

Содержание

Предисловие	10
Благодарности	13
Навигация по этой книге	15
От издательства	18
Часть I. ОСНОВЫ	19
Глава 1. Суперпозиция, запутанность и обратимость	20
Глава 2. Краткая история квантовых вычислений	27
Глава 3. Кубиты, операторы и измерения	33
Диаграммы квантовых схем	37
3.1. Квантовые операторы	37
Унарные операторы	38
Бинарные операторы	42
Тернарные операторы	44
3.2. Сравнение с классическими вентилями	46
3.3. Универсальность квантовых операторов	47
3.4. Теоремы Готтесман–Книлла и Соловья–Китаева	47
3.5. Сфера Блоха	48
3.6. Постулат измерения	49
3.7. Вычисления на месте	51
Глава 4. Сложность теории	54
4.1. Задачи против алгоритмов	54
4.2. Сложность времени	55
4.3. Классы сложности	57
4.4. Квантовые вычисления и тезис Черча–Тьюринга	60
Часть II. АППАРАТУРА И ПРИЛОЖЕНИЯ	62
Глава 5. Построение квантового компьютера	63
5.1. Оценка квантового компьютера	64
5.2. Нейтральный атом	65
5.3. Ядерный магнитный резонанс	67
5.4. Центр NV в алмазе	68
5.5. Фотоника	68

Полупроводниковый квантовый транзистор	70
Топологический фотонный чип	70
5.6. Спиновые кубиты.....	71
5.7. Сверхпроводящие кубиты	73
5.8. Топологические квантовые вычисления.....	74
5.9. Захваченный ион	74
5.10. Резюме	76

Глава 6. Библиотеки разработки для квантового компьютерного программирования

6.1. Квантовые компьютеры и имитаторы	78
6.2. Библиотека Cirq.....	80
6.3. Библиотека Qiskit	82
6.4. Библиотека Forest.....	85
6.5. Библиотека QDK.....	87
6.6. Резюме по библиотекам разработки	90
Использование библиотек разработки	90
Другие библиотеки разработки	91
6.7. Дополнительные квантовые программы	91
Состояния Белла	91
Вентили с параметрами.....	93

Глава 7. Телепортация, сверхплотное кодирование и неравенство Белла.....

7.1. Квантовая телепортация.....	96
7.2. Сверхплотное кодирование	99
7.3. Код квантовой телепортации и сверхплотной связи.....	100
7.4. Тест неравенства Белла	103
7.5. Резюме.....	107

Глава 8. Канон: пошаговые руководства по коду.....

8.1. Алгоритм Дойча–Джозса (DJ).....	110
8.2. Алгоритм Бернштейна–Вазирани	117
Алгоритм Бернштейна–Вазирани.....	118
8.3. Задача Саймона.....	120
8.4. Квантовое преобразование Фурье	121
8.5. Алгоритм Шора	123
Криптография RSA	123
Период функции	125
Период функции как вход в алгоритм факторизации	126
8.6. Алгоритм поиска Гровера.....	138
8.7. Резюме.....	141

Глава 9. Методы квантовых вычислений.....

9.1. Вариационный квантовый собственный решатель.....	142
---	-----

VQE с шумом	147
Более сложные анзацы	148
9.2. Квантовая химия	150
9.3. Алгоритм квантовой приближенной оптимизации (QAOA)	155
Пример реализации QAOA	158
9.4. Машинное обучение на квантовых процессорах	165
9.5. Квантовая оценка фазы	170
Реализация QPE	173
9.6. Решение линейных систем уравнений	176
Описание алгоритма HHL	178
Пример реализации алгоритма HHL	180
9.7. Квантовый генератор случайных чисел	187
9.8. Квантовые блуждания	189
Реализация квантового блуждания	191
9.9. Резюме	197
Глава 10. Приложения и квантовое превосходство	198
10.1. Приложения	198
Квантовое моделирование и химия	198
Выборка из вероятностных распределений	199
Ускорение линейной алгебры с помощью квантовых компьютеров	199
Оптимизация	199
Тензорные сети	199
10.2. Квантовое превосходство	199
Случайная выборка схемы	200
Другие задачи демонстрации квантового превосходства	205
Квантовое преимущество	205
10.3. Будущие направления	205
Квантовая коррекция ошибок	205
Занимаемся физикой с помощью квантовых компьютеров	206
10.4. Заключение	207
Часть III. ИНСТРУМЕНТАРИЙ	208
Глава 11. Математические инструменты	
для квантовых вычислений I	209
11.1. Введение и самопроверка	209
11.2. Линейная алгебра	211
Векторы и обозначения	211
Основные векторные операции	212
Норма вектора	216
Скалярное произведение	219
11.3. Комплексные числа и внутреннее произведение	222
Комплексные числа	222
Внутреннее произведение как усовершенствование скалярного	
произведения	224

