

Содержание

Об авторе.....	12
Благодарности	13
Предисловие.....	15
I Учебник по квантовым вычислениям.....	21
1 Введение в квантовую механику.....	22
Что такое квантовая механика?	22
Квант противоречит интуиции	23
Квантовая механика реальна	24
Основные свойства квантовой механики	27
Фотоны и квантовая механика.....	28
Фотоэлектрический эффект	28
Двойственность волна – частица	29
Принцип вероятности	34
Принцип неопределенности	38
Спиновые состояния и заряды	40
Квантовое туннелирование	41
Суперпозиция.....	42
Эффект наблюдателя.....	44
Теорема об отсутствии клонирования	45
Жуткая запутанность.....	46
Декогеренция	47
Квантовые примеры в современном мире.....	49
Для дополнительной информации.....	50
Резюме	51
2 Введение в квантовые компьютеры	52
В чем отличие квантовых компьютеров?	52
Традиционные компьютеры используют биты	52
Квантовые компьютеры используют кубиты.....	55
Квантовые компьютеры еще не готовы к прайм-тайму.....	59
Квант скоро будет царствовать.....	60
Квантовые компьютеры улучшают кубиты, используя исправление ошибок.....	61
Типы квантовых компьютеров	67

Сверхпроводящие квантовые компьютеры.....	68
Квантовые компьютеры на основе алгоритма отжига	69
Универсальные квантовые компьютеры	71
Топологические квантовые компьютеры	73
Компьютеры Majorana Fermion компании Microsoft.....	74
Квантовые компьютеры с ионными ловушками.....	75
Квантовые компьютеры в облаке	77
Квантовые компьютеры не США.....	78
Компоненты квантового компьютера	79
Квантовое программное обеспечение	80
Квантовый стек	81
Национальное руководство	81
Руководство национальной политикой	81
Денежные гранты и инвестиции.....	82
Другая квантовая научная информация.....	82
Чтобы получить больше информации	83
Резюме	83
3 Как квантовые вычисления могут взломать существующие криптокоды	85
Основы криптографии.....	85
Шифрование	86
Целостность хеширования	100
Применение криптографии.....	101
Как квантовые компьютеры могут взломать криптокоды	102
Сокращение времени.....	102
Квантовые алгоритмы.....	104
Что квант может и что не может сломать.....	108
Все еще теория	112
Резюме	113
4 Когда случится криптопрорыв?.....	114
Это было всегда «лет через 10»	114
Факторы квантового криптопрорыва	115
Квантовая механика реальна?	115
Квантовые компьютеры реальны?.....	116
Суперпозиция реальна?.....	117
Реален ли алгоритм Питера Шора?.....	117
Достаточно ли у нас стабильных кубитов?.....	117
Квантовые ресурсы и конкуренция	118
У нас есть постоянное улучшение?.....	119
Мнения экспертов.....	120
Когда случится квантовый киберпрорыв	120
Временные сценарии.....	120
Когда следует быть готовыми?	123
Сценарии криптопрорыва	125

Длительное время останется в распоряжении национальных государств	126
Применение крупнейшими компаниями	127
Массовое распространение	128
Наиболее вероятный сценарий прорыва	128
Резюме	129
5 Каким будет постквантовый мир?	130
Взломанные приложения	130
Ослабленные хеши и симметричные шифры	131
Взломанные асимметричные шифры	134
Ослабленные и взломанные генераторы случайных чисел	135
Слабые, или взломанные, зависимые приложения	136
Квантовые вычисления	147
Квантовые компьютеры	147
Квантовые процессоры	149
Квантовые облачные вычисления	150
Будет использоваться квантовая криптография	150
Квантовая идеальная конфиденциальность	150
Появляется квантовая сеть	151
Квантовые приложения	152
Улучшение химикатов и лекарств	152
Лучшие аккумуляторы электроэнергии	153
Настоящий искусственный интеллект	154
Управление цепочками поставок	155
Квантовые финансы	155
Улучшенное управление рисками	156
Квантовый маркетинг	156
Улучшение прогноза погоды	156
Квантовые деньги	156
Квантовое моделирование	157
Более совершенное вооружение и точное оружие	157
Квантовая телепортация	157
Резюме	162
II Подготовка к квантовому взрыву	163
6 Квантовоустойчивая криптография	164
Постквантовый конкурс NIST	164
Классификация уровня безопасности	167
PKE против KEM	169
Формальные гарантии неразличимости	169
Размеры ключа и зашифрованного текста	171
Типы постквантовых алгоритмов	172
Криптография на основе кода	172
Криптография на основе хеша	173
Решетчатая криптография	175

