из четырех возможных комбинаций, — если есть возможность послать что-то, что может иметь бесчисленное количество вариантов. Проблема, однако, в том, что Боб может не знать, что представляет кубит. Он может получить информацию только путем измерения. Он измерит спин в стандартном базисе и получит $|0\rangle$ или $|1\rangle$. Если Алиса пошлет ему $a_0|0\rangle + a_1|1\rangle$, он получит $|0\rangle$ с вероятностью a_0^2 и $|1\rangle$ с вероятностью a_1^2. Получив $|0\rangle$, он ничего не будет знать о a_0, кроме того, что это ненулевое значение. Боб может получить из каждого кубита не больше одного бита информации. Чтобы получить два бита информации, он должен извлечь один бит из частицы, которую Алиса послала ему, и один бит из частицы, принадлежащей ему.

Первоначально Алиса и Боб имеют по одному электрону каждый. В конце концов Боб получит два электрона и измерит их спины. У Боба будет иметься некоторая квантовая цепь с двумя входами. Если Алиса захочет послать 00, нам нужно организовать все так, чтобы к моменту, когда Боб начнет измерение, верхний электрон находился в состоянии $|0\rangle$ и нижний электрон находился в состоянии $|0\rangle$, то есть чтобы непосредственно перед измерением пара электронов находилась в незапутанном состоянии $|00\rangle$. Аналогично, если Алиса захочет послать 01, нам нужно, чтобы перед измерением на стороне Боба пара электронов находилась в состоянии $|01\rangle$. Если Алиса захочет послать 10, конечное состояние должно быть $|10\rangle$, и $|11\rangle$, если Алиса решит послать 11.

И последнее наблюдение: с каждой парой электронов Боб должен проделывать одно и то же. Он не может использовать разные операции в зависимости от намерений Алисы, потому что ничего не знает о них. В этом весь смысл!

Идея заключается в том, чтобы Алиса воздействовала на свой электрон одним из четырех способов. В каждом случае состояние кубитов должно соответствовать одному из базисных векторов в базисе Белла. После этого Боб пропустит пару кубитов через обратную цепь Белла и получит правильное незапутанное состояние.

Алиса имеет четыре квантовых цепи, по одной для каждой из двухбитовых комбинаций. В каждой цепи используются вентили Паули. Эти цепи показаны ниже.



Посмотрим, что происходит с кубитами в каждом случае. Первоначально кубиты Алисы и Боба запутаны и находятся в состоянии

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle,$$

которое можно записать как

$$\frac{1}{\sqrt{2}}|0\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |1\rangle.$$

Когда Алиса посылает свой электрон через соответствующую цепь, ее кет изменяется. Обратите внимание, что цепи Алисы никак не воздействуют на электрон Боба. Выполним вычисления для каждого случая.

Если Алиса пожелает послать 00, она ничего не должна делать — кубиты останутся в состоянии

$$\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|11\rangle.$$

Если Алиса пожелает послать 01, она применит вентиль *X*, который превратит $|0\rangle$ в $|1\rangle$. Новое состояние примет вид

$$\frac{1}{\sqrt{2}}|1\rangle\otimes|0\rangle+\frac{1}{\sqrt{2}}|0\rangle\otimes|1\rangle,$$

которое можно записать как $\frac{1}{\sqrt{2}}|10\rangle+\frac{1}{\sqrt{2}}|01\rangle$.

Если Алиса пожелает послать 10, она применит вентиль *Z*, который оставит неизменным $|0\rangle$ и превратит $|1\rangle$ в $-|1\rangle$. Новое состояние примет вид

$$\frac{1}{\sqrt{2}}|0\rangle\otimes|0\rangle+\frac{1}{\sqrt{2}}\left(-|1\rangle\right)\otimes|1\rangle,$$

которое можно записать как $\frac{1}{\sqrt{2}}|00\rangle-\frac{1}{\sqrt{2}}|11\rangle$.

Если Алиса захочет послать 11, она применит вентиль *Y*, который вернет кубиты в незапутанном состоянии

$$\frac{1}{\sqrt{2}}|10\rangle-\frac{1}{\sqrt{2}}|01\rangle.$$

Обратите внимание, что каждое из конечных состояний в точности соответствует ее намерениям. Каждое является отдельным вектором базиса Белла. После этого она посылает Бобу свой электрон. Затем Боб сможет подать на вход обратной цепи Белла два кубита — свой, который имел прежде, и кубит Алисы.

Если Алиса пошлет 00, то после получения Бобом кубиты будут находиться в состоянии

$$\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|11\rangle.$$

Он подаст их на вход обратной цепи Белла и получит на выходе состояние $|00\rangle$. Это состояние незапутанное. Верхний и нижний биты будут иметь состояние $|0\rangle$. То есть он получит 00.

Если Алиса пошлет 01, то после получения Бобом кубиты будут находиться в состоянии

$$\frac{1}{\sqrt{2}}|10\rangle + \frac{1}{\sqrt{2}}|01\rangle .$$

Он подаст их на вход обратной цепи Белла и получит на выходе состояние $|01\rangle$. Это состояние незапутанное. Верхний бит будет иметь состояние $|0\rangle$, а нижний — состояние $|1\rangle$. То есть он получит 01. Другие комбинации получаются аналогично. В каждом случае Боб получает два бита, которые Алиса хотела послать.

Квантовая телепортация

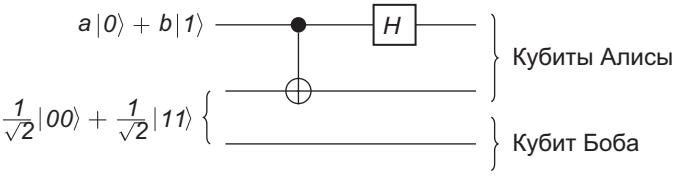
Как и в задаче сверхплотного кодирования, Алиса и Боб находятся далеко друг от друга. У каждого имеется один электрон. Электроны находятся в запутанном состоянии:

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle .$$

У Алисы имеется также еще один электрон. Он находится в состоянии $a|0\rangle + b|1\rangle$. Алиса ничего не знает об амплитудах вероятности a и b, но она и Боб хотят изменить электрон Боба так, чтобы тот получил состояние $a|0\rangle + b|1\rangle$. Они хотят телепортировать Бобу состояние электрона Алисы. Для этого, как мы увидим далее, Алиса должна послать Бобу два классических бита, но обратите внимание, что ее электрон может находиться в одном из бесчисленного множества начальных состояний. Самое необычное в этой задаче, что мы собираемся послать одно из бесчисленного множества состояний, используя всего два классических бита. Также интересно отметить, что Алиса начинает с кубита, а Боб заканчивает им, но ни один из них не знает точно его состояния. Чтобы узнать его, они должны выполнить измерение. Но выполняя измерение, они получают просто $|0\rangle$ или $|1\rangle$.

Мы можем сделать несколько выводов о том, как работает этот процесс. В итоге Боб должен получить электрон в незапутанном состоянии $a|0\rangle + b|1\rangle$. Первоначально электроны Боба и Алисы запутаны. Чтобы распутать их, кто-то должен выполнить измерение. Очевидно, что этим

кем-то должен быть не Боб. Если Боб выполнит измерение, он получит электрон в состоянии $|0\rangle$ или $|1\rangle$, а не в требуемом состоянии $a|0\rangle + b|1\rangle$, поэтому измерение должна выполнить Алиса. Также необходимо как-то задействовать состояние третьего электрона. Алиса должна что-то сделать, чтобы запутать состояние этого электрона с состоянием ее другого электрона, который первоначально запутан с электроном Боба. Самый простой способ сделать это — послать два кубита Алисы в вентиль *управляемого НЕ*. Это станет первым шагом. Вторым шагом станет применение вентиля *Адамара* к верхнему кубиту. Фактически Алиса должна подать два своих кубита на вход обратной цепи Белла. Эта ситуация изображена на следующем рисунке, где кубиты Алисы показаны выше кубита Боба. Вторая и третья линии изображают запутанные кубиты.



У нас имеется три кубита. Начальное состояние электронов описывается так:

$$\left(a|0\rangle + b|1\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right),$$

которое можно записать так:

$$\frac{a}{\sqrt{2}}|000\rangle + \frac{a}{\sqrt{2}}|011\rangle + \frac{b}{\sqrt{2}}|100\rangle + \frac{b}{\sqrt{2}}|111\rangle.$$

Алиса должна воздействовать на свои кубиты, поэтому запишем состояние, подчеркнув этот факт.

$$\frac{a}{\sqrt{2}}|00\rangle \otimes |0\rangle + \frac{a}{\sqrt{2}}|01\rangle \otimes |1\rangle + \frac{b}{\sqrt{2}}|10\rangle \otimes |0\rangle + \frac{b}{\sqrt{2}}|11\rangle \otimes |1\rangle.$$

Алиса должна использовать обратную цепь Белла. Проанализируем это действие, разбив его на два шага: сначала применим вентиль *управляемое НЕ* к двум кубитам, а потом применим вентиль *Адамара* к верхнему биту. Применение *управляемого НЕ* дает:

$$\frac{a}{\sqrt{2}}|00\rangle\otimes|0\rangle+\frac{a}{\sqrt{2}}|01\rangle\otimes|1\rangle+\frac{b}{\sqrt{2}}|11\rangle\otimes|0\rangle+\frac{b}{\sqrt{2}}|10\rangle\otimes|1\rangle.$$

Алиса должна воздействовать на первый кубит, поэтому запишем состояние, подчеркнув этот факт.

$$\frac{a}{\sqrt{2}}|0\rangle\otimes|0\rangle\otimes|0\rangle+\frac{a}{\sqrt{2}}|0\rangle\otimes|1\rangle\otimes|1\rangle+\frac{b}{\sqrt{2}}|1\rangle\otimes|1\rangle\otimes|0\rangle+\frac{b}{\sqrt{2}}|1\rangle\otimes|0\rangle\otimes|1\rangle.$$

Теперь применим вентиль *Адамара* к первому кубиту. Он заменит $|0\rangle$ на

$$\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle \text{ и } |1\rangle \text{ на } \frac{1}{\sqrt{2}}|0\rangle-\frac{1}{\sqrt{2}}|1\rangle.$$

В результате получаем состояние

$$\begin{aligned}&\frac{a}{2}|0\rangle\otimes|0\rangle\otimes|0\rangle+\frac{a}{2}|1\rangle\otimes|0\rangle\otimes|0\rangle+\frac{a}{2}|0\rangle\otimes|1\rangle\otimes|1\rangle+\\&+\frac{a}{2}|1\rangle\otimes|1\rangle\otimes|1\rangle+\frac{b}{2}|0\rangle\otimes|1\rangle\otimes|0\rangle-\frac{b}{2}|1\rangle\otimes|1\rangle\otimes|0\rangle+\\&+\frac{b}{2}|0\rangle\otimes|0\rangle\otimes|1\rangle-\frac{b}{2}|1\rangle\otimes|0\rangle\otimes|1\rangle.\end{aligned}$$

Это выражение можно упростить и получить

$$\begin{aligned}&\frac{1}{2}|00\rangle\otimes\big(a|0\rangle+b|1\rangle\big)+\frac{1}{2}|01\rangle\otimes\big(a|1\rangle+b|0\rangle\big)+\\&+\frac{1}{2}|10\rangle\otimes\big(a|0\rangle-b|1\rangle\big)+\frac{1}{2}|11\rangle\otimes\big(a|1\rangle-b|0\rangle\big).\end{aligned}$$

Теперь Алиса должна измерить два своих электрона в стандартном базисе. Она получит одно из состояний — $|00\rangle$, $|01\rangle$, $|10\rangle$ или $|11\rangle$, — причем каждое с вероятностью 1/4.

Если она получит $|00\rangle$, кубит Боба перейдет в состояние $a|0\rangle+b|1\rangle$.

Если она получит $|01\rangle$, кубит Боба перейдет в состояние $a|1\rangle+b|0\rangle$.

Если она получит $|10\rangle$, кубит Боба перейдет в состояние $a|0\rangle-b|1\rangle$.

Если она получит $|11\rangle$, кубит Боба перейдет в состояние $a|1\rangle-b|0\rangle$.

Алисе и Бобу нужно, чтобы кубит Боба оказался в состоянии $a|0\rangle + b|1\rangle$. Это уже почти достигнуто, но не совсем. Чтобы прийти к окончательному итогу, Алиса должна сообщить Бобу, в какой из четырех возможных ситуаций он находится. Для этого она должна послать Бобу два классических бита информации — 00, 01, 10 или 11, — соответствующих результатам ее измерений. Эти биты можно отправить в любом виде, например в виде текста.

Если Боб получит 00, он будет знать, что его кубит уже имеет нужное состояние и ничего делать с ним не требуется.

Если Боб получит 01, он будет знать, что его кубит имеет состояние $a|1\rangle + b|0\rangle$ и ему нужно применить вентиль *X*.

Если Боб получит 10, он будет знать, что его кубит имеет состояние $a|0\rangle - b|1\rangle$ и ему нужно применить вентиль *Z*.

Если Боб получит 11, он будет знать, что его кубит имеет состояние $a|1\rangle - b|0\rangle$ и ему нужно применить вентиль *Y*.

В каждом случае Боб получает кубит в состоянии $a|0\rangle + b|1\rangle$, то есть в состоянии исходного кубита, которое Алиса хотела телепортировать.

Важно отметить, что в любой точке процесса существует только один кубит в состоянии $a|0\rangle + b|1\rangle$. Первоначально это состояние имеет кубит Алисы. В конце его получает кубит Боба, но, как утверждает теорема о запрете клонирования, мы не можем создавать копии, поэтому в каждый конкретный момент времени только один из них может находиться в данном состоянии.

Интересно также отметить, что когда Алиса пересылает свои кубиты через свою цепь, кубит Боба мгновенно переходит в одно из четырех состояний. Но он вынужден ждать, пока Алиса пришлет ему два классических бита, прежде чем сможет определить, какое из четырех состояний соответствует состоянию оригинального кубита Алисы. Тот факт, что два бита придется передать каким-то традиционным способом, препятствует мгновенной передаче информации.

Квантовая телепортация и сверхплотное кодирование иногда описываются как операции, обратные друг другу. В случае со сверхплотным кодированием Алиса посылает Бобу один кубит, чтобы передать два классических

бита информации. В случае с квантовой телепортацией Алиса посылает Бобу два классических бита информации, чтобы телепортировать один кубит. В задаче сверхплотного кодирования Алиса выполняет кодирование, используя преобразования Паули, а Боб выполняет декодирование, используя обратную цепь Белла. В задаче квантовой телепортации Алиса выполняет кодирование, используя обратную цепь Белла, а Боб выполняет декодирование, используя преобразования Паули.

Квантовая телепортация обычно выполняется с использованием запутанных фотонов, а не электронов, потому что эта операция обычно выполняется на значительных расстояниях. Когда я писал эти строки, в прессе появилось сообщение, что китайским ученым удалось телепортировать кубит с Земли на спутник, вращающийся на низкой околоземной орбите. Эти эксперименты часто упоминаются в новостных передачах, в основном из-за слова «телепортация», которое вызывает в памяти сцены из фильма *Star Trek* («Звездный путь»). К сожалению, явление квантовой телепортации невозможно объяснить в короткой новости, и хотя многие слышали этот термин, мало кто понимает, что именно телепортируется.

Квантовая телепортация — это способ переноса кубита из одного места в другое без фактической транспортировки частицы, представляющей кубит. Она используется некоторыми способами для коррекции ошибок. Это чрезвычайно важно для квантовых вычислений. Кубиты имеют склонность взаимодействовать с окружающей средой и повреждаться. Мы не будем углубляться в изучение проблемы коррекции ошибок и рассмотрим только простой пример.

Коррекция ошибок

Я учился в университете еще до появления компакт-дисков. Мы слушали виниловые пластинки. Чтобы воспроизвести запись на пластинке, мы проделывали сложный ритуал. Сначала осторожно извлекали пластинку из конверта, стараясь держать ее за ребра, чтобы не оставить на поверхности жирных отпечатков. Затем укладывали ее на вращающийся диск проигрывателя. Потом протирали ее от пылинок. При этом часто использовали антистатический спрей и специальную кисточку. Наконец, мы осторожно опускали головку звукоснимателя на поверхность пластинки.

Но даже при соблюдении всех мер предосторожности часто слышались щелчки и шорох, вызванные присутствием невидимой пыли или какими-то другими дефектами. Случайно царапнув пластинку, вы потом слышали щелчки с частотой тридцать три раза в минуту, из-за чего прослушивание музыки делалось почти невозможным. Затем появились компакт-диски. Щелчки остались в прошлом. Вы могли даже поцарапать поверхность диска, и это не ухудшало качества звучания. Это казалось невероятным.

Проигрыватели виниловых пластинок не имели встроенного механизма коррекции ошибок. После повреждения пластинки прежнее звучание уже нельзя было восстановить. Компакт-диски, напротив, предусматривали коррекцию ошибок. При незначительных повреждениях диска программный код проигрывателя часто мог с успехом исправить ошибки.

Цифровое кодирование информации основано на двух важных идеях. Первая заключается в устранении избыточности и максимальном сжатии информации, чтобы сделать сообщение как можно короче. Хорошим примером может служить создание ZIP-архива файла документа. (Некоторым людям не нравятся компакт-диски, потому что они считают, что музыка на них сжимается слишком сильно и из-за этого теряется теплота звучания винила.) Вторая важная идея заключается в добавлении некоторой избыточности, но так, чтобы она была полезной. Эта избыточная информация помогает корректировать ошибки.

В настоящее время цифровая информация почти всегда передается с использованием некоторого механизма коррекции ошибок. Есть много способов немного повредить сообщение, но благодаря этому механизму такие сообщения, поврежденные нефатально, можно восстановить.

Коррекция ошибок совершенно необходима для надежной передачи кубитов. Для их кодирования мы используем фотоны и электроны. Эти частицы могут взаимодействовать с окружающей Вселенной, и эти нежелательные взаимодействия могут изменять состояние некоторых кубитов.

В этом разделе мы рассмотрим наиболее простой классический способ коррекции ошибок, а затем увидим, как применить его для отправки кубитов.