Представление комплексного числа в полярных координатах	229
11.4. Первый взгляд на матрицы	236
Основные матричные операции	236
Матрица идентичности.....	243
Транспонирование, сопряжение и отслеживание.....	245
Возведение матриц в степень.....	252
11.5. Внешнее произведение и тензорное произведение.....	253
Внешнее произведение как способ построения матриц.....	253
Тензорное произведение	255
11.6. Теория множеств	258
Основы теории множеств	258
Декартово произведение	261
Отношения и функции.....	261
Важные свойства функций	267
11.7. Определение линейного преобразования	271
11.8. Как построить векторное пространство с нуля.....	273
Группы.....	274
Поля	280
Определение векторного пространства.....	285
Подпространства	288
11.9. Интервал, линейная независимость, основы и размерность.....	290
Интервал	290
Линейная независимость.....	292
Базис и размерность.....	294
Ортонормированный базис.....	297
Определение ортонормированного базиса.....	298

Глава 12. Математический инструментарий

для квантовых вычислений II	299
12.1. Линейные преобразования как матрицы.....	299
12.2. Матрицы как операторы.....	304
Введение в определитель.....	305
Геометрия определителя.....	308
Инверсии матрицы.....	310
12.3. Собственные векторы и собственные значения	317
Изменение базиса	319
12.4. Дальнейшее исследование внутренних произведений.....	322
Дельта-функция Кронекера как внутреннее произведение	325
12.5. Эрмитовы операторы	325
Почему мы не можем измерять комплексными числами.....	326
Эрмитовы операторы имеют действительные собственные значения.....	327
12.6. Унитарные операторы	329
12.7. Прямая сумма и тензорное произведение.....	330
Прямая сумма	330
Тензорное произведение	333

12.8. Гильбертово пространство	336
Метрики, последовательности Коши и полнота.....	336
Аксиоматическое определение внутреннего продукта.....	340
Определение гильбертова пространства	341
12.9. Кубит как гильбертово пространство	342

Глава 13. Математические инструменты

для квантовых вычислений III..... 346

13.1. Булевы функции	346
13.2. Логарифмы и экспоненты	347
13.3. Формула Эйлера	349

Глава 14. Таблицы квантовых операторов и основных схем 352

Библиография..... 355

Предисловие

Мы вступаем в новую эру вычислений, которая станет катализатором открытий в науке и технологиях. Новые вычислительные платформы исследуют фундаментальные законы нашей Вселенной и помогут в решении сложных проблем, которые затрагивают всех нас. Программы машинного обучения на базе специализированных чипов уже приносят прорыв за прорывом.

В этой книге мы исследуем квантовые вычисления – развивающуюся платформу, которая фундаментально отличается от того, как мы выполняем вычисления на современных цифровых платформах. Безусловно, мы далеки от масштабных квантовых компьютеров на годы. Однако теперь мы знаем, что такие системы возможны; благодаря достижениям в области инженерии мы, вероятно, увидим их реальное влияние.

Квантовые вычисления являются частью более широкой области квантовой информации (quantum information sciences, QIS). Все три ветви QIS – вычисления, коммуникации и зондирование – развиваются быстрыми темпами, и открытие в одной области может стимулировать прогресс в другой. Квантовая коммуникация использует необычные свойства квантовых систем для передачи информации таким образом, чтобы ее не мог прочитать ни один перехватчик. Эта область становится все более важной, поскольку квантовые вычисления подталкивают нас к режиму постквантовой криптографии. В главе 7 мы рассмотрим квантовую телепортацию и сверхплотное кодирование, которые являются протоколами, специфичными для квантовой связи.

Квантовое зондирование – это надежная область исследований, в которой используются квантовые устройства, позволяющие выйти за классические пределы в обнаружении магнитных и других полей. Например, появляется новый класс датчиков для определения положения, навигации и времени (position, navigation and timing, PNT) в атомном масштабе. Эти устройства micro-PNT могут предоставлять высокоточные данные о местоположении, когда GPS заблокирован или недоступен.

В данной книге мы сосредоточимся на квантовых вычислениях. Одно из важнейших различий между квантовыми и классическими вычислениями заключается в том, что при квантовых вычислениях *мы манипулируем непосредственно квантовыми состояниями*; это дает нам гораздо большее рабочее вычислительное пространство, чем классические компьютеры. В классических компьютерах, если мы хотим смоделировать квантовую физическую систему реального мира, мы можем сделать это только с нашими представлениями о такой системе, и мы не можем реализовать саму физику.