Многомерная криптография	177
Криптография изогенной суперсингулярной эллиптической кривой	177
Доказательство нулевого знания	178
Квантовая устойчивость симметричного ключа	180
Квантовоустойчивые асимметричные шифры	181
BIKE.....	182
Classic McEliece.....	183
CRYSTALS-Kyber.....	184
FrodoKEM	184
HQC.....	185
LAC.....	186
LEDACrypt.....	187
NewHope.....	187
NTRU	188
NTRU Prime.....	188
NTS-KEM.....	189
ROLLO.....	189
Round5	190
RQC.....	190
SABER.....	191
SIKE.....	191
ThreeBears.....	192
Общие замечания по размерам ключей PKE, KEM и шифротекста.....	194
Квантовоустойчивые схемы цифровой подписи	195
CRYSTALS-Dilithium.....	196
FALCON.....	197
GeMSS.....	198
LUOV.....	198
MQDSS	199
Picnic	199
qTESLA.....	200
Rainbow.....	201
SPHINCS+	201
Общие замечания о ключе и размерах подписи	204
Рекомендуемые предостережения	204
Недостаток стандартов.....	205
Проблемы производительности	206
Отсутствие проверенной защиты.....	206
Для дополнительной информации.....	207
Резюме	207
7 Квантовая криптография.....	208
Квантовые RNG.....	209
Случайное не всегда случайное	209
Почему истинная случайность так важна?.....	211
Квантовые RNG.....	213

Квантовые хеши и подписи	219
Квантовые хеши	219
Квантовые цифровые подписи	221
Квантовые шифры.....	223
Распределение квантовых ключей.....	224
Резюме	231
8 Квантовые сети.....	233
Компоненты квантовой сети.....	233
Среда передачи	233
Расстояние против скорости	235
Точка–точка.....	236
Доверенные повторители.....	237
Квантовые повторители.....	239
Квантовые сетевые протоколы	241
Квантовые сетевые приложения.....	244
Более безопасные сети	245
Облако квантовых вычислений	245
Лучшая временная синхронизация.....	245
Предотвращение помех.....	247
Квантовый интернет.....	248
Другие квантовые сети	248
Где получить больше информации.....	250
Резюме	250
9 Готовимся сейчас	251
Четыре основных этапа смягчения последствий постквантового прорыва.....	251
Этап 1. Укрепление существующих решений.....	251
Этап 2. Переход к квантоустойчивым решениям.....	255
Этап 3. Применение квантово-гибридных решений.....	258
Этап 4. Применение полностью квантовых решений.....	259
Шесть основных шагов проекта смягчения последствий постквантового прорыва.....	260
Шаг 1. Обучение	261
Шаг 2. Создание плана.....	265
Шаг 3. Сбор данных.....	270
Шаг 4. Анализ.....	272
Шаг 5. Принять меры/исправить.....	274
Шаг 6. Обзор и улучшение	276
Резюме	276
Приложение. Дополнительные источники по квантам	278
Именной указатель.....	285
Предметный указатель.....	286