Повторение

Простая коррекция ошибок основана на простом повторении передаваемого символа. Самый простой вариант — повторить передачу трижды. Если Алиса хочет передать 0, она посылает 000. Если она хочет передать 1, она посылает 111. Получив последовательность из трех 0 или трех 1, Боб может считать, что все в порядке. Получив что-то иное, например 101, он будет знать, что возникла ошибка; последовательность должна быть 000 или 111. Если Алиса послала 000, значит, в переданной последовательности имеют место две ошибки. Если она послала 111, тогда только одна ошибка. Если ошибки маловероятны, значит, скорее всего, возникла одна ошибка, а не две, поэтому Боб может выбрать вариант, который соответствует меньшему числу ошибок, и заменить 101 на 111.

Принимая трехбитовую последовательность, Боб может получить один из восьми возможных вариантов. Четыре из них: 000, 001, 010 и 100. Любой из них Боб декодирует как 000. Другие четыре варианта трехбитовых последовательностей — 111, 110, 101 и 011 — Боб декодирует как 111. Если вероятность ошибок очень мала, такое повторение поможет исправить большую часть ошибок и уменьшит их общую частоту. Казалось бы, все довольно просто, но давайте обобщим действия Боба на случай получения кубитов. Проблема с кубитами заключается в том, что для приема их нужно измерить, а это может заставить их перейти в новое состояние. Нам нужен какой-то новый алгоритм действий Боба. Например, он мог бы выполнить проверку на четность.

Допустим, Боб получил три бита — $b_0 b_1 b_2$. Произведем некоторые вычисления, чтобы увидеть, какие биты следует изменить. Боб вычисляет $b_0 \oplus b_1$ и $b_0 \oplus b_2$.

Первая сумма проверяет четность первых двух битов, то есть она проверяет, являются ли они одной и той же цифрой. Вторая сумма проверяет четность первого и третьего битов.

Если все три бита равны 0 или 1, тогда он получит две суммы, равные 0. Если не все биты равны, тогда два из них будут равны друг другу, а третий будет отличаться. Этот третий бит нужно поменять на 0 или на 1.

Если $b_0 = b_1 \neq b_2$, тогда $b_0 \oplus b_1 = 0$ и $b_0 \oplus b_2 = 1$.

Если $b_0 = b_2 \neq b_1$, тогда $b_0 \oplus b_1 = 1$ и $b_0 \oplus b_2 = 0$.

Если $b_0 \neq b_1 = b_2$, тогда $b_0 \oplus b_1 = 1$ и $b_0 \oplus b_2 = 1$.

То есть Боб может рассматривать пары битов $b_0 \oplus b_1$ и $b_0 \oplus b_2$.

Если он получит 00, значит, ошибки отсутствуют и ему ничего делать не надо.

Если он получит 01, он должен инвертировать b_2.

Если он получит 10, он должен инвертировать b_1.

Если он получит 11, он должен инвертировать b_0.

Теперь посмотрим, как этот алгоритм коррекции ошибок приспособить для работы с кубитами. Но прежде отметим одно важное наблюдение. Это может показаться тривиальным, но именно эта идея обеспечивает работоспособность алгоритма коррекции ошибок с квантовым кульбитом (quantum bit-flip).

Допустим, Боб получил последовательность и выяснил, что ошибка кроется в первом бите. То есть он получил 011 или 100. Выполнив проверку на четность, он в обоих случаях получит 11 и будет знать, что ошибка в первом бите. А теперь обратите внимание на один важный момент: проверка четности сообщает, в каком бите кроется ошибка, но она не говорит, что это за бит: 0, который нужно заменить 1, или 1, которую нужно заменить на 0.

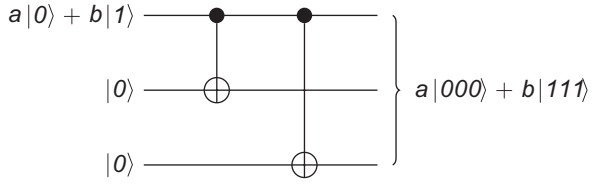
Коррекция с квантовым кульбитом

Алиса хочет передать Бобу кубит $a|0\rangle + b|1\rangle$. В процессе передачи могут возникнуть разные ошибки, но мы ограничимся простым переворотом битов. В данном случае $a|0\rangle + b|1\rangle$ изменится на $a|1\rangle + b|0\rangle$.

Алиса могла бы отправить три копии своего кубита, но это невозможно. Теорема запрета клонирования утверждает, что нельзя создать копию кубита. Но она может выполнить то, что, по сути, является аналогом клас-

сического разветвления, и заменить $|0\rangle$ на $|000\rangle$ и $|1\rangle$ на $|111\rangle$. Делается это с помощью двух вентилей *управляемого НЕ*. Соответствующая цепь показана ниже.

Первоначально у нее имеется три кубита: один из них тот, что требуется закодировать, и два вспомогательных бита, которые оба равны $|0\rangle$, то есть начальное состояние имеет вид: $(a|0\rangle + b|1\rangle)|0\rangle|0\rangle = a|0\rangle|0\rangle|0\rangle + b|1\rangle|0\rangle|0\rangle$. Первый вентиль *управляемого НЕ* изменит его на $a|0\rangle|0\rangle|0\rangle + b|1\rangle|1\rangle|0\rangle$. Второй даст нам желаемое состояние $a|0\rangle|0\rangle|0\rangle + b|1\rangle|1\rangle|1\rangle$.

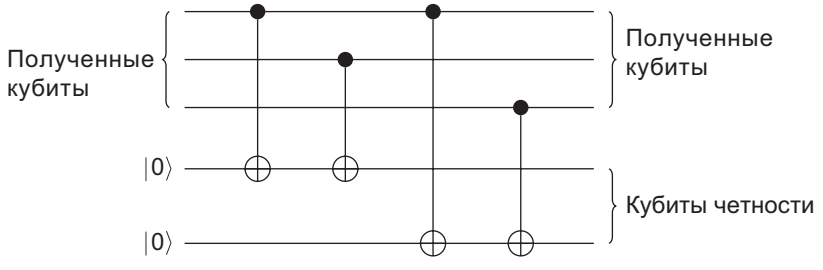


Затем Алиса посылает три кубита Бобу. Но из-за помех в канале есть вероятность, что какой-то кубит перевернется. Боб может получить правильные кубиты $a|000\rangle + b|111\rangle$ или одну из ошибочных версий: $a|100\rangle + b|011\rangle$, $a|010\rangle + b|101\rangle$ или $a|001\rangle + b|110\rangle$, если ошибка возникла в первом, втором или третьем кубите соответственно. Однако ему нужно не только обнаружить ошибку, но и исправить ее. Но обратите внимание, что он не может выполнять измерения в этом запутанном состоянии. Если он сделает это, состояние сразу же перестанет быть запутанным, и он просто получит три кубита, представляющих некоторую комбинацию из $|0\rangle$ и $|1\rangle$, — значения *a* и *b* будут потеряны без всякой возможности восстановить их.

Самое удивительное, что Боб может определить, какой бит перевернулся, и исправить его, не выполняя никаких измерений кубитов, посланных Алисой! Сделать это можно с использованием идеи проверки на четность, которую мы опробовали на классических битах.

Для этого он должен добавить два дополнительных кубита, с которыми будет выполняться проверка на четность. Соответствующая цепь показана ниже. В ней используется четыре вентиля *управляемого НЕ*. Два подключенных к четвертому входу вычисляют $b_0 \oplus b_1$; два подключенных

к пятому входу вычисляют $b_0 \oplus b_2$. Первая мысль, которая возникает при первом взгляде на эту схему, что в конечном результате мы получим пять безнадежно запутанных кубитов. Но на схеме я показал, что два нижних кубита не запутаны с тремя верхними кубитами. Возможно ли это на самом деле?



Допустим, что Боб получил $a|c_0c_1c_2\rangle + b|d_0d_1d_2\rangle$. Обратите внимание, что в случае ошибки она будет иметь место и в $c_0c_1c_2$, и в $d_0d_1d_2$, причем в одном и том же месте. Применив проверку четности к обеим последовательностям, мы получим один и тот же результат.

Для иллюстрации происходящего рассмотрим цепь на стороне Боба, игнорируя пока пятый вход. Итак, четыре первых кубита на входе имеют состояние

$$\left(a|c_0c_1c_2\rangle + b|d_0d_1d_2\rangle\right)|0\rangle = a|c_0c_1c_2\rangle|0\rangle + b|d_0d_1d_2\rangle|0\rangle.$$

Два вентиля *управляемого НЕ*, подключенные к четвертому входу, выполнят проверку четности двух первых цифр. Но $c_0 \oplus c_1 = d_0 \oplus d_1 = 0$, поэтому четыре кубита на выходе из цепи справа будут находиться в одном из двух состояний. Они окажутся в состоянии

$$a|c_0c_1c_2\rangle|0\rangle + b|d_0d_1d_2\rangle|0\rangle = \left(a|c_0c_1c_2\rangle + b|d_0d_1d_2\rangle\right)|0\rangle,$$

если $c_0 \oplus c_1 = d_0 \oplus d_1 = 0$, или в состоянии

$$a|c_0c_1c_2\rangle|1\rangle + b|d_0d_1d_2\rangle|1\rangle = \left(a|c_0c_1c_2\rangle + b|d_0d_1d_2\rangle\right)|1\rangle,$$

если $c_0 \oplus c_1 = d_0 \oplus d_1 = 1$.

В обоих случаях четвертый кубит не будет запутан с тремя верхними кубитами.

То же верно для пятого кубита. Он не будет спутан с другими и получит состояние $|0\rangle$, если $c_0 \oplus c_2 = d_0 \oplus d_2 = 0$, и состояние $|1\rangle$, если $c_0 \oplus c_1 = d_0 \oplus d_1 = 1$.

Поскольку два нижних кубита не спутаны с тремя верхними, Боб может измерить два нижних кубита и оставить три верхних в неприкосновенности. Вот что он должен сделать:

- Получив 00, он ничего не должен делать, потому что ошибки нет.
- Получив 01, он должен перевернуть третий кубит, подключив вентиль X к третьему выходу.
- Получив 10, он должен перевернуть второй кубит, подключив вентиль X ко второму выходу.
- Получив 11, он должен перевернуть первый кубит, подключив вентиль X к первому выходу.

В результате ошибка, вызванная квантовым кульбитом, будет исправлена, и после этого кубиты вернутся в состояние, в котором они были отправлены Алисой.

В этой главе мы познакомились с идеей квантовых вентилей и цепей. Мы увидели много удивительного, что можно сделать с несколькими квантовыми вентилями. Мы также увидели, что квантовые вычисления включают в себя все классические вычисления. Это не означает, что квантовые компьютеры будут использоваться для классических вычислений, а только подчеркивает, что квантовые вычисления являются более фундаментальной формой вычислений.

Следующая тема, которую мы рассмотрим, касается возможности использования квантовых цепей, чтобы получить более высокую скорость вычислений, чем это возможно с классическими цепями. Как измерить скорость вычислений? Всегда ли квантовые компьютеры обгоняют классические? Вот лишь несколько вопросов, на которые мы попробуем найти ответы в следующей главе.

8 Квантовые алгоритмы

В популярной литературе квантовые алгоритмы описываются как намного более быстрые, чем обычные. Высокая скорость объясняется возможностью поместить входы в суперпозицию всех возможных входов и затем выполнить алгоритм для суперпозиции. Как следствие, вместо одного входа, как в классических вычислениях, алгоритм можно применить сразу ко всем возможным входам, воспользовавшись так называемым квантовым параллелизмом. Подобные описания часто заканчиваются на этом, оставляя многие вопросы без ответов. Мы получаем множество возможных результатов, наложенных друг на друга. Если провести измерение, не получим ли мы один из них, выбранный случайно? Вероятность получить неправильный ответ намного выше, поэтому, скорее всего, мы получим неправильный ответ, разве не так?

Очевидно, что квантовые алгоритмы должны быть чем-то большим, чем помещение всего и вся в суперпозицию. Настоящее искусство конструирования таких алгоритмов заключается в умении манипулировать этими суперпозициями, чтобы при выполнении измерений можно было получить полезный ответ. В этой главе мы познакомимся с тремя квантовыми алгоритмами и посмотрим, как они решают эту проблему. Мы увидим, что не каждый алгоритм восприимчив к квантовому ускорению. Квантовые алгоритмы не являются ускоренными версиями классических алгоритмов. В них используются квантовые идеи, помогающие увидеть задачу в новом свете; алгоритмы добиваются высокой скорости не за счет грубой силы, а за счет оригинальных способов использования базовых шаблонов, которые можно увидеть только с квантовой точки зрения.

Мы внимательно рассмотрим три алгоритма. Все три являются результатом изобретательного использования базовых математических моделей. По мере продвижения от алгоритма к алгоритму уровень их сложности будет увеличиваться. В некоторых книгах по математике одной звездочкой отмечаются сложные и двумя звездочками — очень сложные разделы. Алгоритм Дойча—Джозы (Deutsch—Jozsa), вероятно, заслуживает одной звезды, а алгоритм Саймона (Simon) — двух звезд.

В конце главы мы немного поговорим о свойствах, которыми должны обладать задачи, чтобы квантовый алгоритм мог решать их быстрее, чем классический, и о том, почему такие задачи кажутся такими сложными! Но сначала мы должны определить, как измерить скорость алгоритмов.

Классы сложности P и NP

Представьте, что перед вами поставлены следующие задачи. При этом вам запрещено пользоваться калькулятором или компьютером и для их решения вы можете использовать только лист бумаги и карандаш.

- Найдите два целых числа больше 1, произведение которых равно 35.
- Найдите два целых числа больше 1, произведение которых равно 187.
- Найдите два целых числа больше 1, произведение которых равно 2407.
- Найдите два целых числа больше 1, произведение которых равно 88 631.

Вы без труда решите первую задачу, но для решения каждой последующей потребуется выполнить больше шагов и, соответственно, больше времени. Прежде чем углубиться в анализ, рассмотрим еще четыре задачи.

- Умножьте 7 на 5 и убедитесь, что результат равен 35.
- Умножьте 11 на 17 и убедитесь, что результат равен 187.
- Умножьте 29 на 83 и убедитесь, что результат равен 2407.
- Умножьте 337 на 263 и убедитесь, что результат равен 88 631.

Эти четыре задачи несомненно проще предыдущих. И снова для решения каждой последующей потребуется больше времени, чем для предыдущей,

но на этот раз затраты времени будут расти медленнее. Даже четвертую задачу можно решить вручную меньше чем за минуту.

Обозначим число цифр во входном числе как n, соответственно, в первом наборе задач мы начинаем с $n = 2$ и заканчиваем с $n = 5$.

Обозначим через $T(n)$ время или, что то же самое, число шагов, необходимое для решения задачи с входным числом длиной n. Сложность определяет, как растет $T(n)$ с увеличением n. В частности, нас интересует, можно ли найти положительные числа k и p, при которых будет выполняться условие $T(n) \leq kn^p$ для всех значений n. Если можно, мы говорим, что задача может быть решена за *полиномиальное время*. Если можно найти положительные числа k и $c > 1$, при которых будет выполняться условие $T(n) > kc^n$ для всех значений n, мы говорим, что задача может быть решена за *экспоненциальное время*. Вспомним основное свойство полиномиального и экспоненциального роста: при наличии достаточного количества времени величина с экспоненциальным ростом будет расти намного быстрее величины с полиномиальным ростом. Задачи, которые можно решить за полиномиальное время, в информатике считаются решаемыми, а задачи, которые можно решить за экспоненциальное время, — нерешаемыми. Задачи, решаемые за полиномиальное время, считаются простыми, а решаемые за экспоненциальное время — сложными. Как оказывается, для большинства практических задач, решаемых за полиномиальное время, это самое время описывается полиномом низкой степени, поэтому если в данный момент нет технической возможности решить задачу с большим значением n, такая возможность вполне может появиться через несколько лет. В случае с задачами с экспоненциальным временем решения, напротив, если n превысит значение, для которого задачу можно решить при текущем уровне развития техники, то даже небольшое увеличение n может сделать задачу нерешаемой в обозримом будущем.

Вернемся к нашим двум наборам задач. Задачи из второго набора требуют умножить два числа, но это простая операция. С увеличением n будет расти количество времени, необходимое для ее решения, но можно показать, что эти задачи относятся к категории задач с полиномиальным временем решения. А что можно сказать о задачах из первого набора? Если вы пытались их решить, вы легко поверите, что время, необходимое для их решения, растет в экспоненциальной прогрессии от n, но так ли

это на самом деле? Многие верят в это, но никто еще не привел строгих доказательств.

В 1991 году в RSA Laboratories объявили конкурс. Они перечислили большие числа, каждое из которых является произведением двух простых чисел, и предложили разложить их на множители. Предложенные числа насчитывали от 100 до 600 десятичных цифр. Разумеется, участникам конкурса разрешалось пользоваться компьютерами. Были назначены награды для тех, кто первыми найдут разложение. Числа из 100 цифр были разложены относительно быстро, но числа с 300 и более цифр еще никому не удалось разложить.

Если задача может быть решена за полиномиальное время, мы говорим, что она принадлежит к классу сложности *P*. То есть задача, требующая перемножения двух чисел, принадлежит к классу *P*. Предположим, что кто-то даст вам готовый ответ и вам останется только проверить его правильность. Если процесс проверки правильности ответа занимает полиномиальное время, тогда мы говорим, что задача относится к классу сложности *NP*.[1] Задача разложения больших чисел на простые сомножители относится к классу *NP*.

Очевидно, что проверить правильность ответа проще, чем найти его, поэтому каждая задача, принадлежащая к классу *P*, принадлежит также классу *NP*, но можно ли утверждать обратное? Принадлежит ли к классу *P* каждая задача из класса *NP*? Верно ли, что любую задачу, ответ на которую проверяется за полиномиальное время, можно решить за полиномиальное время? Вероятно, что сейчас вы сами себе сказали: «Конечно нет!» Большинство согласится, что это выглядит весьма маловероятным, но пока никому не удалось доказать, что *P* не равно *NP*. Задача разложения больших чисел на простые множители принадлежит к классу *NP*, и нам не кажется, что она может принадлежать к классу *P*, но пока никто не доказал этого.