Это ключевое отличие открывает захватывающие возможности для будущего вычислений и науки. Они начинаются с фундаментальных истин

о нашем мире, которые были разработаны во время революции квантовой механики в первой половине XX века. Мы рассмотрим некоторые из этих фундаментальных концепций в первой главе.

Мне посчастливилось изучать квантовую механику до того, как я стал изучать классическую физику, и поэтому я отношусь к квантовой физике как к норме – это мой интеллектуальный дом. Пока мы не изменим нашу образовательную систему, большинство студентов будут изучать классику раньше кванта, и поэтому квант будет казаться вдвойне странным – как из-за их собственного человеческого опыта, так и из-за внедрения классических идей до того, как могут быть внедрены квантовые идеи.

Что парадоксально в таком положении дел, так это то, что основным математическим инструментом квантовой механики является линейная алгебра, мощный, но очень доступный раздел математики. Однако большинство студентов изучают линейную алгебру только после двух или трех семестров исчисления, если они вообще ее изучают. Тем не менее для изучения линейной алгебры не требуется никакого исчисления! Как бы там ни было, мы оставим исправление математического образования на другой раз, а пока отправимся здесь в путешествие к новой форме вычислений.

В этой книге мы исследуем, как построить компьютер, совершенно не похожий на те, что когда-либо создавались людьми. Что отличает эту книгу, так это то, что мы выйдем за рамки теории и перейдем к практической работе по построению таких компьютерных систем и *написанию приложений для этих систем*.

Сейчас существует несколько библиотек разработки, которые мы можем использовать для программирования облачных квантовых систем. Мы рассмотрим примеры кода и покажем читателю, как построить квантовую схему, состоящую из набора операторов, для решения конкретной задачи. В этой книге мы в основном будем использовать язык программирования Python.

В настоящее время мы находимся в стадии шумных квантовых компьютеров среднего масштаба (noisy intermediate-scale quantum, NISQ). Этот термин введен Джоном Прескиллом (John Preskill) из Калифорнийского технологического института (CalTech) [176]. Он относится к системам, которые еще не имеют полной коррекции ошибок (следовательно, зашумлены) и имеют от десятков до тысяч кубитов, что значительно меньше количества в 10^6 плюс, необходимого для масштабируемых отказоустойчивых вычислений. Несмотря на ограничения этих начальных систем, теория, алгоритмы и методы кодирования, которые мы рассматриваем в этой книге, будут полезны читателям при переходе к более крупным системам, которые появятся в будущем.

Эта книга состоит из трех книг в одной: первая часть посвящена необходимой структуре, которая сопровождает проектирование квантовых компьютеров и схем. Мы также исследуем, какие проблемы могут быть решены с помощью квантовых вычислений при нашем подходе к классам сложности.

Вторая часть книги предназначена для тех читателей, которые хотят углубиться в программирование, обеспечивающее работу этих новых компью-

теров. Если у вас уже есть опыт работы в квантовой механике, квантовой теории информации и теоретической информатике (вы знаете, кто вы!), вы можете сразу перейти ко второй части и окунуться в код. Пожалуйста, обратитесь к руководству на следующих страницах по навигации в этой книге, чтобы наметить план изучения этого материала.

В третьей части мы предлагаем набор критически важных инструментов для использования при осуществлении квантовых вычислений (quantum computing, QC).

Мы формируем основные концепции линейной алгебры и специально связываем их с использованием в QC. Таблица операторов и элементов схем в главе 14 является удобным справочником при разработке собственных протоколов квантовых вычислений.

Книга также является порталом к постоянно растущему объему литературы по данной теме. Мы рекомендуем читателю использовать библиографию для изучения как основополагающих, так и недавних статей в этой области.

Мы будем постоянно давать дополнительные онлайн-примеры и руководства по коду. Это живой текст, который будет развиваться по мере развития технологии квантовых компьютеров. Мы будем вместе путешествовать по этому новому пути; присоединяйтесь к нам онлайн на сайте GitHub, посвященном этой книге¹. Мы будем очень рады видеть, что вы осуществите с помощью этих новых платформ и инструментов. Свяжитесь с нами через сайт – мы с нетерпением ждем встречи с вами.

Джек Д. Хидари
Июнь 2019 г.,
на высоте 35 000 футов

¹ <http://www.github.com/jackhidary/quantumcomputingbook>.

Навигация по этой книге

Вот наши предложения, как наилучшим образом использовать эту книгу.