Об авторе

Роджер А. Граймс боролся со злонамеренными компьютерными хакерами более трех десятилетий (с 1987 года). Он получил десятки компьютерных сертификатов (включая CISSP, CISA, MCSE, CEH и Security+) и даже сдал очень жесткий экзамен на сертифицированного общественного бухгалтера (Certified Public Accountant, CPA), хотя это не имеет никакого отношения к компьютерной безопасности, и он худший когда-либо существовавший бухгалтер. Ему платили как профессиональному тестировщику компьютерной безопасности компании и их веб-сайтов более 20 лет, и это никогда не занимало у него более трех часов. Он создал и обновил классы компьютерной безопасности, был инструктором и учил тысячи студентов, как взламывать криптокоды или защищать. Роджер – частый докладчик на национальных конференциях по компьютерной безопасности. Он ранее написал сам или в соавторстве десять книг по компьютерной безопасности и более тысячи журнальных статей. Он был обозревателем компьютерной безопасности в журналах InfoWorld и CSO (www.infoworld.com/blog/security-adviser/) с августа 2005 года и более двух десятилетий продолжает работать консультантом по компьютерной безопасности. У Роджера часто берут интервью журналы и телевизионные шоу, а также радио, в том числе журнал Newsweek и NPR's All Things Considered. В настоящее время Роджер консультирует большие и малые компании по всему миру, как остановить злоумышленников и вредоносные программы в кратчайшие сроки и наиболее эффективным способом. Он следит за литературой и изучает квантовую физику с 1983 года.

Вы можете связаться и узнать больше от Роджера по адресу:

- E-mail: roger@banneretcs.com
- LinkedIn: www.linkedin.com/in/rogeragrimes/
- Twitter: [@rogeragrimes](https://twitter.com/rogeragrimes)
- CSOnline: www.csonline.com/author/Roger-A.-Grimes/

Предисловие

В конце 1990-х годов мир был озадачен компьютерной проблемой, известной под аббревиатурой Y2K, которую предстояло решить с наступлением грядущего 2000 года. Она заключалась в том, что к этому моменту большинство устройств, компьютеров и программ в мире записывали даты с использованием только двух последних цифр года и потому на программном уровне разницы между 1850, 1950 и 2050 годами для них не существовало. Когда 1999 год превратился в 2000-й, многие из этих компьютеров и программ не могли правильно обрабатывать данные с использованием двузначных дат в новом столетии, и было известно много предстоящих возможных отказов программ и устройств, которые уже использовали даты в будущем (например, программ планирования и гарантий). Симптомы неисправных устройств и программ варьировались от заметных ошибок до ошибок, наличие которых было непросто обнаружить (что может быть чрезвычайно опасным), и полной неработоспособности устройств и программ.

Трудность заключалась и в том, что хотя было известно, что значительный процент устройств и программ подвержены влиянию этой проблемы, никто не знал, что оставалось правильными и не требовало обновления, а что необходимо было обновить или заменить до 1 января 2000 года. Было два-три года, чтобы найти, что необходимо исправить, а что нет. Как и при многих медленно, но неизбежно надвигающихся катастрофах глобального масштаба, большинство в мире до последних нескольких месяцев мало что делало, чтобы быть готовым противостоять этой проблеме. Запоздалые усилия по противостоянию тому, что произойдет, когда часы переместятся в новый век, вызвали в мире накануне этой даты некоторую панику. В 1999 году даже был создан фантастически плохой фильм-катастрофа (www.imdb.com/title/tt0215370), в котором показаны падающие с неба самолеты и другой предстоящий всемирный хаос.

В конце концов, едва ли кто-либо хотел, чтобы с приходом Y2K настоящая жизнь была похожа на кино. Проблемы были, но по большей части мир продолжал жить обычной жизнью. Были устройства и программы, которые не могли обработать новые даты должным образом, но большинство основных систем работали правильно. Не было ни падающих самолетов, ни пожаров, ни прорванных дамб. Для многих людей, ожидавших катастрофы, результаты были несколько разочаровывающими, причем настолько, что со временем термин «Y2K» превратился в неофициальный синоним чрезмерно раскрученных событий, связанных с преждевременной паникой при незначительном ущербе.