Задача равенства *NP* и *P* считается одной из важнейших в информатике. В 2000 году в математическом институте имени Клэя составили список из семи призовых задач тысячелетия, за решение каждой из которых назначена премия в миллион долларов. Задача равенства *NP* и *P* входит в их число.

[1] *NP* — это аббревиатура от *Nondeterministic Polynomial* (недетерминированный полином), который, в свою очередь, имеет отношение к определенным типам машин Тьюринга, которые называют недетерминированными машинами Тьюринга.

Квантовые алгоритмы быстрее классических?

Большинство исследователей в области квантовых вычислений считают, что *P* не равно *NP*. Они также уверены, что есть задачи, принадлежащие к классу *NP*, но не принадлежащие к классу *P*, которые квантовый компьютер способен решить за полиномиальное время. Это означает, что есть задачи, которые квантовый компьютер способен решить за полиномиальное время, а классический компьютер — нет. Однако чтобы доказать это, сначала нужно показать, что некоторая задача принадлежит к классу *NP*, но не принадлежит к классу *P*, но как мы видели выше, никто не знает, как это сделать. Итак, как сравнить скорость квантовых и классических алгоритмов? Есть два пути: теоретический и практический. Теоретический путь заключается в определении нового способа измерения сложности, который облегчит построение доказательства. Практический путь заключается в создании квантового алгоритма, способного решать за полиномиальное время важные практические задачи, для которых не доказана их принадлежность к классу *P*.

Примером второго подхода может служить алгоритм Шора разложения числа на простые сомножители. Питер Шор построил квантовый алгоритм, который решает задачу за полиномиальное время. Мы считаем, хотя и не можем доказать этого, что классический алгоритм не способен решить эту задачу за полиномиальное время. Почему это важно? Дело в том, что, как будет показано далее, от этого зависит наша безопасность в интернете. Но как бы то ни было, в оставшейся части главы мы пойдем первым путем и определим новый способ вычисления сложности.

Запрос сложности

Все алгоритмы, которые мы рассмотрим в этой главе, касаются оценки функций. Алгоритмы Дойча и Дойча—Джозы рассматривают функции как принадлежащие двум классам. Нам дается случайная функция, и мы должны определить, к какому из двух классов она принадлежит. Алгоритм Саймона оценивает периодические функции специального типа. И снова нам дается случайная функция, и мы должны определить ее период.

Запуская эти алгоритмы, мы оцениваем функции. *Запрос сложности* определяет, сколько раз нужно проверить функцию, чтобы определить ее сложность. Иногда такую функцию называют *черным ящиком* или *оракулом*. Мы не говорим, что оцениваем функцию, мы говорим, что посылаем запрос черному ящику или оракулу. Нас не интересует вопрос, как написать алгоритм, имитирующий функцию, поэтому нам не нужно подсчитывать число шагов, которые функция выполняет для обработки входных данных. Мы просто подсчитываем число запросов. Это намного проще. Для иллюстрации начнем с самого простого примера.

Алгоритм Дойча

Дэвид Дойч — один из основателей квантовых вычислений. В 1985-м он опубликовал знаменательную статью, в которой описал квантовые машины Тьюринга и квантовые вычисления.[1] Эта статья также включает представленный ниже алгоритм — впервые показавший, что квантовые алгоритмы могут работать быстрее классических.

Задача касается функций единственной переменной. На вход может подаваться 0 или 1. На выходе также может быть только одно из значений, 0 или 1. Есть четыре такие функции, которые мы обозначим как f_0, f_1, f_2 и f_3:

Для обоих входных значений функция f_0 возвращает 0, то есть $f_0(0)=0$ и $f_0(1)=0$.

Функция f_1 для 0 возвращает 0 и для 1 — 1, то есть $f_1(0)=0$ и $f_1(1)=1$.

Функция f_2 для 0 возвращает 1 и для 1 — 0, то есть $f_2(0)=1$ и $f_2(1)=0$.

Функция f_3 для обоих входных значений возвращает 1, то есть $f_3(0)=1$ и $f_3(1)=1$.

Функции f_0 и f_3 называют *константными*. Для любых входных значений они всегда возвращают одно и то же значение — константу. Функция называется *сбалансированной*, если для половины входных значений она

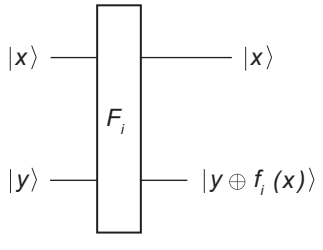
[1] «Quantum theory, the Church-Turing principle and the universal quantum computer», *Proceedings of the Royal Society* A 400 (1818): 97–117.

возвращает 0, а для другой половины — 1. Обе функции, f_1 и f_2, являются сбалансированными.

Дойч поставил перед собой следующий вопрос: выбирая случайную функцию из этих четырех, сколько раз нужно вычислить ее, чтобы определить, является она константной или сбалансированной? Важно понять суть вопроса. В данном случае нужно узнать не какая из четырех функций выбрана, а является ли она константной.

Порассуждаем с классической точки зрения. Мы можем вычислить функцию, передав ей 0 или 1. Предположим, что мы передали ей 0, тогда возможны два исхода — мы получим 0 или 1. Получив 0, мы можем утверждать лишь, что $f(0)=0$. Это может быть функция f_0 или f_1. Так как одна из них константная, а другая сбалансированная, мы вынуждены вычислить функцию еще раз, чтобы сделать выбор между ними. Итак, рассуждая с классической точки зрения, чтобы ответить на вопрос, нужно передать функции оба возможных значения, 0 и 1. То есть мы должны вычислить функцию дважды.

Теперь рассмотрим задачу с квантовой точки зрения. Сначала сконструируем вентили, соответствующие четырем функциям. На следующем рисунке изображена модель вентиля, где *i* может принимать значение 0, 1, 2 или 3.



Согласно этой модели:

Если на вход подать $|0\rangle\otimes|0\rangle$, она выведет $|0\rangle\otimes|f_i(0)\rangle$.

Если на вход подать $|0\rangle\otimes|1\rangle$, она выведет $|0\rangle\otimes|f_i(0)\oplus 1\rangle$.

Если на вход подать $|1\rangle\otimes|0\rangle$, она выведет $|1\rangle\otimes|f_i(1)\rangle$.

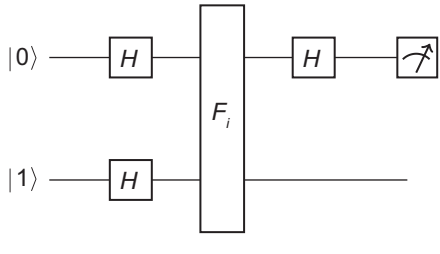
Если на вход подать $|1\rangle\otimes|1\rangle$, она выведет $|0\rangle\otimes|f_i(1)\oplus 1\rangle$.

Обратите внимание, что для каждого i одна из $f_i(0)$ и $f_i(0)\oplus 1$ равна 0, а другая равна 1, и одна из $f_i(1)$ и $f_i(1)\oplus 1$ тоже равна 0, а другая равна 1. Это означает, что четыре выхода всегда дают нам элементы стандартного базиса, то есть матрица, представляющая наш вентиль, ортогональна. Иначе говоря, наша модель действительно является вентилем.

Даже при том, что мы вводим два бита информации и получаем два бита на выходе, информация, которую дают эти вентили для классических битов, $|0\rangle$ и $|1\rangle$ точно такая же, как для функций, получающих 0 и 1. Верхний кубит — это то, что мы вводим, поэтому вывод не дает нам никакой новой информации. Выбирая $|0\rangle$ или $|1\rangle$ для второго входа, мы получаем второй выход, дающий нам тот же результат, что вернула функция для верхнего входного кета, или противоположный. Зная один, мы знаем второй.

Вопрос в квантовых вычислениях, соответствующий вопросу в классических вычислениях, формулируется так: выбирая случайный вентиль из этих четырех, сколько раз нужно использовать его, чтобы определить, является его базовая функция константной или сбалансированной?

Если ограничиться только вводом $|0\rangle$ и $|1\rangle$, мы придем к тому же ответу, что и прежде. Вентиль нужно использовать два раза. Но Дэвид Дойч показал, что если разрешить вводить кубиты, содержащие суперпозиции $|0\rangle$ и $|1\rangle$, достаточно воспользоваться вентилем только один раз. Чтобы доказать это, он использовал следующую цепь.



Маленький значок измерительного прибора на выходе справа вверху означает, что мы измеряем этот кубит. Отсутствие значка измерительного прибора на втором выходе говорит, что мы не собираемся измерять второй выходной кубит. Давайте посмотрим, как работает эта цепь.

Кубиты $|0\rangle \otimes |1\rangle$ — это вход. Они проходят через вентили *Адамара*, которые переводят их в состояние

$$\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) = \frac{1}{2}\left(|00\rangle - |01\rangle + |10\rangle - |11\rangle\right).$$

Затем они попадают на вход вентиля F_i и получают состояние

$$\frac{1}{2}\left(|0\rangle \otimes \left|f_i(0)\right\rangle - |0\rangle \otimes \left|f_i(0) \oplus 1\right\rangle + |1\rangle \otimes \left|f_i(1)\right\rangle - |1\rangle \otimes \left|f_i(1) \oplus 1\right\rangle\right).$$

Это выражение можно упростить:

$$\frac{1}{2}\left(|0\rangle \otimes \left(\left|f_i(0)\right\rangle - \left|f_i(0) \oplus 1\right\rangle\right) + |1\rangle \otimes \left(\left|f_i(1)\right\rangle - \left|f_i(1) \oplus 1\right\rangle\right)\right).$$

Теперь обратите внимание, что $\left|f_i(0)\right\rangle - \left|f_i(0) \oplus 1\right\rangle$ может быть либо $|0\rangle - |1\rangle$, либо $|1\rangle - |0\rangle$, в зависимости от того, что вернет $f_i(0)$ — 0 или 1. Но мы можем проявить немного изобретательности и записать

$$\left|f_i(0)\right\rangle - \left|f_i(0) \oplus 1\right\rangle = (-1)^{f_i(0)}\left(|0\rangle - |1\rangle\right).$$

Аналогично можно вывести, что

$$\left|f_i(1)\right\rangle - \left|f_i(1) \oplus 1\right\rangle = (-1)^{f_i(1)}\left(|0\rangle - |1\rangle\right).$$

Состояние кубитов после прохождения через вентиль F_i теперь можно записать так:

$$\frac{1}{2}\left(|0\rangle \otimes \left((-1)^{f_i(0)}\left(|0\rangle - |1\rangle\right)\right) + |1\rangle \otimes \left((-1)^{f_i(1)}\left(|0\rangle - |1\rangle\right)\right)\right).$$

Упростив, получаем

$$\frac{1}{2}\left((-1)^{f_i(0)}|0\rangle \otimes \left(\left(|0\rangle - |1\rangle\right)\right) + (-1)^{f_i(1)}|1\rangle \otimes \left(\left(|0\rangle - |1\rangle\right)\right)\right),$$

затем

$$\frac{1}{2}\left((-1)^{f_i(0)}|0\rangle + (-1)^{f_i(1)}|1\rangle\right) \otimes \left(|0\rangle - |1\rangle\right),$$

и, наконец,

$$\frac{1}{\sqrt{2}}\left((-1)^{f_i(0)}|0\rangle+(-1)^{f_i(1)}|1\rangle\right)\otimes\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right).$$

Это показывает, что два кубита не спутаны и верхний кубит имеет состояние

$$\frac{1}{\sqrt{2}}\left((-1)^{f_i(0)}|0\rangle+(-1)^{f_i(1)}|1\rangle\right).$$

Исследуем это состояние для каждой из четырех возможных f_i.

Для f_0 мы имеем $f_0(0)=f_0(1)=0$, то есть кубит имеет состояние $\left(1/\sqrt{2}\right)\left(|0\rangle+|1\rangle\right)$.

Для f_1 мы имеем $f_1(0)=0$ и $f_1(0)=1$, то есть кубит имеет состояние $\left(1/\sqrt{2}\right)\left(|0\rangle-|1\rangle\right)$.

Для f_2 мы имеем $f_2(0)=1$ и $f_2(0)=0$, то есть кубит имеет состояние $\left(-1/\sqrt{2}\right)\left(|0\rangle-|1\rangle\right)$.

Для f_3 мы имеем $f_3(0)=f_3(1)=1$, то есть кубит имеет состояние $\left(-1/\sqrt{2}\right)\left(|0\rangle+|1\rangle\right)$.

Следующий шаг в цепи — передача кубита в вентиль *Адамара*. Этот вентиль выводит $\left(1/\sqrt{2}\right)\left(|0\rangle+|1\rangle\right)$ для $|0\rangle$ и $\left(1/\sqrt{2}\right)\left(|0\rangle-|1\rangle\right)$ для $|1\rangle$. То есть мы знаем:

если $i=0$, кубит имеет состояние $|0\rangle$.

если $i=1$, кубит имеет состояние $|1\rangle$.

если $i=2$, кубит имеет состояние $-|1\rangle$.

если $i=3$, кубит имеет состояние $-|0\rangle$.

Если теперь измерить кубит в стандартном базисе, мы получим 0, если $i=0$ или $i=3$, и получим 1, если $i=1$ или $i=2$. Очевидно, что f_0 и f_3 — константные функции, а f_1 и f_2 — сбалансированные. Итак, если в результате измерения мы получим 0, мы будем точно знать, что функция константная. Если мы получим 1, мы будем точно знать, что функция сбалансированная.

Следовательно, мы можем задать оракулу только один вопрос, а не два. Таким образом, квантовый алгоритм решения задачи Дойча выполняется быстрее. Этот алгоритм не имеет практического применения, но, как отмечалось выше, он стал первым примером, доказывающим существование квантовых алгоритмов, выполняющихся быстрее классических.

Далее мы подробно рассмотрим два других квантовых алгоритма. Они оба предполагают ввод нескольких кубитов с последующей их передачей на вход вентиля *Адамара*. Введем дополнительный математический аппарат, чтобы описание нескольких кубитов в суперпозиции не стало слишком громоздким.

Кронекеровское произведение матриц Адамара

Мы знаем, что матрица для вентиля *Адамара* задается формулой

$$H = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Из этого определения вытекает, что

$$H\left(|0\rangle\right) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

и

$$H\left(|1\rangle\right) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \end{bmatrix} - \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$$

Предположим, что мы подаем на вход два кубита и оба передаем в вентили *Адамара*. В результате мы получим четыре базисных вектора:

Для $|0\rangle \otimes |0\rangle$ получим:

$$\left(\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle\right)\otimes\left(\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle\right)=\frac{1}{2}\left(|00\rangle+|01\rangle+|10\rangle+|11\rangle\right).$$

Для $|0\rangle\otimes|1\rangle$ получим:

$$\left(\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle\right)\otimes\left(\frac{1}{\sqrt{2}}|0\rangle-\frac{1}{\sqrt{2}}|1\rangle\right)=\frac{1}{2}\left(|00\rangle-|01\rangle+|10\rangle-|11\rangle\right).$$

Для $|1\rangle\otimes|0\rangle$ получим:

$$\left(\frac{1}{\sqrt{2}}|0\rangle-\frac{1}{\sqrt{2}}|1\rangle\right)\otimes\left(\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle\right)=\frac{1}{2}\left(|00\rangle+|01\rangle-|10\rangle-|11\rangle\right).$$

Для $|1\rangle\otimes|1\rangle$ получим:

$$\left(\frac{1}{\sqrt{2}}|0\rangle-\frac{1}{\sqrt{2}}|1\rangle\right)\otimes\left(\frac{1}{\sqrt{2}}|0\rangle-\frac{1}{\sqrt{2}}|1\rangle\right)=\frac{1}{2}\left(|00\rangle-|01\rangle-|10\rangle+|11\rangle\right).$$

Напомню, что все это можно переписать в терминах четырехмерных кетов. Предыдущие четыре утверждения эквивалентны следующим высказываниям:

$$\text{Для } \begin{bmatrix}1\\0\\0\\0\end{bmatrix} \text{ получим } \frac{1}{2}\begin{bmatrix}1\\1\\1\\1\end{bmatrix},$$

$$\text{Для } \begin{bmatrix}0\\1\\0\\0\end{bmatrix} \text{ получим } \frac{1}{2}\begin{bmatrix}1\\-1\\1\\-1\end{bmatrix},$$

$$\text{Для } \begin{bmatrix}0\\0\\1\\0\end{bmatrix} \text{ получим } \frac{1}{2}\begin{bmatrix}1\\1\\-1\\-1\end{bmatrix},$$

$$\text{Для } \begin{bmatrix}0\\0\\0\\1\end{bmatrix} \text{ получим } \frac{1}{2}\begin{bmatrix}1\\-1\\-1\\1\end{bmatrix}.$$

Это описание ортонормированного базиса, передаваемого другому ортонормированному базису. То есть мы можем записать матрицу, соответствующую этому преобразованию. Назовем эту новую матрицу $H^{\otimes 2}$.

$$H^{\otimes 2} = \frac{1}{2}\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{bmatrix}.$$

В этой матрице наблюдается базовый шаблон, включающий H.

$$H^{\otimes 2} = \frac{1}{2}\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}\begin{bmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\end{bmatrix} & \begin{bmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\end{bmatrix}\\ \begin{bmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\end{bmatrix} & -\begin{bmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\end{bmatrix}\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}H & H\\ H & -H\end{bmatrix}.$$

Этот шаблон можно распространить дальше. Матрицу, соответствующую трем кубитам на входе, передаваемым в вентили *Адамара*, можно записать с использованием $H^{\otimes 2}$.

$$H^{\otimes 3} = \frac{1}{\sqrt{2}}\begin{bmatrix}H^{\otimes 2} & H^{\otimes 2}\\ H^{\otimes 2} & -H^{\otimes 2}\end{bmatrix} = \frac{1}{2\sqrt{2}}\begin{bmatrix}\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{bmatrix} & \begin{bmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{bmatrix}\\ \begin{bmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{bmatrix} & \begin{bmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{bmatrix}\end{bmatrix} =$$

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

С увеличением n эти матрицы быстро растут в размерах, но всегда остается верным

$$H^{\otimes n} = \frac{1}{\sqrt{2}} \begin{bmatrix} H^{\otimes(n-1)} & H^{\otimes(n-1)} \\ H^{\otimes(n-1)} & -H^{\otimes(n-1)} \end{bmatrix},$$

что дает нам рекурсивную формулу, позволяющую быстро вычислять их. Эти матричные произведения, определяющие тензорные произведения, называются произведениями Кронекера (Kronecker), или кронекеровскими произведениями.