1. *Преподаватели университета*: вы можете создать несколько различных курсов, используя материал данной книги. Весь код из книги есть на сайте книги. В главы по математике встроены упражнения; для других глав обратитесь, пожалуйста, к онлайн-сайту, где вы найдете упражнения по кодированию и другие наборы задач.

(a) Курс квантовых вычислений для специальностей STEM:

- i) для этого курса мы рекомендуем определить главы 1 и 2 в качестве предварительного чтения курса, а затем переходить последовательно к главам с упражнениями, представленными на сайте GitHub. Решения также доступны на сайте;
- ii) если студенты не обладают достаточной глубиной познаний формальной линейной алгебры и связанных с ней математических инструментов, часть III образует прочную основу для многонедельного изучения с упражнениями.

(b) Курс квантовых вычислений для аспирантов-физиков:

- i) для данного курса мы рекомендуем использовать эту книгу вместе с Майком и Айком (как многие из нас говорят, ссылаясь на превосходный учебник Нильсена и Чуанга [161]) или другую подходящую книгу, в которой подробно рассматриваются теоретические концепции. Мы все очень благодарны Майклу Нильсену, Исааку Чуангу и авторам других учебников за последние двадцать лет. Мы также рекомендуем обращаться к конспектам лекций Джона Прескилла, если вы создаете свой курс для продвинутых студентов-физиков [174]. Наша работа должна дополнять Майка и Айка в нескольких отношениях:
 - A) эта работа больше сосредоточена на кодировании. По очевидным причинам книги, написанные до последних нескольких лет, не могли охватывать инструменты разработки и подходы к квантовым вычислениям на основе Python, которые существуют теперь;
 - B) эта книга не углубляется, как Майк и Аик, в теоретические концепции информации;
 - C) в разделе математических инструментов этой книги есть более подробный набор для тех студентов, которые, возможно, не прошли строгий курс линейной алгебры. Краткого изложения линейной алгебры и других необходимых математических инструментов в других учебниках по квантовой механике, как показывает наш опыт, зачастую недостаточно;

- ii) мы рекомендуем сначала определить в качестве предварительного чтения главы 1 и 2;
 - iii) затем мы предлагаем охватить главы об унитарных операторах, измерениях и квантовых схемах с упражнениями на сайте Github для проверки знаний;
 - iv) потом рекомендуем посвятить большую часть курса части II книги, чтобы студенты получили практический опыт работы с кодом.
- (с) Курс квантовых вычислений для аспирантов CS:
- i) мы предлагаем сделать первые две главы предварительным чтением, а затем – обзором математических инструментов в части III. Обычно недостаточно предварительного знакомства с линейной алгеброй только на уровне бакалавриата, поскольку ее, скорее всего, изучали без полного формализма;
 - ii) затем мы рекомендуем главы 3 и 4, чтобы познакомиться с унитарными операторами, измерениями и классами сложности в квантовом режиме. Преподаватель может использовать обзорные вопросы и ответы на сайте GitHub;
 - iii) потом курс может охватывать подходы к созданию квантового компьютера, а затем следовать всем главам, посвященным кодированию.

Посетите сайт книги GitHub, чтобы найти дополнительные ресурсы, в том числе код из книги, наборы задач, решения, ссылки на видео и другие педагогические ресурсы.

2. *Физики*: для физиков, которые специализируются в областях, не связанных с квантовыми вычислениями, но хотят быстро развиваться в этой области, мы рекомендуем прочитать краткую историю квантовых компьютеров, поскольку предоставляем больше деталей, чем типичные трактовки, а затем обзор квантового оборудования по приложениям во второй части книги.
3. *Инженеры-программисты*: мы рекомендуем начать с первых двух глав, а потом рассмотреть сводку математических инструментов в части III. Затем мы предлагаем вернуться к рассмотрению кубитов и унитарных операторов в части I и продолжить далее.
4. *Руководители инженерного отдела и бизнеса*: читателям, которые не собираются заниматься программированием на практике, мы рекомендуем сосредоточиться на главах 1–4. Более смелые могут захотеть проработать некоторые примеры кода, чтобы ощутить смысл алгоритмов.
5. *Самостоятельное изучение*: эту книгу можно легко использовать как учебник для самостоятельного изучения. Рекомендуем совместить с онлайн-ресурсами. Пожалуйста, посетите сайт GitHub для получения обновленного списка ресурсов: <http://www.github.com/jackhidary/Quantumcomputingbook>.