Большинство людей сегодня не осознают, что катастрофический Y2K был разочаровывающим именно потому, что у нас были годы для подготовки и предупреждения последствий. Большинство основных систем были про-

верены на наличие проблем 2000 года, и по мере необходимости они были заменены или обновлены. Если бы мир не осознал проблемы Y2K и вообще ничего бы не сделал, ее последствия наверняка были бы намного, намного хуже (хотя я все же не уверен, что самолеты стали бы падать). Y2K не стал преждевременной паникой. Он стал предсказуемым результатом многолетней подготовки, демонстрирующей успех того, что человечество может сделать, столкнувшись с надвигающейся цифровой проблемой.

Грядущий квантовый судный день

Большая часть мира этого еще не осознает, но мы приближаемся к еще более весоному, по сравнению с Y2K, моменту, который, вероятно, уже и теперь вызывает серьезные проблемы и наносит ущерб. Хуже того, мы не можем исключить весь ущерб, даже если начнем готовиться заранее. Сегодня существуют организации, уже наносящие вред программам, избежать которого системы не могут. Национальные государства и корпоративные противники, вероятно, уже извлекают для себя преимущества из этого обстоятельства.

Квантовые компьютеры, вероятно, в ближайшем будущем взломают традиционные криптокоды с открытым ключом, включая шифры, защищающие большинство цифровых секретов мира. Эти протоколы и компоненты включают HTTPS, TLS, SSH, PKI, цифровые сертификаты, RSA, DH, ECC, большинство сетей Wi-Fi, многие сети VPN, смарт-карт, HSM, большинство криптовалют и большинство устройств многофакторной аутентификации, которые полагаются на криптографию с открытым ключом. Даже если бы список включал только HTTPS и TLS, то он уже охватывал бы большую часть интернета. В тот день, когда квантовые вычисления нарушат традиционную публичную криптографию, все секреты, защищенные этими протоколами и механизмами, будут читабельны.

Еще более важно, что любой, кто сейчас перехватит и сохранит эти защищенные в настоящее время секреты, после квантового криптографического взлома будет иметь возможность вернуться и раскрыть секреты. Сколько секретов есть у вас или вашей организации, которые вы хотите, чтобы кто-то открыл через несколько лет? Это новая проблема Y2K, с которой мы имеем дело уже сегодня.

Есть много выполнимых решений, которые можно реализовать сегодня, хотя некоторые из них либо выходят за рамки имеющихся возможностей средней компании, либо, если их преждевременно реализовать, могут привести к значительным нарушениям ведущихся работ. Подготовка к грядущему квантовому взрыву требует образования, критичного выбора и планирования. Люди и организации, которые четко понимают, что нас ждет впереди, могут предпринять правильные шаги уже сейчас, чтобы быть как можно более подготовленными. Они могут остановить сегодня необоснованное подслушивание и начать переводить свои управляемые активы в более устойчивую среду. Данная книга содержит необходимые для этого знания и дает вам план, помогающий минимизировать риски вашей организации от прихода квантового криптовзлома. Если достаточное количество организаций бу-

дут готовиться к этому уже сейчас, мы можем избежать квантовых проблем и сделать их столь же малосущественными, как это было с проблемой Y2K.

Для кого эта книга

Эта книга в первую очередь предназначена для тех, кто отвечает за управление безопасностью компьютерной техники своей организации и, в частности, компьютерную криптографию. Это люди, которые, разрабатывая проекты, будут отвечать на вызовы постквантовой миграции. Эта книга также для менеджеров и других лидеров, понимающих важность хорошей криптографии и ее влияние на их организацию. Наконец, любой, интересующийся квантовой механикой, квантовыми компьютерами и квантовой криптографией, найдет в ней много новых фактов, делающих эту книгу достойной прочтения.

Что вы найдете в этой книге

Книга «Апокалипсис криптографии» подготавливает читателя к квантовому прорыву в вычислениях. Она состоит из девяти глав, разделенных на две части.