При изучении алгоритма Саймона нам потребуется исследовать некоторые детали этих матриц, но для объяснения следующего алгоритма достаточно заметить, что элементы в верхней строке каждой такой матрицы равны друг другу; для $H^{\otimes n}$ они равны $\left(1/\sqrt{2}\right)^n$.

Алгоритм Дойча—Джозы

Алгоритм Дойча рассматривал функции одной переменной. Мы случайно выбирали одну из них и должны были определить, является она константной или сбалансированной. Задача Дойча—Джозы является его обобщением.

Теперь у нас есть функции n переменных. Каждая из этих переменных, как и прежде, может иметь значение 0 или 1. На выходе также получается 0 или 1. Мы должны сказать, является ли функция константной: для всех комбинаций входов возвращает одно и то же значение 0 или 1 — или

сбалансированной: для половины комбинаций входов возвращает 0, а для другой половины — 1. Случайно выбирая одну из таких функций, сколько раз нужно ее вычислить, чтобы определить ее принадлежность к группе константных или сбалансированных функций?

Для примера рассмотрим случай, когда $n = 3$. Наша функция принимает три входные переменные, каждая из которых может иметь одно из двух значений. Это означает, что на входе мы имеем 2^3, или 8 возможных входных комбинаций:

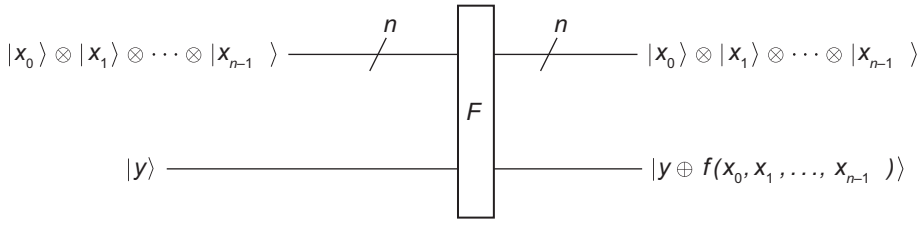
$$(0, 0, 0), (0, 0, 1), (0, 1, 0), (0, 1, 1), (1, 0, 0), (1, 0, 1), (1, 1, 0), (1, 1, 1).$$

Рассматривая задачу с классической точки зрения, предположим, что мы вычисляем $f(0, 0, 0)$ и получаем результат $f(0, 0, 0) = 1$. По этой неполной информации нельзя сделать какой-то вывод, поэтому мы снова вычисляем функцию для другой комбинации, например $f(0, 0, 1)$. Если мы получим $f(0, 0, 1) = 0$, вывод очевиден. Такая функция не может быть константной, значит, она сбалансированная. С другой стороны, если мы получим $f(0, 0, 1) = 1$, мы снова не сможем сказать ничего определенного по двум имеющимся результатам. Если события продолжат развиваться по худшему сценарию, мы могли бы получить один и тот же ответ на первые четыре комбинации и все еще не иметь возможности ответить на вопрос. Например, из того факта, что $f(0, 0, 0) = 1$, $f(0, 0, 1) = 1$, $f(0, 1, 0) = 1$, $f(0, 1, 1) = 1$, нельзя сделать вывод, что функция является константной или сбалансированной. Мы должны опробовать еще одну комбинацию. Если и в этом случае мы получим 1, тогда можно точно сказать, что функция является константной. Получив 0, мы будем точно знать, что функция сбалансированная.

Эти рассуждения легко распространить на общий случай. Для функции n переменных имеется 2^n возможные входные комбинации. Чтобы решить задачу, в лучшем случае достаточно задать оракулу два вопроса, но в худшем случае мы должны будем задать $2^{n-1} + 1$ вопрос. Так как $n - 1$ — это показатель степени, задача имеет экспоненциальную сложность. В худшем случае для ее решения потребуется задать оракулу число вопросов, растущее в экспоненциальной прогрессии. Алгоритм Дойча—Джозы — это квантовый алгоритм, требующий задать оракулу только один вопрос, поэтому ускорение может получиться весьма существенным!

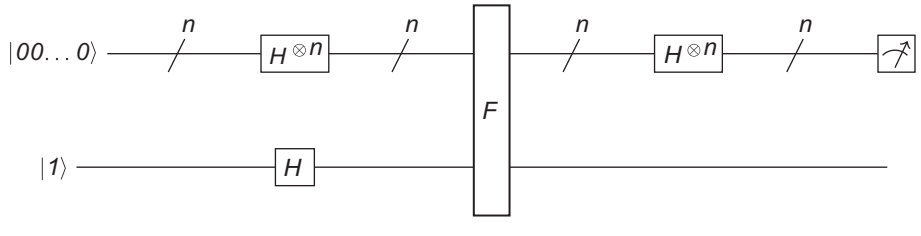
Первым делом опишем оракула. Для каждой функции мы должны построить отражающую ее ортогональную матрицу. Давайте просто обобщим наш предыдущий опыт.

Для любой функции $f(x_0, x_1, \ldots x_{n-1})$ n булевых переменных, имеющей единственный булев результат, мы сконструируем вентиль F, который определяется следующей цепью, где косые наклонные черты с индексом n сверху показывают, что мы имеем n параллельных входов/выходов.



Эта цепь сообщает нам, что происходит, когда каждый из кетов $|x_i\rangle$ представлен $|0\rangle$ или $|1\rangle$. На входе мы имеем $n + 1$ кетов, $|x_0\rangle \otimes |x_1\rangle \otimes \ldots \otimes |x_{n-1}\rangle$ и $|y\rangle$, где первые n кетов соответствуют входным переменным. На выходе также имеется $n + 1$ кетов, первые n из которых в точности совпадают со входными кетами. Последний выходной кет $|f(x_0, x_1, \ldots, x_{n-1})\rangle$, если $y = 0$, и кет с другим булевым значением, если $y = 1$.

Следующий шаг после описания, как работает функция «черного ящика», — создание квантовой цепи, включающей эту функцию. Это естественное обобщение цепи, использованной в алгоритме Дойча: все входные кубиты проходят через вентили *Адамара* по обе стороны от черного ящика.



Как и прежде, проанализируем работу этой цепи шаг за шагом. Чтобы уместить формулы в рамки книжной страницы, рассмотрим случай $n = 2$, но вообще все остальные случаи для любых n работают аналогично.

Шаг 1. Передача кубитов через вентили Адамара

Все верхние n входов равны $|0\rangle$. Для $n = 2$ мы имеем $|00\rangle$. Следующие вычисления иллюстрируют происходящее.

$$H^{\otimes 2}\left(|00\rangle\right) = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right).$$

В результате мы получаем суперпозицию всех возможных состояний; все базисные кеты имеют одинаковые амплитуды вероятности (в данном случае 1/2).

(Эти вычисления распространяются на любые значения n. После прохождения n кубитов через $H^{\otimes n}$ они оказываются в суперпозиции всех возможных состояний, каждое из которых имеет одну и ту же амплитуду вероятности: $\left(1/\sqrt{2}\right)^n$.)

Нижний вход — это просто $|1\rangle$. После прохождения кубита через вентиль *Адамара* он получает состояние $\left(1/\sqrt{2}\right)|0\rangle - \left(1/\sqrt{2}\right)|1\rangle$. На этом шаге наши три входных кубита получат следующее состояние.

$$\frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right).$$

Его можно записать как

$$\begin{aligned} &\frac{1}{2\sqrt{2}}|00\rangle \otimes \left(|0\rangle - |1\rangle\right) + \\ &+\frac{1}{2\sqrt{2}}|01\rangle \otimes \left(|0\rangle - |1\rangle\right) + \\ &+\frac{1}{2\sqrt{2}}|10\rangle \otimes \left(|0\rangle - |1\rangle\right) + \\ &+\frac{1}{2\sqrt{2}}|11\rangle \otimes \left(|0\rangle - |1\rangle\right). \end{aligned}$$

Шаг 2. Передача кубитов через вентиль F

После передачи через вентиль *F* кубиты перейдут в следующее состояние.

$$\frac{1}{2\sqrt{2}}|00\rangle\otimes\Big(\big|f(0,0)\big\rangle-\big|f(0,0)\oplus 1\big\rangle\Big)+$$
$$+\frac{1}{2\sqrt{2}}|01\rangle\otimes\Big(\big|f(0,1)\big\rangle-\big|f(0,1)\oplus 1\big\rangle\Big)+$$
$$+\frac{1}{2\sqrt{2}}|10\rangle\otimes\Big(\big|f(1,0)\big\rangle-\big|f(1,0)\oplus 1\big\rangle\Big)+$$
$$+\frac{1}{2\sqrt{2}}|11\rangle\otimes\Big(\big|f(1,1)\big\rangle-\big|f(1,1)\oplus 1\big\rangle\Big).$$

Далее, если *a* может иметь только значение 0 или 1, тогда выполняется равенство:

$$|a\rangle-|a\oplus 1\rangle=\big(-1^{a}\big)\big(|0\rangle-|1\rangle\big).$$

Воспользовавшись этим фактом, мы можем переписать состояние как

$$(-1)^{f(0,0)}\frac{1}{2}|00\rangle\otimes\frac{1}{\sqrt{2}}\big(|0\rangle-|1\rangle\big)+$$
$$+(-1)^{f(0,1)}\frac{1}{2}|01\rangle\otimes\frac{1}{\sqrt{2}}\big(|0\rangle-|1\rangle\big)+$$
$$+(-1)^{f(1,0)}\frac{1}{2}|10\rangle\otimes\frac{1}{\sqrt{2}}\big(|0\rangle-|1\rangle\big)+$$
$$+(-1)^{f(1,1)}\frac{1}{2}|11\rangle\otimes\frac{1}{\sqrt{2}}\big(|0\rangle-|1\rangle\big).$$

Как и прежде, это свидетельствует о том, что нижний кубит не запутан с верхними кубитами. Теперь просто рассмотрим два верхних кубита. Они находятся в состоянии

$$\frac{1}{2}\Big((-1)^{f(0,0)}|00\rangle+(-1)^{f(0,1)}|01\rangle+(-1)^{f(1,0)}|10\rangle+(-1)^{f(1,1)}|11\rangle\Big).$$

(Это доказательство верно для любого n. На данном шаге мы получили состояние, являющееся суперпозицией всех базисных кетов. Каждый кет $|x_0 x_1 \ldots x_{n-1}\rangle$ умножается на $\left(1/\sqrt{2}\right)^n (-1)^{f(x_0, x_1, \ldots, x_{n-1})}$.)

Шаг 3. Передача верхних кубитов через вентили Адамара

Стандартный способ заключается в преобразовании нашего состояния в вектор-столбец с последующим умножением на соответствующее кронекеровское произведение матрицы Адамара:

$$\frac{1}{4}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}\begin{bmatrix} (-1)^{f(0,0)} \\ (-1)^{f(0,1)} \\ (-1)^{f(1,0)} \\ (-1)^{f(1,1)} \end{bmatrix}.$$

Однако нам не требуется вычислять все элементы вектора-столбца результата. Достаточно вычислить только верхний элемент. Он получается умножением бра, соответствующего верхней строке матрицы на кет, заданный вектором-столбцом:

$$\frac{1}{4}\left((-1)^{f(0,0)} + (-1)^{f(0,1)} + (-1)^{f(1,0)} + (-1)^{f(1,1)}\right).$$

Это — амплитуда вероятности кета $|00\rangle$. Вычислим эту амплитуду для возможных функций.

Если f — константная и всегда возвращает 0, амплитуда вероятности равна 1.

Если f — константная и всегда возвращает 1, амплитуда вероятности равна –1.

Для сбалансированных функций амплитуда вероятности равна 0.

Шаг 4. Измерение верхних кубитов

Измерив верхние кубиты, мы получим одно из значений: 00, 01, 10 или 11. Встает вопрос: получим ли мы 00? Если функция константная, мы получим вероятность 1. Если функция сбалансированная, мы получим вероятность 0. То есть получив в результате измерения 00, можно утверждать, что функция была константной. В случае любого другого результата, отличного от 00, можно утверждать, что функция была сбалансированной.

Это доказательство верно для любого n. Непосредственно перед измерением кубитов амплитуда вероятности для $|0\ldots0\rangle$ равна

$$\frac{1}{2^n}\left((-1)^{f(0,0,\ldots,0)}+(-1)^{f(0,0,\ldots,1)}+\cdots+(-1)^{f(1,1,\ldots,1)}\right).$$

Как и для $n = 2$, в результате получится число ±1, если f — константная, и 0, если f — сбалансированная. Если все измерения дадут 0, функция константная. Если хотя бы одно измерение даст 1, функция сбалансированная.

Следовательно, решить задачу Дойча—Джозы для любого n можно за одно использование цепи. Нам потребуется задать оракулу только один вопрос. Напомню, что в классическом случае для решения той же задачи в худшем случае требовалось задать $2^{n-1} + 1$ вопроса, то есть ускорение получилось весьма существенным.

Алгоритм Саймона

Два алгоритма, описанные выше, необычны тем, что позволяют дать окончательный ответ уже после первого вопроса оракулу. Большинство квантовых алгоритмов использует смесь классических и квантовых алгоритмов; они предполагают более одного использования квантовой цепи и опираются на вероятности. Алгоритм Саймона включает все эти компоненты. Однако прежде, чем переходить к описанию алгоритма, мы должны обсудить стоящую перед нами задачу, но перед этим введем новый способ добавления двоичных последовательностей.

Поразрядное сложение последовательностей по модулю 2

Мы определили операцию $\oplus$ как *исключающее ИЛИ* (*XOR*), или, что то же самое, сложение по модулю 2. Напомню, что

$$0 \oplus 0 = 0 \quad 0 \oplus 1 = 1 \quad 1 \oplus 0 = 1 \quad 1 \oplus 1 = 0.$$

Распространим это определение на случай двоичных последовательностей одинаковой длины:

$$a_0 a_1 \cdots a_n \oplus b_0 b_1 \cdots b_n = c_0 c_1 \cdots c_n,$$

где

$$c_0 = a_0 \oplus b_0, c_1 = a_1 \oplus b_1, \ldots, c_n = a_n \oplus b_n.$$

Это напоминает сложение двоичных чисел, но без учета любых переносов. Вот конкретный пример поразрядного сложения:

$$\begin{array}{rr} & 1101 \\ \oplus & 0111 \\ \hline & 1010. \end{array}$$

Формулировка задачи Саймона

Имеется функция f, которая принимает двоичную последовательность длиной n и возвращает двоичную последовательность длиной n. Она содержит внутри неизвестную двоичную последовательность s такую, что равенство $f(x) = f(y)$ выполняется тогда и только тогда, когда $y = x$ или $y = x \oplus s$. Последовательность s не может состоять из одних 0; поэтому существуют пары входных последовательностей, отличающихся друг от друга, для которых генерируются одинаковые последовательности на выходе. Задача состоит в том, чтобы определить неизвестную последовательность s. Следующий пример поможет понять суть.

Пусть $n = 3$, то есть наша функция f принимает двоичные последовательности длиной 3 и возвращает двоичную последовательность длиной 3. Допустим, что неизвестная последовательность $s = 110$. Тогда

$$000 \oplus 110 = 110 \quad 001 \oplus 110 = 111 \quad 010 \oplus 110 = 100 \quad 011 \oplus 110 = 101$$
$$100 \oplus 110 = 010 \quad 101 \oplus 110 = 011 \quad 110 \oplus 110 = 000 \quad 111 \oplus 110 = 001.$$

То есть для этой последовательности s мы получаем следующие пары:

$$f(000) = f(110) \quad f(001) = f(111) \quad f(010) = f(100) \quad f(011) = f(101).$$

Для данной функции выполняются следующие равенства:

$$f(000) = f(110) = 101 \quad f(001) = f(111) = 010$$
$$f(010) = f(100) = 111 \quad f(011) = f(101) = 000.$$

Мы, конечно, не знаем ни того, как действует функция f, ни самой последовательности s: нам нужно найти s. Вопрос: сколько раз потребуется вычислить функцию, чтобы определить эту последовательность?

Будем продолжать вычислять функцию f и остановимся только тогда, когда повторно получим некоторый ответ. Обнаружив две входные последовательности, для которых функция дает одинаковый результат, мы сможем сразу же вычислить s.

Например, обнаружив, что $f(011) = f(101)$, мы сразу сможем определить, что

$$011 \oplus s_0 s_1 s_2 = 101.$$

Воспользовавшись тем фактом, что

$$011 \oplus 011 = 000,$$

поразрядно прибавим 011 к обеим сторонам уравнения и получим

$$s_0 s_1 s_2 = 011 \oplus 101 = 110.$$

Сколько раз потребуется вычислить функцию классическому алгоритму? У нас есть восемь разных входных последовательностей. В худшем случае мы можем вычислить функцию четыре раза и получить разные результаты, но на пятой попытке мы гарантированно получим совпадение. В общем случае для произвольного n существует 2^n разные двоичные последовательности, то есть в худшем случае потребуется вычислить функцию $2^{n-1}+1$ раз, а значит, в худшем случае потребуется задать оракулу $2^{n-1}+1$ вопроса.

Прежде чем перейти к квантовому алгоритму, рассмотрим немного подробнее кронекеровское произведение матриц Адамара.

Скалярное произведение и матрица Адамара

Для двух двоичных последовательностей $a = a_0 a_1 \cdots a_{n-1}$ и $b = b_0 b_1 \cdots b_{n-1}$ одинаковой длины *скалярное произведение* определяется как

$$a \cdot b = a_0 \times b_0 \oplus a_1 \times b_1 \oplus \cdots \oplus a_{n-1} \times b_{n-1},$$

где символ $\times$ обозначает обычное умножение.