Мы рекомендуем сначала оценить ваше текущее понимание основных инструментов из части III; в данном разделе есть множество самопроверок, которые можно использовать для этой цели. Затем читатель может перейти

к части I. Для тех, кто хорошо разбирается в квантовой механике и/или теории информации, мы рекомендуем, прежде чем переходить к части II книги «Аппаратное обеспечение и приложения», поискать статьи, упомянутые в главах 2–4, чтобы получить более глубокое понимание состояния этой области.

Посетите сайт книги GitHub, чтобы найти ряд ресурсов, в том числе код из книги, наборы задач, решения, ссылки на видео и другие педагогические ресурсы.

От издательства

Отзывы и пожелания

Мы всегда рады отзывам наших читателей. Расскажите нам, что вы думаете об этой книге – что понравилось или, может быть, не понравилось. Отзывы важны для нас, чтобы выпускать книги, которые будут для вас максимально полезны.

Вы можете написать отзыв на нашем сайте www.dmkpress.com, зайдя на страницу книги и оставив комментарий в разделе «Отзывы и рецензии». Также можно послать письмо главному редактору по адресу dmkpress@gmail.com; при этом укажите название книги в теме письма.

Если вы являетесь экспертом в какой-либо области и заинтересованы в написании новой книги, заполните форму на нашем сайте по адресу http://dmkpress.com/authors/publish_book/ или напишите в издательство по адресу dmkpress@gmail.com.

Скачивание исходного кода примеров

Скачать файлы с дополнительной информацией для книг издательства «ДМК Пресс» можно на сайте www.dmkpress.com на странице с описанием соответствующей книги.

Список опечаток

Хотя мы приняли все возможные меры для того, чтобы обеспечить высокое качество наших текстов, ошибки все равно случаются. Если вы найдете ошибку в одной из наших книг, мы будем очень благодарны, если вы сообщите о ней главному редактору по адресу dmkpress@gmail.com. Сделав это, вы избавите других читателей от недопонимания и поможете нам улучшить последующие издания этой книги.

Нарушение авторских прав

Пиратство в интернете по-прежнему остается насущной проблемой. Издательства «ДМК Пресс» и Springer очень серьезно относятся к вопросам защиты авторских прав и лицензирования. Если вы столкнетесь в интернете с незаконной публикацией какой-либо из наших книг, пожалуйста, пришлите нам ссылку на интернет-ресурс, чтобы мы могли применить санкции.

Ссылку на подозрительные материалы можно прислать по адресу электронной почты dmkpress@gmail.com.

Мы высоко ценим любую помощь по защите наших авторов, благодаря которой мы можем предоставлять вам качественные материалы.

Часть I

ОСНОВЫ

Суперпозиция, запутанность и обратимость

Что такое квантовый компьютер? Ответ на этот вопрос охватывает квантовую механику (quantum mechanics, QM), квантовую теорию информации (quantum information theory, QIT) и компьютерные науки (computer science, CS).

Для наших целей мы сосредоточим внимание на том, что отличает квантовый компьютер от классических компьютеров.

1.1 Определение квантового компьютера

Квантовый компьютер – это устройство, которое использует для выполнения вычислений определенные свойства, описанные квантовой механикой.

Каждый классический (то есть не квантовый) компьютер может быть описан квантовой механикой, поскольку квантовая механика является основой физической вселенной. Однако классический компьютер не использует преимущества специфических свойств и состояний, которые позволяют квантовой механике выполнять вычисления.

Чтобы вникнуть в специфические свойства, которые мы используем в квантовых компьютерах, давайте сначала обсудим несколько ключевых концепций квантовой механики:

- Как мы представляем суперпозицию состояний в квантовой системе?
- Что такое запутанность?
- Какая связь между обратимостью, вычислением и физическими системами?

Мы будем широко использовать нотацию Дирака, линейную алгебру и другие математические инструменты; читателям предлагается по мере необходимости обращаться к математическим главам в данной книге.

Согласно принципам квантовой механики, системы переходят в определенное состояние только после измерения. Перед измерением системы находятся в неопределенном состоянии; после того как мы их измерим, они находятся в определенном состоянии. Если у нас есть система, которая может принимать одно из двух дискретных состояний при измерении, мы можем представить эти два состояния в обозначениях Дирака как $|0\rangle$ и $|1\rangle$. Затем мы можем представить суперпозицию состояний как их линейную комбинацию, например

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle.$$

1.2 Принцип суперпозиции

Линейная комбинация двух или более векторов состояния является другим вектором состояния в том же гильбертовом пространстве^a и описывает другое состояние системы.

^a См. часть III, где рассматриваются гильбертовы пространства.