Часть I «Учебник по квантовым вычислениям» – это базовый учебник по квантовой механике и вычислениям, рассказывающий о том, как можно взломать сегодняшнюю криптографическую защиту.

Глава 1 «Введение в квантовую механику»

Если вы не понимали квантовую механику, читая о ней впервые, не расстраивайтесь – квантовая механика досаждала самым блестящим умам, которые наша планета имела когда-либо в последнее столетие. Нас, простых смертных, можно простить за то, что мы сразу не поняли ее основные идеи. Глава 1 объясняет свойства, наиболее важные для понимания того, как квантовая механика влияет на наш цифровой мир. Если я проделал свою работу хорошо и правильно, вы поймете это лучше, чем 99 % кого-либо еще в этом компьютерном мире.

Глава 2 «Введение в квантовые компьютеры»

Квантовые компьютеры используют квантовые свойства и обеспечивают возможности, логические и арифметические результаты, которых просто невозможно достигнуть с помощью традиционных бинарных компьютеров. Глава 2 охватывает различные типы квантовых компьютеров, которые, скорее всего, станут окружать нас в следующем десятилетии и будут поддерживать различные квантовые свойства.

Глава 3 «Как квантовые вычисления могут взломать сегодняшние криптокоды?»

Наиболее распространенный вопрос, который задают, когда человеку говорят, что квантовые компьютеры, вероятно, взломают традиционные криптокоды с открытым ключом, – каким образом? В главе 3 рассказы-

вается, почему традиционным бинарным компьютерам нелегко взломать большинство шифров с открытым ключом и как квантовые компьютеры, вероятно, смогут достаточно просто это сделать. Здесь показано, что квантовые компьютеры, скорее всего, будут иметь возможность взломать, а также что будет устойчивым к квантовым вычислительным мощностям.

Глава 4 «Когда произойдет квантовый взлом криптокодов?»

После объяснения того, как квантовые компьютеры могут сломать традиционные криптокоды с открытым ключом, вторым наиболее часто задаваемым вопросом является вопрос, когда это произойдет. Хотя этого никто (достоверно) не знает, это, вероятно, произойдет скорее раньше, чем позже. В главе 4 обсуждаются различные возможные сроки и их вероятность.

Глава 5 «Как будет выглядеть постквантовый мир?»

Как и изобретение интернета, будет мир до и мир после квантового доминирования. Квант решит проблемы, которые мучили нас на протяжении веков, и даст нам новые проблемы, и это в будущем будет раздражать нас. Глава 5 опишет этот постквантовый мир и как он будет влиять на нас.

Часть II «Подготовка к квантовому прорыву» поможет вам и вашей организации наиболее эффективно подготовиться к грядущему квантовому доминированию.

Глава 6 «Традиционная квантовая криптография»

Глава 6 охватывает более двух десятков квантовоустойчивых шифров и схем, которые Национальный институт стандартов и технологий (NIST) рассматривает во втором раунде своего постквантового конкурса. Два или более из этих квантовоустойчивых алгоритмов станут следующими национальными стандартами криптографии. Вы узнаете о конкурентах, их сильных и слабых сторонах.

Глава 7 «Квантовая криптография»

Глава 7 посвящена традиционной бинарной квантовоустойчивой криптографии, которая не использует квантовые защитные свойства. Глава 7 охватывает шифры и схемы, которые квантовые свойства используют, чтобы обеспечить их криптографическую устойчивость. В долгосрочной перспективе вы, вероятно, будете использовать криптографию на основе квантов, а не только квантовоустойчивую криптографию. Узнайте, как это выглядит.

Глава 8 «Квантовые сети»

Глава 8 охватывает квантовые сетевые устройства, такие как квантовые повторители и приложения, которые ищут квантовую защиту сети. Она охватывает текущее состояние квантовых сетей и как это, вероятно, будет выглядеть в ближайшем и долгосрочном будущем. Однажды весь интернет, скорее всего, будет основан на квантах. Читайте о таких сетях и их компонентах и о том, как мы к ним придем.