Так, например, если $a = 101$ и $b = 111$, тогда $a \cdot b = 1 \oplus 0 \oplus 1 = 0$. Эту операцию можно рассматривать как сумму произведений соответствующих элементов последовательностей и определение четности результата.

В информатике принято вести счет с 0, поэтому будем вести счет не от 1 до 4, а от 0 до 3. Также часто используется двоичная форма записи. Числа 0, 1, 2 и 3 имеют двоичное представление 00, 01, 10 и 11 соответственно. Определим матрицу 4×4 и подпишем строки и столбцы этими числами, как показано ниже:

$$\begin{array}{c} \\ 00 \\ 01 \\ 10 \\ 11 \end{array} \begin{array}{c} \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\ \begin{bmatrix} * & * & * & * \\ * & * & * & * \\ * & * & * & * \\ * & * & * & * \end{bmatrix} \end{array}.$$

Местоположение любого элемента в этой матрице определяется перечислением меток его строки и столбца. Если определить каждый элемент матрицы в i-й строке и j-м столбце как $i \cdot j$, мы получим следующую матрицу.

$$\begin{array}{c} \\ 00 \\ 01 \\ 10 \\ 11 \end{array} \begin{array}{c} \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\ \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \end{array}.$$

Сравните эту матрицу с матрицей $H^{\oplus 2}$. Обратите внимание, что элементы, имеющие значение 1 в матрице скалярных произведений, находятся в тех же ячейках, что и отрицательные элементы в матрице $H^{\oplus 2}$. Учитывая, что $(-1)^0 = 1$ и $(-1)^1 = -1$, мы можем записать

$$H^{\otimes 2} = \frac{1}{2}\begin{bmatrix} (-1)^{00 \cdot 00} & (-1)^{00 \cdot 01} & (-1)^{00 \cdot 10} & (-1)^{00 \cdot 11} \\ (-1)^{01 \cdot 00} & (-1)^{01 \cdot 01} & (-1)^{01 \cdot 10} & (-1)^{00 \cdot 11} \\ (-1)^{10 \cdot 00} & (-1)^{10 \cdot 01} & (-1)^{10 \cdot 10} & (-1)^{10 \cdot 11} \\ (-1)^{11 \cdot 00} & (-1)^{11 \cdot 01} & (-1)^{11 \cdot 10} & (-1)^{11 \cdot 11} \end{bmatrix}.$$

Этот метод поиска положительных и отрицательных элементов универсален; например, чтобы получить элемент матрицы $H^{\otimes 3}$ в строке с номером 101 и в столбце с номером 111, достаточно вычислить скалярное произведение. В данном случае получится 0, а это значит, что соответствующий элемент положителен.

Матрицы Адамара и задача Саймона

Теперь, когда мы знаем, как найти элементы кронекеровское произведения матриц Адамара, мы воспользуемся этим знанием, чтобы увидеть, что получится при сложении двух столбцов одного из таких произведений. Мы сложим два столбца, образующих пару при данной неизвестной двоичной последовательности s, приведенной в задаче Саймона. Если один подписан последовательностью b, тогда другой будет подписан как $b \oplus s$. Мы должны сложить эти два столбца.

Для иллюстрации будем использовать последовательности длиной 2 и предположим, что секретная последовательность s равна 10. Сложим столбцы 00 и 10 или столбцы 01 и 11.

Вот матрица $H^{\otimes 2}$:

$$H^{\otimes 2} = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

Сложив столбцы 00 и 10, получаем:

$$\frac{1}{2}\begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \frac{1}{2}\begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 2 \\ 2 \\ 0 \\ 0 \end{bmatrix}.$$

Сложив столбцы 01 и 11, получаем:

$$\frac{1}{2}\begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix} + \frac{1}{2}\begin{bmatrix} 1 \\ -1 \\ -1 \\ 1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 2 \\ -2 \\ 0 \\ 0 \end{bmatrix}.$$

Обратите внимание, что некоторые амплитуды вероятности усиливаются, а некоторые обнуляются. Что же на самом деле здесь происходит?

Легко проверить, что произведения и поразрядные сложения подчиняются обычному экспоненциальному закону.

$$(-1)^{a\cdot(b\oplus s)} = (-1)^{a\cdot b}(-1)^{a\cdot s}.$$

То есть $(-1)^{a\cdot(b\oplus s)}$ и $(-1)^{a\cdot b}$ будут равны, если $a \cdot s = 0$, и $(-1)^{a\cdot(b\oplus s)}$ и $(-1)^{a\cdot b}$ будут иметь противоположные знаки, если $a \cdot s = 1$.

Мы можем обобщить это, как показано ниже:

$$(-1)^{a\cdot(b\oplus s)} + (-1)^{a\cdot b} = \pm 2,$$

если $a \cdot s = 0$,

$$(-1)^{a\cdot(b\oplus s)} + (-1)^{a\cdot b} = 0,$$

если $a \cdot s = 1$.

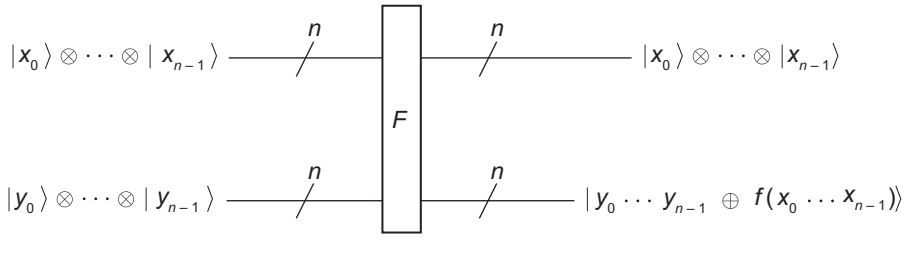
Отсюда следует, что при сложении двух столбцов с метками b и $b \oplus s$ элемент в строке будет равен 0, если $a \cdot s = 1$, и равен 2 или –2, если $a \cdot s = 0$. В общем случае обнуляются элементы строк с метками, скалярное произведение которых на s дает в результате 1.

Вернемся к нашему примеру. Причина, по которой два нижних элемента получились равными 0, заключается в том, что их строки имеют метки 10 и 11 и скалярное произведение обеих на секретную последовательность s равно 1. Ненулевые элементы находятся в строках с метками 00 и 01, скалярное произведение которых на секретную последовательность s равно 0.

Теперь у нас есть вся информация, необходимая для понимания квантовой цепи в задаче Саймона. Она должна дать нам последовательность, скалярное произведение которой на секретную последовательность s равно 0. Для этого она выполнит сложение двух столбцов из матрицы Адамара. Давайте посмотрим, как она работает.

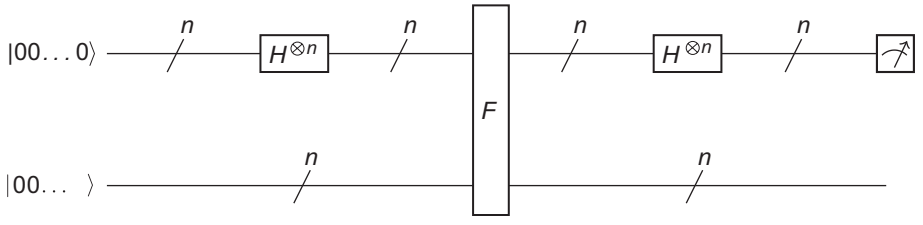
Квантовая цепь для задачи Саймона

Для начала сконструируем «черный ящик» — вентиль, действующий подобно функции f. Он показан на следующем рисунке.



Эту цепь можно рассматривать как принимающую две последовательности одинаковой длины, состоящие из 0 и 1. Верхняя последовательность остается неизменной. Нижняя выходная последовательность — это результат, вычисленный функцией для верхней последовательности, поразрядно суммированный с нижней последовательностью.

На следующем рисунке изображена цепь для данного алгоритма.



Проиллюстрируем происходящее на примере случая для $n = 2$. Все последующие рассуждения прямо обобщаются для любого значения n.

На первом шаге верхние кубиты передаются через вентили *Адамара*. Этот этап теперь должен быть вам понятен. Верхние два кубита первоначально находятся в состоянии $|00\rangle$, а после прохождения вентиля *Адамара* они перейдут в состояние

$$\frac{1}{2}\left(|00\rangle+|01\rangle+|10\rangle+|11\rangle\right).$$

Нижние два кубита останутся в состоянии $|00\rangle$. То есть после этого шага четыре кубита получат состояние

$$\frac{1}{2}\left(|00\rangle\otimes|00\rangle+|01\rangle\otimes|00\rangle+|10\rangle\otimes|00\rangle+|11\rangle\otimes|00\rangle\right).$$

Далее эти кубиты проходят через вентиль F. Он изменит их состояние на

$$\frac{1}{2}\left(|00\rangle\otimes|f(00)\rangle+|01\rangle\otimes|f(01)\rangle+|10\rangle\otimes|f(10)\rangle+|11\rangle\otimes|f(11)\rangle\right).$$

Далее верхние кубиты проходят через вентили *Адамара*, который изменяет их состояние на

$$\begin{aligned}
&\frac{1}{4}\left(|00\rangle+|01\rangle+|10\rangle+|11\rangle\right)\otimes|f(00)\rangle+\\
&+\frac{1}{4}\left(|00\rangle-|01\rangle+|10\rangle-|11\rangle\right)\otimes|f(01)\rangle+\\
&+\frac{1}{4}\left(|00\rangle+|01\rangle-|10\rangle-|11\rangle\right)\otimes|f(10)\rangle+\\
&+\frac{1}{4}\left(|00\rangle-|01\rangle-|10\rangle+|11\rangle\right)\otimes|f(11)\rangle.
\end{aligned}$$

Закономерность следования знаков + и – определяется матрицей $H^{\otimes 2}$. Теперь переупорядочим члены выражения, чтобы найти решение для двух первых кубитов, в результате получаем

$$\frac{1}{4}|00\rangle\otimes\left(|f(00)\rangle+|f(01)\rangle+|f(10)\rangle+|f(11)\rangle\right)+$$
$$+\frac{1}{4}|01\rangle\otimes\left(|f(00)\rangle-|f(01)\rangle+|f(10)\rangle-|f(11)\rangle\right)+$$
$$+\frac{1}{4}|10\rangle\otimes\left(|f(00)\rangle+|f(01)\rangle-|f(10)\rangle-|f(11)\rangle\right)+$$
$$+\frac{1}{4}|11\rangle\otimes\left(|f(00)\rangle-|f(01)\rangle-|f(10)\rangle+|f(11)\rangle\right).$$

Такой способ записи состояния обладает двумя замечательными свойствами. Во-первых, здесь также закономерность следования знаков + и – определяется матрицей $H^{\otimes 2}$. Во-вторых, пары кубитов слева от тензорного произведения соответствуют номерам строк.

Теперь используем уже известный нам факт, что $f(b)=f(b\oplus s)$, то есть $|f(b)\rangle=|f(b)\oplus s\rangle$. Мы можем упростить выражение, объединив члены и сложив их амплитуды вероятности. Это соответствует сложению со столбцом, которое мы только что рассмотрели. Для иллюстрации допустим, что s = 10, тогда $f(00)=f(10)$ и $f(01)=f(11)$. Подставив эти значения в состояние, мы получим

$$\frac{1}{4}|00\rangle\otimes\left(|f(00)\rangle+|f(01)\rangle+|f(00)\rangle+|f(01)\rangle\right)+$$
$$+\frac{1}{4}|01\rangle\otimes\left(|f(00)\rangle-|f(01)\rangle+|f(00)\rangle-|f(01)\rangle\right)+$$
$$+\frac{1}{4}|10\rangle\otimes\left(|f(00)\rangle+|f(01)\rangle-|f(00)\rangle-|f(01)\rangle\right)+$$
$$+\frac{1}{4}|11\rangle\otimes\left(|f(00)\rangle-|f(01)\rangle-|f(00)\rangle+|f(01)\rangle\right).$$

и после упрощения

$$\frac{1}{4}|00\rangle\otimes\left(2|f(00)\rangle+2|f(01)\rangle\right)+$$
$$+\frac{1}{4}|01\rangle\otimes\left(2|f(00)\rangle-2|f(01)\rangle\right)+$$

$$+\frac{1}{4}|10\rangle\otimes(0)+$$
$$+\frac{1}{4}|11\rangle\otimes(0).$$

Кеты слева от тензорных произведений отмечены номерами строк в матрице. Нули справа от тензорных произведений соответствуют строкам, скалярное произведение которых на s равно единице.

Мы можем упростить состояние до

$$\frac{1}{\sqrt{2}}|00\rangle\otimes\frac{1}{\sqrt{2}}\left(\left|f(00)\right\rangle+\left|f(01)\right\rangle\right)+\frac{1}{\sqrt{2}}|01\rangle\otimes\frac{1}{\sqrt{2}}\left(\left|f(00)\right\rangle-\left|f(01)\right\rangle\right).$$

Измерив два верхних кубита, мы получим 00 или 01, каждое с вероятностью 1/2.

Мы рассмотрели относительно простой случай с $n = 2$, но все вышесказанное верно для любого значения n. В конце процесса мы получаем одну из последовательностей, скалярное произведение которой на секретную последовательность s равно 0. Каждая из этих последовательностей одинаково вероятна.

Возможно, вас волнует, что после всего проделанного мы все еще не получили s. Это как раз тот момент, когда в игру вступает классическая часть алгоритма Саймона.

Классическая часть алгоритма Саймона

Начнем с примера с $n = 5$. Мы знаем, что существует некоторое секретное число $s = s_0s_1s_2s_3s_4$. Число 00000 недопустимо, поэтому остается $2 \wedge 5 - 1 = 31$ возможное значение s. Попробуем отыскать его, использовав квантовую цепь Саймона.

Допустим, мы использовали ее и получили ответ 10100. Мы знаем, что скалярное произведение этого результата на s дает 0. То есть

$$1\times s_0 \oplus 0\times s_1 \oplus 1\times s_2 \oplus 0\times s_3 \oplus 0\times s_4 = 0.$$

Отсюда следует, что $s_0 \oplus s_2 = 0$. Поскольку эти цифры могут быть только 0 или 1, делаем вывод, что $s_0 = s_2$.

Снова используем цепь, надеясь, что на этот раз мы не получим 10100 снова. (Вероятность этого события равна 1/16, поэтому мы в полной безопасности.) Также мы надеемся, что не получим число 00000, потому что в этом случае мы не получим никакой новой информации. Допустим, мы получили 00100. Теперь мы знаем, что

$$0 \times s_0 \oplus 0 \times s_1 \oplus 1 \times s_2 \oplus 0 \times s_3 \oplus 0 \times s_4 = 0.$$

Этот результат показывает, что s_2 должно быть равно 0. Из первого шага теперь можно сделать вывод, что s_0 также должно быть равно 0. Снова используем цепь и получаем 11110. Мы знаем, что

$$1 \times 0 \oplus 1 \times s_1 \oplus 1 \times 0 \oplus 1 \times s_3 \oplus 0 \times s_4 = 0,$$

а значит, $s_1 = s_3$. Снова используем цепь и получаем 00111, откуда следует, что

$$0 \times 0 \oplus 0 \times s_1 \oplus 1 \times 0 \oplus 1 \times s_3 \oplus 1 \times s_4 = 0.$$

Соответственно, должно выполняться равенство $s_3 = s_4$, и поскольку $s_1 = s_3$, мы получаем $s_1 = s_3 = s_4$.

Мы знаем, что все цифры не могут быть равны 0, поэтому должно выполняться равенство $s_1 = s_3 = s_4 = 1$, откуда следует, что число s должно быть 01011. В этом примере нам потребовалось задать оракулу четыре вопроса.

На данный момент вы можете задать еще пару вопросов. Первый касается алгоритма поиска s с использованием выходов квантовой цепи. Мы видели, что нужно делать в конкретном случае, но существует ли более общий алгоритм — пошаговая процедура, — который говорит, что делать в каждом возможном случае? Второй вопрос касается определения количества вопросов, которые нужно задать оракулу. Рассматривая классический алгоритм, мы взяли худший случай и определили, что после $2^{n-1} + 1$ вопроса мы получим точный ответ. Но в квантовом алгоритме худший случай намного хуже! Мы получаем случайный ответ. Ответ равен ска-

лярному произведению 0 на s, но мы можем получить один и тот же ответ несколько раз. Мы можем использовать нашу квантовую цепь $2^{n-1} + 1$ раз и каждый раз получать последовательность из 0. Это маловероятно, но возможно. Последовательность из 0 не дает никакой информации, поэтому вполне возможно, что, задав оракулу $2^{n-1} + 1$ вопроса, мы не придем ни к какому выводу ни об одной из цифр в секретном числе. Рассмотрим обе эти проблемы.

Каждый раз, используя цепь, мы получаем число, скалярное произведение которого на s равно нулю. Это дает нам линейное уравнение с n неизвестными. Использовав цепь несколько раз, мы получаем несколько — систему — таких уравнений. В предыдущем примере на каждом шаге мы получали новое уравнение, и каждое новое уравнение давало нам некоторую новую информацию. На техническом языке каждое такое новое уравнение называется *линейно независимым* от предыдущих уравнений. Чтобы вычислить s, нам необходима система из $n - 1$ линейно независимых уравнений.[1]

Алгоритмы решения систем уравнений хорошо известны. Они изучаются в курсах линейной алгебры и теории матриц и имеют широчайший круг применения. Они настолько востребованы, что их решение заложено в большинство научных калькуляторов. Мы не будем затрагивать их здесь, но упомянем, что число шагов, необходимых для решения системы из n уравнений, ограничивается сверху квадратичным выражением с n. Мы говорим, что система может быть решена за квадратичное время.

Другой вопрос, на который мы должны ответить: сколько раз придется использовать квантовую цепь? Как уже отмечалось, в худшем случае мы можем продолжать передавать наши кубиты через цепь снова и снова, но так и не получить никакой полезной информации. Однако такой исход крайне маловероятен. Мы исследуем этот вопрос в следующем разделе.