В качестве примера рассмотрим свойство света, иллюстрирующее суперпозицию состояний. Свет имеет внутреннее свойство, называемое *поляризацией*, которое мы можем использовать для иллюстрации суперпозиции состояний. Практически весь свет, который мы видим в повседневной жизни, например свет солнца, не имеет предпочтительного направления поляризации. Состояния поляризации могут быть выбраны с помощью *поляризационного фильтра*, тонкой пленки с осью, которая пропускает только свет с поляризацией, параллельной этой оси.

С одним поляризационным фильтром мы можем выбрать одну поляризацию света, например *вертикальную поляризацию*, которую можем обозначить как $|\uparrow\rangle$. *Горизонтальная поляризация*, которую мы можем обозначить как $|\rightarrow\rangle$, является ортогональным состоянием по отношению к *вертикальной поляризации*¹. Вместе эти состояния составляют основу любой поляризации света. То есть любое состояние поляризации $|\psi\rangle$ можно записать как линейную комбинацию этих состояний. Мы используем греческую букву ψ для обозначения состояния системы.

$$|\psi\rangle = \alpha|\uparrow\rangle + \beta|\rightarrow\rangle.$$

Коэффициенты α и β – это комплексные числа, известные как *амплитуды*. Коэффициент α связан с вертикальной поляризацией, а коэффициент β

¹ Мы могли в равной степени использовать $|0\rangle$ и $|1\rangle$ для обозначения двух состояний поляризации; символы, используемые в кетах (векторах состояния), произвольны.

связан с горизонтальной поляризацией. У них есть важная интерпретация в квантовой механике, которую мы вскоре увидим.

После выбора вертикальной поляризации с помощью поляризационного фильтра мы можем затем ввести второй поляризационный фильтр после первого.

Представьте, что мы сориентировали ось второго фильтра перпендикулярно оси первого. Увидим ли мы, что свет проходит через второй фильтр?

Если вы ответите на этот вопрос «нет», вы будете правы. Горизонтальное состояние второго фильтра $|\rightarrow\rangle$ ортогонально первому, поэтому после первого вертикального фильтра нет никакой горизонтальной поляризации.

Предположим, что теперь мы сориентировали ось второго поляризационного фильтра под углом 45° по отношению к первому (т. е. вдоль диагонали \nearrow между вертикалью \uparrow и горизонталью \rightarrow , а не горизонтали). Теперь мы задаем тот же вопрос: увидим ли мы, что свет проходит через второй фильтр?

Если вы ответили «нет» на этот вопрос, вы можете быть удивлены, обнаружив, что ответ «да». Фактически мы бы увидели, как некоторое количество света проходит через второй фильтр. Как это могло быть, если весь свет после первого фильтра имел вертикальную поляризацию? Причина в том, что мы можем выразить вертикальную поляризацию как *суперпозицию* диагональных компонентов. То есть, позволяя $|\nearrow\rangle$ обозначать поляризацию 45° и $|\nwarrow\rangle$ обозначать поляризацию -45° , мы можем написать

$$|\uparrow\rangle = \frac{1}{\sqrt{2}}|\nearrow\rangle + \frac{1}{\sqrt{2}}|\nwarrow\rangle.$$

Как подсказывает геометрическая интуиция, вертикальное состояние состоит из равных частей $|\nearrow\rangle$ и $|\nwarrow\rangle$.

Именно по этой причине мы видим, что некоторое количество света проходит через второй фильтр. То есть вертикальную поляризацию можно записать как *суперпозицию* состояний, одним из которых является именно 45° -градусное диагональное состояние $|\nearrow\rangle$, которое мы пропускаем через второй фильтр. Поскольку состояние $|\nwarrow\rangle$ – это только один член в суперпозиции, не весь свет проходит через фильтр, но некоторые проходят. В данном случае передается ровно $\frac{1}{2}$. (Более формально, интенсивность проходящего света равна $\frac{1}{2}$ интенсивности падающего света.) Это значение определяется из амплитуд состояния суперпозиции по закону, известному как правило Борна, которое мы сейчас обсудим.

Макс Борн (Max Born) продемонстрировал в своей статье 1926 года, что **квадрат модуля амплитуды состояния – это вероятность того, что результирующее состояние наступит после измерения** [38]. В таком случае, поскольку амплитуда равна $\frac{1}{\sqrt{2}}$, вероятность достижения этого

состояния равна $\left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$. Таким образом, вероятность измерения света в состоянии вертикальной или горизонтальной поляризации составляет

50 %. Обратите внимание, что мы выбрали амплитуду $\frac{1}{\sqrt{2}}$, чтобы нормализовать состояния так, дабы сумма модуля в квадрате амплитуд была равна единице; это позволяет нам с помощью правила Борна связать амплитуды с вероятностями измерения.