Глава 9 «Готовимся сейчас»

Глава 9 является идеальной причиной для покупки этой книги. Она сообщает любой организации, как уже сегодня они могут начать подготовку к грядущему квантовому криптографическому взрыву. Она рассказывает вам, что вы можете сделать сегодня, чтобы защитить ваши наиболее важные долгосрочные секреты, какие размеры криптографических ключей вам нужно увеличить, что и когда должно быть заменено. Обобщенный план, применявшийся ранее для глобальных обновлений криптографии, может быть использован и для преодоления апокалипсиса криптографии.

В приложении перечислены десятки ссылок на квантовые информационные ресурсы, в том числе книги, видео, блоги, официальные документы и веб-сайты.

Если я хорошо справился со своей работой, к концу этой книги вы лучше, чем прежде, поймете квантовую физику, поймете, как она ломает сегодняшнюю традиционную криптографию с открытым ключом, и будете в состоянии надлежащим образом подготовить и лучше защитить ваши важные цифровые секреты.

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.

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 – возможно, ошибку в основном тексте или программном коде, – мы будем очень благодарны, если вы сообщите нам о ней. Сделав это, вы избавите других читателей от недопонимания и поможете нам улучшить последующие издания этой книги.

Если вы найдете какие-либо ошибки в тексте, пожалуйста, сообщите о них главному редактору по адресу dmkpress@gmail.com, и мы исправим это в следующих тиражах.

Нарушение авторских прав

Пиратство в интернете по-прежнему остается насущной проблемой. Издательства «ДМК Пресс» и Wiley 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.



Учебник по КВАНТОВЫМ ВЫЧИСЛЕНИЯМ

- Глава 1 Что такое квант?
- Глава 2 Квантовый компьютер
- Глава 3 Как квантовые вычисления могут взломать сегодняшние криптокоды
- Глава 4 Когда произойдет квантовый взлом криптокодов?
- Глава 5 Как будет выглядеть постквантовый мир?

1

Введение в квантовую механику

Ничего удивительного в том, что те, кто впервые встречается с квантовой механикой, возможно, не могут понять ее.

*– Нильс Бор, квантовый физик
и лауреат Нобелевской премии 1922 года*

Любая достаточно развитая технология неотличима от магии.

– Артур Чарльз Кларк, писатель-фантаст

В главе 1 будут обсуждаться основы квантовой механики, особенно аспектов, касающихся квантовых вычислений. Данная глава намеренно не будет полностью охватывать все аспекты, поскольку для этого потребовалась бы книга, а не просто глава на эту тему. Не будет описана каждая частица, ее свойства или возможное взаимодействие, и будут опущены все сложные математические уравнения. Эта глава даст вам понимание квантовой физики, достаточное, чтобы объяснить, как квантовые компьютеры способны быстро решать считавшиеся ранее не решаемыми математические задачи, на которых основаны многие распространенные, обеспечивающие защиту, типы шифрования. Понимание квантовой механики и квантовых вычислений совершенно не требуется для подготовки к грядущей эпохе криптографических взломов, но оно поможет вам иметь некоторые базовые основы для обсуждения соответствующих проблем.

Что такое квантовая механика?

В этом разделе я буду объяснять квантовую механику, но если это ваша первая встреча с этой темой, отнеситесь к ней с некоторой осторожностью. Квантовая механика невероятно крута, и иногда мы не способны полностью понять, что происходит. Многие в ней кажутся таким странным для нашего нынешнего понимания того, как устроен мир, что большинству людей, которые впервые сталкиваются с квантовой механикой, понять ее очень нелегко. Даже после почти 30 лет попыток полностью осознать сущность этой области знаний и ее значение мой мозг психологически все еще не готов к этому. Я не одинок. Приятно снисходительно сказать, что это только на первый взгляд квантовая механика противоречит интуиции и выглядит неестественно, но часто это совсем не так. Это идет вразрез со многим, чему нас учили ранее об устройстве нашего мира и Вселенной. Один плюс: один

не всегда равняется двум. Это идет также вразрез с тем, что мы можем легко увидеть, потрогать и почувствовать, хотя вся наша реальность возможна именно благодаря этому.