---

[1] Возможно, вы уже сталкивались с системами линейных уравнений и помните, что для решения системы с n неизвестными требуется n уравнений. Это верно, когда коэффициенты могут быть действительными числами, но в нашем случае коэффициенты могут принимать только значение 0 или 1. Это ограничение и тот факт, что секретная последовательность s не может состоять из одних нулей, позволяют нам уменьшить число необходимых уравнений на одно.

Классы сложности

В теории сложности основная граница проводится между задачами, которые можно решить за полиномиальное время, и задачами, требующими для решения больше времени. Алгоритмы с полиномиальным временем считаются практически осуществимыми даже для очень больших n, но алгоритмы с неполиномиальным временем считаются неосуществимыми для больших n.

Задачи, которые классические алгоритмы решают за полиномиальное время, обозначаются как *P*. Задачи, которые квантовые алгоритмы решают за полиномиальное время, обозначаются как *QP* (иногда их также обозначают как *EQP*, от *англ.* Exact Quantum Polynomial time — строго квантовое полиномиальное время). Обычно, используя эти термины, мы подразумеваем количество шагов, выполняемых алгоритмом, но, как вы помните, мы определили новый способ измерения сложности — запрос сложности, — который подсчитывает число вопросов, которое нужно задать оракулу. Мы увидели, что задача Дойча—Джозы не относится к классу *P*, но принадлежит к классу *QP* с точки зрения запроса сложности. (Константная функция является полиномом степени 0.) Иногда говорят, что задача Дойча—Джозы разделяет *P* и *QP*, — эта задача принадлежит к *QP*, но не принадлежит к *P* с точки зрения запроса сложности.

Однако давайте вспомним худший сценарий в классическом алгоритме. Для конкретики примем $n = 10$. Нам дана функция, принимающая 10 входных значений, и мы знаем, что она константная или сбалансированная. Мы должны продолжать вычислять функцию с разными входными значениями, пока не сможем вывести ответ. Всего возможно $2^{10} = 1024$ комбинации входных значений. В худшем случае, когда функция сбалансированная, мы получаем один и тот же результат в первых 512 попытках и только в 513-й попытке получаем другой результат. Но какова вероятность столкнуться с таким худшим случаем?

Если функция сбалансированная, то для каждой комбинации входных значений мы с равной вероятностью получим 0 или 1. Это можно сравнить с подбрасыванием идеальной монеты и выпадением орла или решки. Какова вероятность в 512 бросках подряд получить решку? Ответ: $(1/2)^{512}$.

Это меньше, чем разделить 1 на гугол, где гугол равен 10^{100}. Это ничтожно малое число!

Допустим, вам дали монету и попросили определить, является она правильной или имеет две одинаковые стороны. Подбросив монету один раз, вы не сможете ответить на этот вопрос. Но подбросив монету 10 раз и 10 раз получив один и тот же результат, вы будете совершенно уверены, что монета имеет две одинаковые стороны. Конечно, ошибка не исключена, но на практике мы готовы поступиться этим, если вероятность ошибки очень мала.

Именно так мы и поступаем, определяя классы сложности с ограниченной ошибкой. Мы выбираем некоторую граничную вероятность ошибки, которую считаем приемлемой. Затем мы рассматриваем алгоритмы, способные ответить на вопрос, оставаясь в пределах допустимой вероятности ошибки.

Теперь вернемся к задаче Дойча—Джозы и предположим, что нам необходима 99,9-процентная уверенность в успехе, что эквивалентно 0,1 % вероятности ошибки. Если функция сбалансированная, вероятность вычислить функцию 11 раз и во всех попытках получить 0 равна 0,00049, с точностью до пятого десятичного знака. Аналогично, вероятность получить 1 во всех 11 попытках тоже равна 0,00049. Следовательно, вероятность получения одного и того же ответа 11 раз подряд для четной функции составляет меньше 0,001. То есть если мы допускаем вероятность ошибки равной 0,1 %, мы можем ограничиться 11 вычислениями функции. Если в процессе испытаний появятся два результата, 0 и 1, мы сможем прервать серию и с полной уверенностью утверждать, что функция сбалансированная. Если все 11 испытаний дадут один и тот же результат, мы скажем, что функция константная. Мы можем ошибиться, но вероятность ошибки при этом будет ниже предела, выбранного нами. Обратите внимание, что этот аргумент действителен для любого числа n. В любом случае достаточно вычислить функцию 11 раз.

Задачи, которые классические алгоритмы способны решить за полиномиальное время с учетом некоторой граничной вероятности ошибки, обозначаются как *BPP* (от *англ.* Bounded-error Probabilistic Polynomial time — полиномиальное время с ограниченной вероятностью ошибки). Задача Дойча—Джозы относится к классу *BPP*.

У кого-то из вас может возникнуть вопрос: возможна ли ситуация, когда при одном значении вероятности ошибки задача относится к классу *BPP*, а при меньшем значении — нет? Нет, такая ситуация невозможна. Если задача относится к классу *BPP*, она останется в этом классе при выборе любого другого значения вероятности ошибки.

Теперь вернемся к алгоритму Саймона. Мы должны снова и снова посылать кубиты в цепь, пока не получим $n - 1$ линейно независимых уравнений. Как мы уже знаем, в худшем случае этот процесс может продолжаться вечно, поэтому алгоритм Саймона не относится к классу *QP*. Но давайте выберем некоторую допустимую вероятность ошибки. Тогда мы сможем определить N такое, что $(1/2)^N$ будет меньше этой вероятности.

Мы не будем доказывать это утверждение, но можем показать, что если использовать цепь $n + N$ раз, вероятность получить систему $n - 1$ линейно независимых уравнений в $n + N$ испытаниях будет больше $1 - (1/2)^N$.

Теперь мы можем сформулировать алгоритм Саймона. Сначала нужно выбрать допустимую вероятность ошибки и вычислить N. Напомню, что число N не зависит от n. Одно и то же значение N можно использовать во всех случаях. Затем нужно использовать цепь Саймона $n + N$ раз. Число испытаний, равное $n + N$, является линейной функцией от n, потому что N имеет фиксированное значение. Далее, предполагаем, что наша система из $n + N$ уравнений содержит $n - 1$ независимых векторов. Мы можем ошибиться, но вероятность ошибки меньше выбранного нами порога. После этого решаем систему $n + N$ уравнений, используя классический алгоритм. Время, необходимое на вычисления, будет иметь квадратичную зависимость от $n + N$, но так как N — константа, можно сказать, что время имеет квадратичную зависимость от n.

Алгоритм содержит квантовую часть с линейным временем выполнения и классическую часть с квадратичным временем, поэтому в целом он имеет квадратичное время выполнения. Задачи, которые квантовые алгоритмы способны решить за полиномиальное время с некоторой вероятностью ошибки, обозначаются как *BQP* (от *англ.* Bounded-error Quantum Polynomial time — квантовое полиномиальное время с ограниченной вероятностью ошибки). Алгоритм Саймона показывает, что задача относится к классу *BQP* с точки зрения запроса сложности.

Мы показали, что в худшем случае классический алгоритм требует вычислить функцию $2^{n-1} + 1$ раза — это экспоненциальная зависимость от n, а не полиномиальная, поэтому данная задача определенно не относится к классу *P*. Также можно показать, что даже если задать допустимую вероятность ошибки, алгоритм все равно останется экспоненциальным, то есть данная задача не принадлежит классу *BPP*. Мы говорим, что задача Саймона разделяет *BPP* и *BQP* с точки зрения запроса сложности.

Квантовые алгоритмы

В начале этой главы мы отметили, что во многих популярных публикациях скорость квантовых алгоритмов объясняется исключительно квантовым параллелизмом, то есть возможностью поместить входные данные в суперпозицию, включающую все базисные состояния. Но потом мы рассмотрели три алгоритма и увидели, что должны использовать не только квантовый параллелизм, но и кое-что еще. Давайте кратко рассмотрим, что еще нужно и почему это так сложно.

Три алгоритма, которые мы рассмотрели, являются наиболее простыми и считаются стандартными, но как вы возможно заметили, их никак нельзя назвать тривиальными. Даты их публикации отмечают важные вехи в истории. Дэвид Дойч опубликовал свой алгоритм в знаменательной статье в 1985 году. Это был первый квантовый алгоритм, показавший, что квантовые алгоритмы могут выполняться быстрее классических. Дойч и Джоза опубликовали обобщение алгоритма Дойча в 1992 году, семь лет спустя. Может показаться удивительным, что на поиск столь простого обобщения потребовалось так много времени, но не забывайте, что простым и естественным это обобщение выглядит только в свете современных знаний и представлений. В статье Дойча задача сформулирована не так, как здесь, и в ней отсутствуют диаграммы квантовых цепей, которые сейчас считаются стандартными. Тем не менее период с 1993 по 1995 год оказался более продуктивным, и за эти годы были открыты многие важные алгоритмы. В этот период был опубликован алгоритм Даниэля Саймона, а также алгоритмы Питера Шора и Лова Гровера, которые мы рассмотрим в следующей главе.

Ортогональные матрицы представляют квантовые вентили. Квантовые цепи состоят из комбинаций вентилей. Эти комбинации соответствуют

умножению ортогональных матриц, а так как произведение ортогональных матриц дает в результате ортогональную матрицу, любую квантовую цепь можно описать единственной ортогональной матрицей. Как мы уже видели, ортогональная матрица соответствует изменению базиса — другому способу представления задачи. Это — ключевая идея. Квантовые вычисления позволяют рассмотреть задачу с большего числа точек зрения, чем классические. Но чтобы они были эффективными, должно существовать представление, показывающее правильный ответ отдельно от других возможных и неправильных ответов. Задачи, которые квантовые компьютеры смогут решать быстрее, чем классические, должны иметь структуру, которая проявляется только при применении преобразования с использованием ортогональной матрицы.

Задачи, которые мы рассмотрели, явно получены методом обратной инженерии. Они не являются важными задачами, решение которых люди искали долгие годы и только теперь обнаружили, что если взглянуть на них с правильной точки зрения квантовых вычислений, они оказываются легко решаемыми. Эти задачи были специально сконструированы с использованием структуры кронекеровского произведения матриц Адамара. На самом деле гораздо интереснее не получить задачу методом обратной инженерии, а взять действительно важную задачу и сконструировать квантовый алгоритм, решающий ее быстрее, чем любой известный классический алгоритм. Именно это сделал Питер Шор в своей знаменательной статье, опубликованной в 1994 году, где он показал (кроме всего прочего), как можно использовать квантовые вычисления для взлома шифров, которые в настоящее время используются в интернете для защиты информации. Мы кратко обсудим алгоритм Шора в следующей главе, где рассмотрим влияние квантовых вычислений.

9 Влияние квантовых вычислений

Очевидно, что мы не можем предсказать влияние квантовых вычислений в долгосрочной перспективе с какой бы то ни было точностью. Если оглянуться назад в 1950-е годы, когда рождался современный компьютер, никто не мог предсказать, насколько компьютеры изменят общество и насколько зависимыми от них мы станем. Известны высказывания компьютерных пионеров, в которых они утверждали, что миру достаточно будет нескольких компьютеров и никому и никогда не понадобится иметь компьютер дома. Да, эти цитаты вырваны из контекста. Их авторы в большинстве случаев подразумевали конкретные типы компьютеров, но они производят верное впечатление, хотя и преувеличенное. Первые компьютеры были очень большими, они должны были размещаться в отдельных помещениях с кондиционерами и были не очень надежными. Сегодня у меня есть ноутбук, смартфон и планшет. Каждое из этих устройств мощнее первых компьютеров. Я думаю, что даже такие провидцы, как Алан Тьюринг, были бы поражены, насколько глубоко проникли компьютеры во все слои общества. Тьюринг действительно обсуждал игру в шахматы и искусственный интеллект, но никто не смог предсказать, что электронная коммерция и социальные сети займут доминирующие позиции в нашей жизни.

В настоящее время квантовые вычисления находятся в зачаточном состоянии, поэтому сравнение с первыми компьютерами кажется вполне подходящим. Машины, сконструированные к настоящему времени, обычно очень громоздкие и не слишком мощные, часто в их конструкции присутствуют сверхпроводники, требующие экстремально низких температур. Уже есть люди, которые говорят, что нет нужды строить много квантовых

компьютеров и что их влияние на общество будет минимальным. Но, как мне кажется, эти точки зрения крайне недальновидны. Да, мы не можем предсказать, каким будет мир через пятьдесят лет, но мы можем видеть, какие значительные изменения произошли в квантовых вычислениях за последние годы и в каком направлении они развиваются. Пройдет еще какое-то время, прежде чем мы получим мощные, универсальные квантовые компьютеры, но уже сейчас можно сказать, что квантовые вычисления окажут серьезное влияние на нашу жизнь. В этой главе мы посмотрим, что может получиться. В отличие от предыдущей главы, где довольно подробно рассматривались три алгоритма, в этой главе мы обсудим самые разные темы, но уже не так детально.

Алгоритм Шора и криптоанализ

Главным достижением квантовых вычислений в сфере криптоанализа является алгоритм Шора. Чтобы понять этот алгоритм, нужна серьезная математическая подготовка. Он использует теорему Эйлера и разложение в цепную дробь из теории чисел. Также необходимо знать комплексный анализ и дискретное преобразование Фурье. Это поворотная точка, где теория квантовых вычислений требует более обширных знаний, кроме элементарной математики. Поэтому я не буду подробно описывать алгоритм, но он играет настолько важную роль, что мы должны хотя бы взглянуть на него.

Этот алгоритм, как и алгоритм Саймона, состоит из двух частей — квантовой и классической. Квантовая часть аналогична квантовой части алгоритма Саймона. Но прежде чем дать краткое описание алгоритма Шора, я хочу сформулировать задачу, которую пытался решить Шор.

Алгоритм шифрования RSA

Алгоритм шифрования RSA назван в честь его изобретателей, Рона Ривеста (Ron Rivest), Ади Шамира (Adi Shamir) и Леонарда Адлемана (Leonard Adleman). Они опубликовали статью с описанием алгоритма, а затем запатентовали его в 1978 году. Позже стало известно, что Клиффорд Кокс (Clifford Cocks), работавший в управлении правительственной связи (Government Communications Headquarters, GCHQ) британских

спецслужб, изобрел такой же по сути алгоритм еще в 1973 году. Британцы засекретили его, но потом передали американцам. Но похоже, что ни американские, ни британские спецслужбы не использовали его и не понимали, какую важность он приобретет. В настоящее время он широко используется в интернете для шифрования данных, передаваемых между компьютерами. Он используется в интернет-банкинге и в электронной коммерции для выполнения операций с кредитными картами.

Мы покажем, как работает алгоритм шифрования на примере ситуации, когда нам нужно обменяться с банком некоторой конфиденциальной информацией и в то же время требуется защитить ее от постороннего взгляда.

Обмениваясь информацией с банком, желательно шифровать ее, чтобы никто не мог перехватить и прочитать ее. Фактическое шифрование данных производится с применением ключа, который вы и банк вместе используете для шифрования и расшифровывания. Такой ключ называется симметричным и должен храниться в секрете от третьих сторон. Ключ генерируется на вашем компьютере и пересылается в банк, но, конечно же, крайне нежелательно пересылать ключ в открытом, незашифрованном виде. Нам нужно зашифровать ключ, который потом будет использоваться для шифрования общения с банком. Именно здесь на сцену выходит алгоритм шифрования RSA. Он предлагает безопасный способ отправки ключа в банк.

Чтобы установить связь с банком, ваш компьютер генерирует ключ, который позднее будет использоваться для шифрования и расшифровывания сообщений и вами, и банком. Назовем этот ключ K.

Компьютер банка находит два больших простых числа, которые мы обозначим как p и q. Простые числа должны иметь примерно одинаковый размер и их произведение $N = pq$, которое называется модулем, должно содержать не меньше 300 стандартных десятичных цифр (1024 двоичные цифры). В настоящее время это число считается достаточно большим, чтобы обеспечить безопасность. Это довольно просто, потому что существуют эффективные способы поиска простых чисел, а перемножить два простых числа, чтобы получить модуль N, вообще не составляет труда.

Второй шаг для банка — найти относительно небольшое число e, не имеющее общих множителей с $p - 1$ или $q - 1$. Его тоже легко вычислить. Банк сохраняет простые числа p и q в тайне, но посылает числа N и e.

Ваш компьютер берет ключ K, возводит его в степень e и берет остаток от деления на N. И снова эти операции выполняются очень просто. Это число называется $K^e \bmod N$. Затем оно отправляется в банк. Банк знает, как разложить N на p и q, и это позволяет ему быстро вычислить K.

Если кто-то перехватит сообщения, он узнает числа N и e, отправленные банком, а также число $K^e \bmod N$, отправленное вами. Чтобы вычислить K, злоумышленник должен знать множители p и q числа N, но они хранятся банком в секрете. Безопасность основывается на отсутствии у злоумышленника простой возможности разложить число N на p и q.

Вопрос в том, насколько сложно разложить число, являющееся произведением двух больших простых чисел? На самом деле это очень сложно. Все остальные шаги, связанные с шифрованием RSA, выполняются с применением классических алгоритмов, имеющих полиномиальное время выполнения, но пока никто не изобрел классический алгоритм, способный разложить произведение двух больших простых чисел за полиномиальное время. Но с другой стороны, пока никто не доказал, что такого алгоритма в принципе не существует.

И здесь появляется Шор. Он сконструировал квантовый алгоритм, способный разложить произведение двух больших простых чисел. Алгоритм принадлежит к классу *BQP*, то есть он выполняется за полиномиальное время при ограничении вероятности ошибки. Здесь важно подчеркнуть, что мы больше не говорим о запросе сложности. Мы не предполагаем возможности задавать вопросы оракулу. Мы подсчитываем общее число шагов или, что то же самое, время, необходимое для выполнения всей цепочки вычислений. Шор дает конкретный алгоритм для каждого шага. Сам факт принадлежности алгоритма к классу *BQP* означает, что если он будет реализован, появится возможность раскладывать большие числа на простые множители, и, что особенно важно, если удастся сконструировать такую квантовую цепь, шифрование RSA перестанет быть безопасным.

Алгоритм Шора

Алгоритм Шора использует обширный математический аппарат. Далее мы рассмотрим только самое общее описание квантовой его части.