1.3 Правило Борна

В суперпозиции состояний квадрат модуля амплитуды состояния представляет собой вероятность того, что состояние возникнет после измерения. Кроме того, сумма квадратов амплитуд всех возможных состояний в суперпозиции равна 1. Итак, для состояния $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ имеем:

$$|\alpha|^2 + |\beta|^2 = 1.$$

В то время как в приведенном выше примере поляризации мы имеем разделение вероятностей 50/50 для каждого из двух состояний, если мы исследуем какую-либо другую физическую систему, она может иметь разделение 75/25 или какое-то другое распределение вероятностей. Одно важное различие между классической и квантовой механикой состоит в том, что амплитуды (*не вероятности*) могут быть комплексными числами.

Другими словами, коэффициенты α и β , которые появляются в формулировке правила Борна, могут быть комплексными числами, такими как $i = \sqrt{-1}$ или $(1 + i)/\sqrt{2}$. Только после того, как мы возьмем квадрат модуля этих амплитуд, мы получим действительные числа, а следовательно, и фактические вероятности. Обратитесь к главе 11, чтобы узнать о комплексных числах и о том, как определить квадрат модуля комплексного числа.

Как будто, чтобы квантовая суперпозиция была недостаточно странной, квантовая механика описывает особый вид суперпозиции, который еще больше поражает наше воображение: *запутанность*. В 1935 году, когда Эйнштейн (Einstein) работал с Подольским (Podolsky) и Розеном (Rosen) над публикацией их совместной статьи о квантовой запутанности [75], их целью была атака на квантовую механику (эта статья теперь известна как EPR). Несмотря на то что Эйнштейн получил Нобелевскую премию за свою работу 1905 года о квантовой природе фотоэлектрического эффекта, он тем не менее до последних лет выступал против положений квантовой механики.

Эйнштейн писал в 1952 году, что квантовая механика кажется ему «системой заблуждений чрезвычайно умного параноика, состряпанной из бессвязных элементов мысли» [74]. Он надеялся, что статья EPR продемонстрирует то, что, он полагал, является недостатками квантовой механики.

Статья EPR показала, что если вы возьмете две запутанные друг с другом частицы и затем измерите одну из них, то это автоматически вызовет коррелированное состояние второй частицы – даже если эти две частицы

находятся на большом расстоянии друг от друга; это, казалось, был тот нелогичный результат, который давал надежду использовать публикацию в EPR, чтобы показать, что сама по себе квантовая механика должна иметь недостатки. По иронии судьбы, мы теперь считаем запутанность краеугольным камнем квантовой механики. Запутанность возникает, когда у нас есть неразрывная суперпозиция состояний. Позже мы дадим в книге более формальный контекст этого.

Это «жуткое действие на расстоянии», похоже, противоречит нашей интуиции и предыдущей физике. Подольский, самый молодой из соавторов, как сообщалось, передал информацию о такой точке зрения Эйнштейна газете «Нью-Йорк таймс», чтобы привлечь внимание общественности к его атаке на сущность квантовой механики. Газета поместила на первой полосе номера от 4 мая 1935 года статью под заголовком «Эйнштейн атакует квантовую теорию».

Запутанность принята не только как часть стандартной квантовой механики. Позже мы увидим, что можем использовать запутанность как средство для выполнения новых типов вычислений и коммуникации. С теоретико-информационной точки зрения запутанность – это другой способ кодирования информации. Если у нас есть две запутанные частицы, информация о них не кодируется локально в каждой частице, а скорее в их корреляции.

Джон Прескилл (John Preskill) любит проводить аналогию с двумя видами книг: незапутанными и запутанными [176]. В обычной, незапутанной книге мы можем читать информацию на каждой странице, как обычно. Однако в запутанной книге каждая страница содержит то, что кажется тарбарщиной. Информация закодирована в соотношении страниц, а не на каждой отдельной странице. Это отражает то, что Шредингер (Schrödinger) выразил, когда он ввел термин запутанность:

Другой способ выразить особую ситуацию: наилучшее возможное знание целого не обязательно включает наилучшее возможное знание всех его частей [196].

Шредингер далее отмечал, что, по его мнению, запутанность была не просто *одним из явлений*, описываемых квантовой механикой, «но скорее является *характерной чертой* квантовой механики, которая полностью меняет классический образ мыслей» [196].

1.4 Запутывание

Две системы находятся в специальном случае квантово-механической суперпозиции, называемой *запутанностью*, если измерение одной системы коррелирует с состоянием другой системы более сильным образом, чем корреляции в классическом случае. Другими словами, состояния двух систем *неразделимы*. Мы исследуем точные математические определения разделимости и запутанности позже в этой книге.