Важной частью алгоритма является вентиль, который называется *вентилем квантового преобразования Фурье*. Его можно рассматривать как обобщенный вариант вентиля *Адамара*. Фактически для одного кубита вентиль квантового преобразования Фурье в точности повторяет вентиль H. Вспомните рекурсивную формулу, которая описывала, как получить матрицу $H^{\otimes n}$ из матрицы $H^{\otimes n-1}$. Аналогично можно дать рекурсивную формулу для получения матрицы квантового преобразования Фурье. Основное отличие $H^{\otimes n}$ от матрицы квантового преобразования Фурье состоит в том, что в последнем случае элементы матрицы обычно являются комплексными числами — точнее, они являются комплексными корнями из 1. Как вы помните, элементы $H^{\otimes n}$ могут принимать значение 1 или -1. Они являются двумя возможными квадратными корнями из 1. Попытавшись отыскать корни четвертой степени из 1, мы снова получим ± 1, если использовать только действительные числа, но при использовании комплексных чисел мы получим два других корня. В общем случае 1 имеет n комплексных корней n-й степени. Матрица квантового преобразования Фурье для n кубитов включает все комплексные корни 2^n-й степени из 1.

Алгоритм Саймона основан на свойствах $H^{\otimes n}$. Он использовал эффект взаимовлияния (интерференции), амплитуды могли иметь только значения 1 и -1, в результате чего при сложении членов кеты усиливали или аннулировали друг друга. Шор подметил, что аналогичное явление применимо к матрице квантового преобразования Фурье, в этом случае амплитуды могут быть не только 1 и -1, но любыми комплексными корнями 2^n-й степени из 1. А это означает, что появляется возможность обнаруживать большее число типов периодов, кроме тех, что рассматривает алгоритм Саймона.

Итак, мы знаем число N и хотим разложить его на простые сомножители p и q. Алгоритм выбирает число a, удовлетворяющее условию $1 < a < N$. Затем проверяет, имеют ли a и N общие делители, и если имеют, то можно сделать вывод, что a является множителем числа p или q. Отсюда легко завершить разложение. Если a не имеет общих делителей с N, тогда вычисляется $a \bmod(N)$, $a^2 \bmod(N)$, $a^3 \bmod(N)$, и так далее, где $a^i \bmod(N)$ означает вычисление a^i и затем взятие остатка от деления на N. Поскольку эти числа являются остатками, они гарантированно будут меньше N. Следовательно, в какой-то момент последовательность чисел начнет повторяться. В ре-

зультате будет найдено такое число r, для которого выполняется равенство $a^r \bmod(N) = a \bmod(N)$. Число r можно рассматривать как период, и именно это число находит квантовая часть алгоритма Шора. Как только будет найдено число r, классические алгоритмы смогут использовать его для разложения числа N.

Это довольно схематичное описание, но оно позволяет получить некоторое представление о том, как работает квантовая часть алгоритма Шора. Ключевой является возможность обобщить алгоритм Саймона поиска секретной последовательности s для поиска неизвестного периода r.

Алгоритм действительно был реализован, но только для маленьких чисел. В 2001 году он использовался для разложения числа 15, а в 2012-м — для разложения числа 21. На сегодняшний день его нельзя использовать для разложения 300-значного числа. Но сколько времени потребуется, чтобы сконструировать цепь для разложения чисел такого размера? Похоже, что это лишь вопрос времени, когда алгоритм шифрования RSA станет небезопасным.

За прошедшие годы были разработаны другие методы шифрования, но алгоритм Шора способен справиться со многими из них. Очевидно, что пришло время придумывать новые методы шифрования, и эти новые методы должны обладать стойкостью не только к классическим атакам, но и к атакам со стороны квантовых компьютеров.

В настоящее время ведутся активные исследования в области постквантовой криптографии и изобретаются новые методы шифрования. Конечно, нет причин использовать квантовые вычисления в этих методах. Нам просто нужна возможность зашифровать сообщение так, чтобы его было трудно расшифровать с применением квантового компьютера. Но квантовые идеи помогают нам обнаруживать способы построения надежных шифров.

Мы видели две безопасные схемы квантового распределения ключа (Quantum Key Distribution, QKD): протоколы BB84 и Экерта. В некоторых лабораториях получилось успешно создать и запустить системы QKD. Есть также несколько компаний, предлагающих системы QKD для покупки. Один из первых случаев использования QKD в реальных условиях имел место в 2007 году, когда компания ID Quantique создала

систему для безопасной передачи результатов голосования между счетной станцией и центральной избирательной комиссией в Женеве во время парламентских выборов в Швейцарии.

Во многих странах ведутся эксперименты с небольшими квантовыми сетями, использующими оптоволоконные кабели. Существует теоретическая возможность соединить их через спутник и сформировать всемирную квантовую сеть. Эти работы представляют большой интерес для финансовых учреждений.

Наиболее впечатляющие результаты были достигнуты в квантовых экспериментах с китайским спутником. Он назван Micius в честь китайского философа, занимавшегося исследованиями в области оптики. Именно этот спутник использовался в эксперименте с квантовой телепортацией, упоминавшемся в главе 7. Он также был использован для квантового распределения ключа. Коллектив ученых из Китая установил связь с коллективом из Австрии — впервые было осуществлено межконтинентальное квантовое распределение ключа. После установки безопасного соединения ученые пересылали друг другу изображения. Китайские ученые переслали фотографию спутника Micius, а австрийские ученые — фотографию Шредингера.

Алгоритм Гровера и поиск данных

Мы вступаем в эпоху больших данных. Эффективный поиск в гигантских массивах данных в настоящее время является животрепещущей задачей для многих крупных компаний. Алгоритм Гровера теоретически способен ускорить поиск данных.

Свой алгоритм Лов Гровер изобрел в 1996 году. Подобно алгоритмам Дойча и Саймона, он имеет более высокую скорость выполнения, по сравнению с классическими алгоритмами с точки зрения запроса сложности. Однако мы не сможем реализовать действующий алгоритм поиска данных, не имея оракулов, которым могли бы задавать свои вопросы. Мы должны сконструировать алгоритм, выполняющий работу оракула. Но прежде чем начать говорить о реализации алгоритма Гровера, посмотрим, что он делает и как.

Алгоритм Гровера

Представьте, что перед вами четыре игральные карты. Они повернуты рубашками вверх. Вы знаете, что одна из них — туз червей и вам нужно найти ее. Сколько карт придется перевернуть, пока вы не узнаете, где лежит туз червей?

Если вам повезет, вы найдете искомую карту с первой же попытки, если не повезет, вы можете перевернуть три карты, и ни одна из них не будет тузом червей. В худшем случае, перевернув три карты, вы будете точно знать, что последняя карта — это искомый туз червей. Итак, мы можем узнать, где находится туз, перевернув от одной до трех карт. В среднем понадобится перевернуть 2,25 карты.

Это одна из задач, которые решает алгоритм Гровера. Перед началом описания алгоритма переформулируем задачу. У нас есть четыре двоичные последовательности: 00, 01, 10 и 11. У нас есть функция f, которая возвращает 0 для трех из этих последовательностей и 1 — для четвертой последовательности. Нам нужно найти двоичную последовательность, соответствующую выходному значению 1. Например, мы можем получить такие результаты: $f(00) = 0$, $f(01) = 0$, $f(10) = 1$ и $f(11) = 0$. Теперь задача состоит в том, чтобы выяснить, сколько раз следует вычислить функцию, чтобы получить результат $f(10) = 1$. Здесь мы просто переформулировали задачу, заменив игральные карты функциями, поэтому ответ на этот вопрос уже известен: как и прежде, в среднем потребуется вычислить функцию 2,25 раза.

Как и во всех алгоритмах с запросом сложности мы сконструируем оракула — вентиль, инкапсулирующий функцию. Оракул для нашего примера, где имеется всего четыре двоичные последовательности, показан на рис. 9.1.

Цепь для алгоритма Гровера изображена на рис. 9.2.

Алгоритм выполняет два шага. На первом переворачивается знак амплитуды вероятности, связанной с местом, которое мы пытаемся отыскать. Второй усиливает эту амплитуду вероятности. Посмотрим, как цепь делает это.

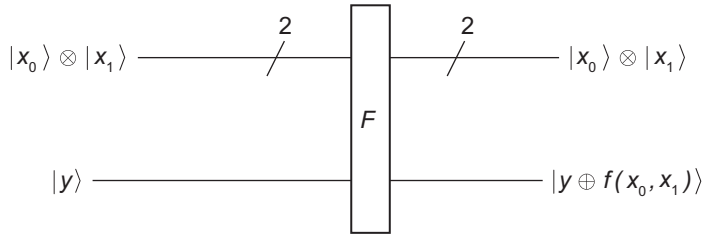


Рис. 9.1. Оракул для функции f

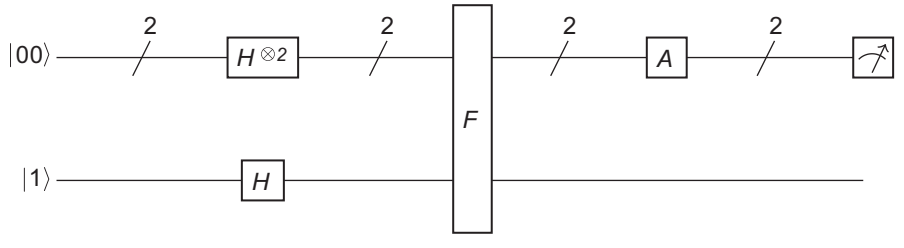


Рис. 9.2. Цепь для алгоритма Гровера

После передачи через вентили *Адамара* два верхних кубита получают состояние

$$\frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right),$$

а нижний кубит имеет состояние

$$\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$$

Объединенное состояние можно записать как

$$\frac{1}{2}\left(|00\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) + |01\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) + \right.$$
$$\left. + |10\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) + |11\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)\right).$$

Затем кубиты проходят через вентиль *F*. Он инвертирует 0 и 1 в третьем кубите в местоположение, которое мы пытаемся найти. Для нашего случая $f(10) = 1$ мы получим

$$\frac{1}{2}\left(|00\rangle\otimes\left(\frac{1}{\sqrt{2}}|0\rangle-\frac{1}{\sqrt{2}}|1\rangle\right)+|01\rangle\otimes\left(\frac{1}{\sqrt{2}}|0\rangle-\frac{1}{\sqrt{2}}|1\rangle\right)+\right.$$
$$\left.+|10\rangle\otimes\left(\frac{1}{\sqrt{2}}|1\rangle-\frac{1}{\sqrt{2}}|0\rangle\right)+|11\rangle\otimes\left(\frac{1}{\sqrt{2}}|0\rangle-\frac{1}{\sqrt{2}}|1\rangle\right)\right).$$

Это можно переписать как

$$\frac{1}{2}\left(|00\rangle+|01\rangle-|10\rangle+|11\rangle\right)\otimes\left(\frac{1}{\sqrt{2}}|0\rangle-\frac{1}{\sqrt{2}}|1\rangle\right).$$

В результате мы получаем два верхних кубита, не спутанных с нижним, но амплитуда вероятности $|10\rangle$ поменяет знак, что указывает на искомое местоположение.

Если на этом шаге измерить два верхних кубита, мы получим одно из четырех местоположений, при этом все четыре возможных ответа равновероятны. Нам нужно сделать еще один шаг — усилить амплитуду вероятности. Усиление амплитуды осуществляется путем переворачивания последовательности чисел относительно их среднего. Если число выше среднего, оно переворачивается и становится ниже среднего. Если число ниже среднего, оно переворачивается и становится выше среднего. В каждом случае удаленность от среднего сохраняется. Для иллюстрации используем четыре числа: 1, 1, 1 и –1. Их сумма равна 2, а среднее равно 2/4, или 1/2. Затем начинаем перебирать числа в последовательности. Первое число — это 1. Оно выше среднего на 1/2. После переворота оно должно стать на 1/2 ниже среднего. В данном случае оно превратится в 0. Число –1 ниже среднего на 3/2. После переворота оно должно стать на 3/2 выше среднего, то есть превратиться в 2.

В настоящее время два верхних кубита имеют состояние

$$\frac{1}{2}|00\rangle+\frac{1}{2}|01\rangle-\frac{1}{2}|10\rangle+\frac{1}{2}|11\rangle.$$

Перевернув амплитуды относительно среднего, получаем $0|00\rangle + 0|01\rangle + +1|10\rangle + 0|11\rangle = |10\rangle$. Выполнив измерение, мы определенно получим 10, то есть переворот относительно среднего дает нам именно то, что нужно. Мы должны лишь убедиться в существовании вентиля или, что то же самое, ортогональной матрицы, описывающей переворот относительно среднего. Такая матрица существует:

$$A = \frac{1}{2}\begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix}.$$

В результате воздействия вентиля на два верхних кубита мы получаем

$$A\left(\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle - \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle\right) = \frac{1}{4}\begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix}\begin{bmatrix} 1 \\ 1 \\ -1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |10\rangle.$$

В этом примере, где у нас всего два кубита, мы должны использовать оракула только один раз. Нам достаточно задать единственный вопрос. Для случая $n = 2$ алгоритм Гровера дает точный ответ после единственного вопроса, тогда как в классическом случае в среднем требуется задать 2,25 вопроса.

Эта идея распространяется на случай произвольного числа n кубитов. Мы начинаем с того, что переворачиваем знак амплитуды вероятности, которая соответствует искомому местоположению. Затем выполняем переворот относительно среднего. Однако в этом случае усиление амплитуды происходит не так существенно, как в ситуации с двумя кубитами. Возьмем для примера восемь чисел, семь из которых 1 и одно -1. Их сумма равна 6, а среднее равно $6/8$. После переворота относительно среднего числа 1 превратится в $1/2$, а число -1 превратится в $10/4$. Как следствие, при наличии трех кубитов, измерив один кубит после усиления амплитуды, мы получим искомое местоположение с большей вероятностью, чем другие. Проблема в том, что существует значительная вероятность получить неверный ответ. Нам нужна более высокая вероятность получения верного

ответа — нужно еще больше усилить амплитуду перед измерением. Решение состоит в том, чтобы передать все кубиты обратно через цепь. Мы снова переворачиваем знак амплитуды вероятности, связанной с искомым местоположением, и снова выполняем переворот относительно среднего.

Рассмотрим обобщенный случай. Нам нужно найти нечто, находящееся в одном из m возможных местоположений. Чтобы найти его классическим способом, в худшем случае мы должны задать $m - 1$ вопросов. Число вопросов растет пропорционально m. Гровер рассчитал формулу, которая определяет, сколько раз нужно использовать его цепь, чтобы получить максимальную вероятность правильного ответа. Число, которое дает эта формула, растет пропорционально $\sqrt{m}$. Это квадратичное ускорение.

Применения алгоритма Гровера

С реализацией алгоритма связано несколько проблем. Во-первых, квадратичное ускорение оценивается относительно запроса сложности. Чтобы использовать оракула, его нужно создать, и если не отнестись с к этой задаче с должной осторожностью, число шагов, выполняемых оракулом, перевесит число шагов, которое экономит алгоритм, и в результате алгоритм станет медленнее, а не быстрее классического. Другая проблема состоит в том, что, определяя ускорение, мы предполагаем неупорядоченность набора данных. Если набор данных имеет определенную структуру, часто можно найти классический алгоритм, использующий эту структуру и отыскивающий решение намного быстрее. Последняя проблема связана с ускорением. Квадратичное ускорение — не что иное, как экспоненциальное ускорение, которое мы наблюдали в других алгоритмах. Можно ли добиться большего? Давайте рассмотрим эти проблемы.

Обе проблемы, связанные с реализацией оракула и наличием структуры в наборе данных, обоснованы и показывают, что в большинстве случаев алгоритм Гровера не имеет практического применения для поиска в базе данных. Но в некоторых ситуациях наличие структуры в данных делает возможным создание оракула, действующего с высокой эффективностью. В таких ситуациях алгоритм может обогнать классические алгоритмы. Ответ на вопрос о возможности добиться большего успеха уже был дан. Доказано, что алгоритм Гровера является оптимальным. Не существует

квантового алгоритма, способного решить задачу с более чем квадратичным ускорением. Квадратичное ускорение, хотя и не такое впечатляющее, как экспоненциальное, все еще дает определенные выгоды. При работе с большими наборами данных любое ускорение может оказаться ценным.

Вероятно, главное применение алгоритм Гровера найдет не для поиска, как было представлено выше, а для его вариаций. В частности, может пригодиться идея усиления амплитуды.

Мы рассмотрели всего несколько алгоритмов, но алгоритмы Шора и Гровера считаются наиболее важными. Существует множество других алгоритмов, основанных на идеях, заложенных в этих двух.[1] А теперь переключим наше внимание с квантовых алгоритмов на другие сферы применения квантовых вычислений.

Химия и моделирование

В 1929 году Поль Дирак, рассуждая о квантовой механике, отметил: «Основные физические законы, необходимые для построения математической теории большей части физики и всей химии, полностью известны, трудность только в том, что точное применение этих законов приводит к слишком сложным уравнениям».

Вся теория химии построена на взаимодействиях атомов и конфигурациях электронов. Базовый математический аппарат известен — это квантовая механика, но хотя мы можем записать уравнения, мы не можем решить их точно. На практике химики используют приближенные вычисления, не пытаясь найти точное решение. В этих приближениях не учитываются мелкие детали. Этот подход используется в вычислительной химии, и в целом он дает неплохие результаты. Во многих случаях классические компьютеры способны дать довольно точный ответ, но есть области, где современные приемы вычислений не работают. Приближенный результат оказывается недостаточно хорошим — требуется учесть больше деталей.

[1] Исчерпывающий список всех квантовых алгоритмов можно найти в онлайн-сборнике «Quantum Algorithm Zoo», доступном по адресу https://math.nist.gov/quantum/zoo/.

Фейнман считал, что одним из основных применений квантовых компьютеров станет моделирование квантовых систем. Использование квантовых компьютеров для изучения химии, которая принадлежит к квантовому миру — естественная идея, обладающая огромным потенциалом. Существует множество областей, где можно надеяться, что квантовые вычисления внесут важный вклад. Одна из них — понимание, как работает фермент нитрогеназа, используемый при производстве удобрений. Существующая технология производства удобрений связана с выделением большого объема парниковых газов и весьма энергоемка. Квантовые компьютеры могут сыграть важную роль в понимании этой и других каталитических реакций.

В Чикагском университете есть группа ученых, занимающихся проблемой фотосинтеза. Преобразование солнечного света в химическую энергию — это быстрый и очень эффективный процесс. К тому же это квантово-механический процесс. Долгосрочная задача состоит в том, чтобы понять этот процесс и затем использовать в фотоэлектрических элементах.

Сверхпроводимость и магнетизм — это квантово-механические явления. Квантовые компьютеры могут помочь нам понять их лучше. Одной из целей является разработка сверхпроводников, не требующих охлаждения до температур, близких к абсолютному нулю.

Существующая конструкция квантовых компьютеров еще находится в зачаточном состоянии, но даже с несколькими кубитами уже можно начинать изучать законы химии. Недавно в IBM смоделировали молекулу гидрида бериллия (BeH_2) на семикубитном квантовом процессоре. Это относительно маленькая молекула, состоящая из трех атомов. В моделировании не использовались приближения, которые применялись в классических вычислениях. Однако из-за того, что процессор IBM использует всего несколько кубитов, квантовый процессор можно смоделировать на классическом компьютере. Следовательно, все, что можно сделать на этом квантовом процессоре, можно сделать и на классическом компьютере. Однако с увеличением числа кубитов мы достигнем точки, когда квантовые процессоры будет невозможно смоделировать классическими средствами. Очень скоро мы вступим в эпоху, когда квантовое моделирование окажется не под силу никаким классическим компьютерам.

Теперь, рассмотрев некоторые возможные применения, кратко рассмотрим способы, которые используются для создания квантовых компьютеров.

Оборудование

Чтобы создать квантовый компьютер, имеющий практическую ценность, необходимо решить ряд проблем, наиболее серьезной из которых является декогеренция — проблема взаимодействия кубита с чем-то в окружающей среде, не являющимся частью вычислений. Нужна возможность установить кубит в исходное состояние и удерживать его в этом состоянии, пока не потребуется использовать его. Также нужна возможность конструировать вентили и цепи. Что можно использовать в качестве кубита?

Фотоны обладают полезными свойствами: они легко инициализируются и запутываются и слабо взаимодействуют с окружающей средой, поэтому они могут оставаться когерентными в течение долгого времени. С другой стороны, фотоны трудно хранить и держать их в готовности до момента, когда они могут понадобиться. Фотоны идеально подходят для передачи информации, но их сложно использовать для построения квантовых цепей.

В своих примерах мы часто использовали спин электрона. Можно ли использовать его? В первых главах упоминалась установка, использовавшаяся в проверке неравенства Белла. В ней использовались электроны, пойманные в ловушки в синтетических алмазах. Управление ими производилось путем воздействия на алмазы лучом лазера. Проблема заключается в масштабировании. В настоящее время таким способом можно создать один-два кубита, но не больше. Также были попытки использовать спин ядра, но опять возникла проблема масштабируемости.

Еще один метод основан на использовании на энергетических уровнях ионов. В вычислениях с ионной ловушкой используются ионы, удерживаемые в электромагнитных полях. Чтобы удержать ион, необходимо минимизировать колебания; охлаждение до температуры, близкой к абсолютному нулю, позволяет добиться этого. Энергетические уровни ионов кодируют кубиты, а для управления ими можно использовать лазеры. Дэвид Уайнленд (David Wineland) использовал ионные ловушки для создания первого вентиля *управляемое НЕ* (*CNOT*) в 1995 году, за что получил Нобелевскую премию, а в 2016 году исследователи из NIST запутали более 200 ионов бериллия. Ионные ловушки действительно можно использовать в будущих квантовых компьютерах, но вообще такие компьютеры можно строить с использованием других подходов.

Чтобы минимизировать взаимодействие квантовых компьютеров с окружающей средой, они всегда защищаются от воздействия света и тепла. Они защищаются от любого электромагнитного излучения и охлаждаются. При сильном охлаждении некоторые материалы превращаются в сверхпроводники — теряют сопротивление электрическому току. Сверхпроводники обладают квантовыми свойствами, которые можно использовать. К ним относятся, например, так называемые пары Купера (Cooper) и переходы Джозефсона (Josephson).

Электроны в сверхпроводнике объединяются, образуя *пары Купера*. Эти пары электронов действуют как самостоятельные частицы. Если поместить тонкие слои сверхпроводника между тонкими слоями изолятора, получится переход Джозефсона.[1] В настоящее время это явление используется для создания высокочувствительных приборов, измеряющих магнитные поля. Для нас важным фактом является то обстоятельство, что энергетические уровни куперовских пар в сверхпроводящей цепи, содержащей переход Джозефсона, дискретны и могут использоваться для кодирования кубитов.

В своих квантовых компьютерах IBM использует сверхпроводящие кубиты. В 2016-м IBM представила пятикубитный процессор, к которому они предоставили бесплатный доступ в облаке. Любой желающий может спроектировать свою квантовую цепь, если она использует пять или меньше кубитов, и опробовать ее на этом компьютере. Цель IBM — представить квантовые вычисления широкой аудитории: на этом компьютере были опробованы цепи для сверхплотного кодирования, неравенства Белла и моделирования атома водорода. Также была запущена простейшая версия Battleships, давшая программисту возможность создать первую многопользовательскую игру для квантового компьютера. В конце 2017 года IBM подключила к облаку двадцатикубитный компьютер. Но он является коммерческим предприятием, и доступ к нему необходимо оплачивать.

Компания Google тоже работает над своим квантовым компьютером. Он также основан на сверхпроводящих кубитах. Ожидается, что в ближайшее

[1] Брайан Дэвид Джозефсон (Brian David Josephson) получил Нобелевскую премию по физике за работу, объяснившую, как могут перетекать пары Купера через переход Джозефсона в результате квантового туннелирования.

время Google объявит о создании 72-кубитного компьютера. Что такого особенного в этом числе?

Классические компьютеры способны моделировать работу квантового компьютера с небольшим числом кубитов, но с увеличением числа кубитов мы подходим к пределу, когда такое моделирование становится невозможным. Ожидается, что Google объявит о достижении или превышении этого порога, что даст им право претендовать на квантовое превосходство — впервые появится возможность запустить алгоритм на квантовом компьютере, который нельзя выполнить или смоделировать на классическом компьютере. Однако и IBM не отступит без боя. Исследователи из этой компании, используя некоторые инновационные идеи, недавно нашли способ моделирования 56-кубитной системы на классической основе, подняв нижнюю границу числа кубитов, необходимых для квантового превосходства.

Поскольку работы по созданию квантовых компьютеров продолжаются, мы, вероятно, увидим побочные эффекты в других областях. Кубиты, как бы мы их ни кодировали, чувствительны к взаимодействиям с их окружением. Чем лучше мы будем понимать природу этих взаимодействий, тем надежнее сможем защищать кубиты, а также научимся проектировать методы, которыми кубиты смогут измерять их окружение.

Примером могут служить электроны, попадающие в ловушки в синтетических алмазах. Они очень чувствительны к магнитным полям. NVision Imaging Technologies — это начинающий проект, использующий эту идею для создания томографов, основанных на эффекте ядерно-магнитного резонанса, которые, как надеются участники, будут лучше, быстрее и дешевле современных.

Квантовый отжиг

Компания D-Wave предлагает компьютеры для продажи. Их последняя модель D-Wave 2000Q, как можно догадаться по названию, имеет 2000 кубитов. Однако это не обычные компьютеры, они проектировались для решения некоторых задач оптимизации с использованием квантового отжига. Я кратко расскажу, что это означает.

Кузнецам часто приходится плющить и гнуть металл. Металл может быть закаленным, когда в его кристаллической структуре имеют место различные напряжения и деформации, что усложняет работу. В таких случаях кузнецы прибегают к отжигу. Традиционный отжиг — это метод восстановления однородной кристаллической структуры, делающий металл податливым. Производится отжиг нагреванием металлической детали до высокой температуры и последующим медленным охлаждением.

Для решения некоторых задач оптимизации можно использовать имитацию отжига — стандартный прием, основанный на отжиге. Например, предположим, что у нас есть график, изображенный на рис. 9.3, и мы должны найти самую нижнюю точку — абсолютный минимум. Представьте, что этот график изображает дно двумерного ведра. Мы бросаем в ведро металлический шарик. Он скатится на дно одной из седловин, которые на рис. 9.3 обозначены буквами *A*, *B* и *C*. Мы должны найти *C*. Шарик может скатиться не только в точку C, но также в точку *A*. Было сделано важное для отжига наблюдение: чтобы поднять шарик вверх по склону и уронить его в седловину *B*, требуется намного меньше энергии, чем чтобы поднять шарик вверх из седловины *B* и уронить его в седловину *A*. Поэтому мы встряхиваем ведро энергично настолько, насколько необходимо для преодоления барьера между двумя седловинами. Шарик может перекатиться из *A* в *B*, но не может перекатиться обратно. Итак, встряхивая ведро, мы заставим шарик перекатиться из *A* в *B*. Но если встряхивать его столь же энергично, шарик может перекатиться из *C* в *B*. Следующий шаг — снова

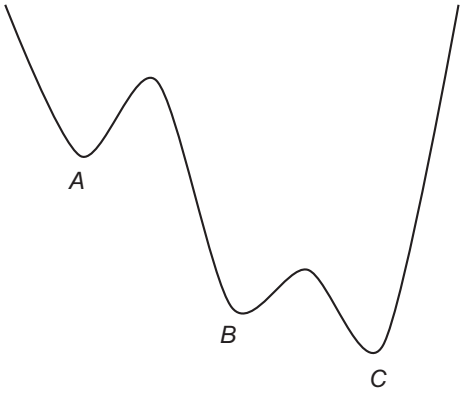


Рис. 9.3. График функции — дно ведра

встряхнуть ведро, но менее энергично, только чтобы шарик мог перекатиться из *B* в *C*, но не мог перекатиться обратно, из *C* в *B*.

Итак, мы встряхиваем ведро все менее и менее энергично. Это похоже на постепенное охлаждение металла при традиционном отжиге. В результате металлический шарик оказывается в самой нижней точке. Мы нашли абсолютный минимум функции.

Квантовый отжиг добавляет квантовое туннелирование. Это квантовый эффект, заставляющий шарик появляться по другую сторону барьера. Вместо того чтобы подниматься вверх по склону барьера, он может пройти сквозь него. Вместо уменьшения высоты барьера, по склону которого может подняться шарик, вы уменьшаете длину туннеля, который тот может проделать.

D-Wave выпустила несколько компьютеров, использующих квантовый отжиг для решения задач оптимизации. В первое время они столкнулись с неверием, что их компьютеры действительно используют эффект квантового туннелирования, но теперь скептики согласились, что это действительно так. Остается еще некоторое сомнение — действительно ли их компьютеры находят решение быстрее классических, но люди покупают их. Среди многих других компьютеры D-Wave приобрели такие крупные компании, как Volkswagen, Google и Lockheed Martin.

После этого краткого обзора оборудования перейдем к более глубоким вопросам. Что квантовые вычисления могут рассказать нам о нас и о Вселенной? И какие вычисления находятся на самом фундаментальном уровне?

Квантовое превосходство и параллельные Вселенные

Существует 8 возможных трехбитных комбинаций: 000, 001, 010, 011, 100, 101, 110, 111. Число 8 — это 2^3. Два значения может принимать первый бит, два значения — второй и два значения — третий, и мы перемножаем эти три двойки. Если вместо битов использовать кубиты, каждая из 8 трехбитных последовательностей будет связана с базисным вектором, то есть получится 8-мерное векторное пространство. Следуя той же логике, для

n кубитов мы получим 2^n базисных векторов и 2^n-мерное пространство. С ростом числа кубитов количество базисных векторов растет в экспоненциальной прогрессии и мерность соответствующего векторного пространства увеличивается очень быстро.

Для 72 кубитов количество базисных векторов равно 2^{72}, то есть что-то около 4 000 000 000 000 000 000 000. Это огромное число, и считается, что оно примерно соответствует точке, выше которой классические компьютеры уже не смогут моделировать работу квантовых компьютеров. Как только появится квантовый компьютер, имеющий 72 или более кубита, мы вступим в эпоху квантового превосходства — когда квантовые компьютеры смогут выполнять вычисления, непосильные для любых классических компьютеров. Как уже упоминалось выше, ожидается, что в ближайшее время Google объявит о достижении этой эпохи. (Последний компьютер D-Wave имеет 2000 кубитов. Однако эта специализированная машина не способна делать что-то, что было бы не под силу обычному компьютеру, поэтому она не преодолела барьер квантового превосходства.)

Давайте представим машину с 300 кубитами. Это число не кажется недостижимым в не слишком отдаленном будущем. Но 2^{300} — это гигантское число. Это больше, чем число элементарных частиц в известной Вселенной! В вычислениях с 300 кубитами будут участвовать 2^{300} базисных элемента. Дэвид Дойч задался вопросом, где могут существовать вычисления, вовлекающие больше базисных элементов, чем частиц во Вселенной. Он полагал, что мы должны принять идею существования параллельных вселенных, взаимодействующих друг с другом.

Этот взгляд на квантовую механику и параллельные вселенные восходит к исследованиям Хью Эверетта (Hugh Everett). Идея Эверетта состоит в том, что при каждом измерении Вселенная расщепляется на несколько копий, в каждой из которых получается свой результат. И хотя с этой точкой зрения согласны очень немногие, Дойч твердо верит в ее верность. Одной из целей, которые Дойч преследовал в своей фундаментальной статье, посвященной квантовым вычислениям и опубликованной в 1985 году, было показать возможность существования параллельных вселенных. Он надеется, что однажды появится тест, аналогичный проверке неравенства Белла, который подтвердит эту точку зрения.

Вычисления

Алан Тьюринг является одним из отцов теории вычислений. В своем историческом труде 1936 года он тщательно проанализировал вычисления. Он рассматривал действия, которые люди предпринимали в процессе вычислений, и разбивал их на элементарные шаги. Он показал, что простая теоретическая машина, которую теперь мы называем машиной Тьюринга, способна выполнить любой алгоритм. Теоретические машины Тьюринга превратились в современные компьютеры. Эти компьютеры универсальны. Анализ Тьюринга показал нам самые элементарные операции, включающие манипуляции с битами. Но не забывайте, что Тьюринг основывался на том, что делают люди.

Фредкин, Фейнман и Дойч утверждают, что Вселенная тоже делает вычисления и что вычисления являются частью физики. Квантовые вычисления переносят фокус с людей на Вселенную. Статью Дойча, опубликованную в 1985 году, также следует рассматривать как поворотную в теории вычислений. В ней он показал, что фундаментальным объектом является не бит, а кубит.

Мы уже знаем, что вскоре достигнем точки квантового превосходства, что мы создадим квантовые компьютеры, которые невозможно смоделировать ни на каком классическом компьютере. Но возможно ли обратное? Смогут ли квантовые компьютеры моделировать классические? Да, смогут. На квантовом компьютере можно выполнить любые классические вычисления. Следовательно, квантовые вычисления являются более общей формой, чем классические. Квантовые вычисления — это не замысловатый способ выполнения некоторых специальных вычислений, это новый способ представления вычислений с концептуальной точки зрения. Мы не должны рассматривать квантовые и классические вычисления как два разных предмета. Любые вычисления — это, по сути, квантовые вычисления. Классические вычисления являются лишь частным случаем квантовых вычислений.

С этой точки зрения классические вычисления выглядят как антропоцентрическая версия того, чем на самом деле являются вычисления. Подобно тому, как Коперник показал, что Земля не является центром Вселенной, а Дарвин — что люди произошли от других животных, мы теперь начина-

ем понимать, что человек не является центром вычислений. Квантовые вычисления кардинально меняют наши представления.

Я не думаю, что классические вычисления уйдут в прошлое, но общепризнанным станет факт существования более фундаментальной формы вычислений. Самый элементарный уровень вычислений основывается на кубитах, запутывании и суперпозициях. В настоящее время основное внимание уделяется тому обстоятельству, что некоторые квантовые алгоритмы работают быстрее классических, но эта ситуация изменится. Квантовая физика существует дольше квантовых вычислений. Ныне она воспринимается как самостоятельная область науки. Физики не пытаются сравнивать квантовую и классическую физику и показывать, что в чем-то она лучше. Они изучают квантовую физику отдельно. То же произойдет с квантовыми вычислениями. Мы получим новые инструменты, меняющие подходы к изучению вычислений. Мы будем использовать их в экспериментах, чтобы понять, что нового можно сконструировать. Мы начали с телепортации и сверхплотного кодирования и продолжаем свои исследования.

Мы вступаем в новую эру, с новыми представлениями об истинной природе вычислений. Пока нельзя сказать, какие новые открытия поджидают нас, но время для исследований и открытий настало. Нас ждут лучшие годы квантовых вычислений.

Крис Бернхард

Квантовые вычисления для настоящих айтишников

Перевел с английского *А. Киселев*

Заведующая редакцией	*Ю. Сергиенко*
Ведущий редактор	*К. Тульцева*
Литературный редактор	*О. Букатка*
Художественный редактор	*В. Мостипан*
Корректоры	*С. Беляева, Н. Викторова*
Верстка	*Л. Егорова*

Изготовлено в России. Изготовитель: ООО «Прогресс книга».
Место нахождения и фактический адрес: 194044, Россия, г. Санкт-Петербург,
Б. Сампсониевский пр., д. 29А, пом. 52. Тел.: +78127037373.

Дата изготовления: 10.2019. Наименование: книжная продукция. Срок годности: не ограничен.

Налоговая льгота — общероссийский классификатор продукции ОК 034-2014, 58.11.12 —
Книги печатные профессиональные, технические и научные.

Импортер в Беларусь: ООО «ПИТЕР М», 220020, РБ, г. Минск, ул. Тимирязева, д. 121/3, к. 214, тел./факс: 208 80 01.

Подписано в печать 25.09.19. Формат 70×100/16. Бумага офсетная. Усл. п. л. 19,350. Тираж 1500. Заказ 0000.