Теперь, когда мы рассмотрели две основные идеи квантовой механики – суперпозицию и запутанность, – давайте обратимся к другой фундаментальной концепции, которая не так часто рассматривается, – физическому представлению информации. Рольф Ландауэр (Rolf Landauer) открыл новое направление исследований, задав следующий вопрос:

Поиск более быстрых и более компактных вычислительных схем приводит непосредственно к вопросу: каковы основные физические ограничения прогресса в этом направлении? ... Мы можем показать или, по крайней мере, убедительно предположить, что обработка информации неизбежно сопровождается определенным минимальным выделением тепла [128].

Другими словами, существует ли нижняя граница для энергии, рассеиваемой в процессе базовой единицы вычисления? Благодаря Ландауэру и другим исследователям мы теперь считаем, что такой предел существует; это называется границей Ландауэра (Landauer's bound, LB). Более конкретно, затраты энергии на стирание n бит равны $nkT \ln 2$, где k – постоянная Больцмана, T – температура в кельвинах радиатора, окружающего вычислительное устройство, а $\ln 2$ – это натуральный логарифм 2 (≈ 0.69315). Этот предел представляет собой минимальное количество энергии, рассеиваемой для необратимых вычислений.

Ландауэр признал, что этот минимум не обязательно является ограничивающим фактором для энергопотребления системы:

Конечно, очевидно, что и тепловой шум, и требования к рассеянию энергии находятся в масштабе, которым в настоящее время можно пренебречь для современных компьютерных компонентов. Однако расчетное рассеяние является абсолютным минимумом [128].

Ландауэр определил логическую необратимость как состояние, при котором «выход устройства не определяет однозначно входы». Затем он заявил, что «логическая необратимость ... в свою очередь, подразумевает физическую необратимость, а последняя сопровождается диссипативными эффектами». Это следует из второго закона термодинамики, который гласит, что полная энтропия системы не может уменьшаться и, точнее говоря, должна увеличиваться в результате необратимого процесса.

Дополнительные сведения об обратимости, термодинамике и вычислениях см.: *Лекции Фейнмана по вычислениям* [Feynman's Lectures on Computation, 84].

В классических вычислениях мы используем необратимые вычисления. Например, логический элемент включающего ИЛИ (OR, обозначается \vee) имеет следующую таблицу истинности, где 0 означает «ложь», а 1 – «истина»:

X	Y	$X \vee Y$
0	0	0
0	1	1
1	0	1
1	1	1

Обратите внимание, что выход значения 1 не может быть однозначно определен для набора входов. Мы можем получить этот результат с помощью комбинации входов; состояние входов теряется, когда мы переходим к выходу. Это не нарушает сохранения информации, потому что информация была преобразована в рассеиваемое тепло.

Исключающее ИЛИ так же необратимо, как и вентиль НЕ-И (NAND), универсальный для классических вычислений. NAND означает «НЕ И» и является обратным логическому оператору И. Убедитесь сами в необратимости NAND, изучив его таблицу истинности:

X	Y	$X \uparrow Y$
0	0	1
0	1	1
1	0	1
1	1	0

В квантовых вычислениях мы ограничиваемся обратимыми логическими операциями [161, с. 29]. Далее в этой книге мы рассмотрим, какие комбинации квантовых операторов универсальны. А пока давайте сосредоточимся на требовании в квантовых вычислениях ограничить наш набор операторов обратимыми вентилями.

Это требование проистекает из природы необратимых операций: если мы выполняем необратимую операцию, то теряем информацию и, следовательно, измерения. В таком случае наш вычислительный цикл будет завершен, и мы больше не сможем продолжать нашу программу. Ограничивая вместо этого все шлюзы обратимыми операторами, мы можем продолжить применять операторы к нашему набору кубитов, пока можем поддерживать согласованность в системе. Когда мы говорим «обратимый», то подразумеваем теоретический бесшумный квантовый компьютер. В шумном квантовом компьютере (QC), который декогерирует, мы, конечно, не можем обратить операцию.

1.5 Обратимость квантовых вычислений

Все операторы, используемые в квантовых вычислениях, кроме измерений, должны быть обратимыми. В этой главе мы рассмотрели четыре основных принципа квантово-механических систем: суперпозицию, правило Борна, запутанность и обратимые вычисления. Как мы увидим далее в книге, все четыре необходимы для понимания разницы между классическими и квантовыми вычислениями. На веб-сайте этой книги мы даем ссылки на ряд ресурсов для тех, кто хочет углубить свое понимание квантовой механики.