Хотя лучшие умы нашей цивилизации неоднократно доказывали, что в существовании квантовой механики нет ни тени сомнения, то, что она влечет за собой, звучит так странно для обычного человека, что часто остается для него невероятным и волшебным. Понимание значения квантовой механики даже впервые ставит вопрос о существовании реальности.

Первый необычный отклик на квантовую теорию заключается в предположении, что все, кто проповедует ее, должно быть, находятся под воздействием какой-то научной фантастики, что это результат массового заблуждения, потому что они говорят то, что не может быть правдой. Или, как однажды сказала мне одна моя подруга, после того как я сделал явно неудачную попытку объяснить ей квантовую механику: «Ты можешь верить во все, что хочешь, но это просто выхлоп быка»... правда, она не произнесла слова *бык*.

Даже Альберт Эйнштейн, который помогал открытию некоторых из наиболее важных принципов, лежащих в основе квантовой механики, не полностью верил в некоторые ее другие принципы. Он потратил десятилетия, пытаясь понять их, и понял их лучше, чем многие другие. Это его глубокое понимание ее основ создавало для него проблемы. Он даже ставил эксперименты, пытаясь доказать или опровергнуть их. Он не мог логически проверить или объяснить многие ее странные свойства и «пугающие на удалении» результаты. После десятилетий ожидания подтверждения своих предположений в результате экспериментов он просто перешел к изучению других научных областей. Видимо, его мозг просто устал постоянно думать об этом. Так что не столь великие умы вполне можно извинить.

С учетом сказанного я написал эту главу учебника по квантовой механике так, как я хотел бы, чтобы это было объяснено мне самому, когда я впервые начал изучать ее. Я надеюсь, что эта глава поможет сократить вам время обучения.

Квант противоречит интуиции

Несмотря на то что квантовая механика лежит в основе всей реальности, она не всегда выглядит такой, какую мы наблюдаем в нашей повседневной жизни. Например, собака одной масти не может быть белой и черной масти в одно и то же время, белая собака, находящаяся в комнате, не становится черной собакой, когда она выходит из нее, и собака не может разделиться на две собаки прямо на ваших глазах, а затем снова слиться воедино. Но на атомном и субатомном уровнях особенности квантовой механики состоят как раз в подобных странностях. Какие же свойства квантов, о которых я говорю, столь странные? Вот некоторые примеры:

- одна квантовая частица может находиться в двух местах и быть одновременно двумя совершенно разными частицами;
- одна квантовая частица может разделиться на две, а затем, позже, столкнуться или смешаться и восстановиться или исчезнуть;

- в реально пустом пространстве, где абсолютно ничего нет (о чем ученым известно), квантовые частицы могут просто появиться «из воздуха» и затем исчезнуть;
- кажется, что квантовая частица ведет себя одним образом, когда ее не измеряют, а другим, будучи измеренной, как будто природа позаботилась о воздействии процедуры измерения. Похоже, это даже изменит ее путь или сделает ее поведение обратным во времени, если вы решите измерить ее после того, как она прошла свой первоначальный путь;
- две квантовые частицы могут быть «спутаны» таким образом, что когда вы меняете одну, другая каждый раз также мгновенно меняется таким же образом, независимо от того, насколько далеко они друг от друга, хоть через вселенную;
- квантовое состояние – это всегда все возможные состояния (называемые суперпозицией состояний), но единственное, конечное состояние с уверенностью предсказано быть не может;
- каждый возможный ответ будет ответом в какой-то момент, хотя каждый из этих ответов может быть из своей отдельной совокупности. Для каждой возможной комбинации на атомном уровне могут быть разные совокупности вариантов ответа – так называемые мультиверсы (multiverses);
- телепортация, подобная показанной в научно-фантастическом сериале «Star Trek» («Звездный путь»), возможна.

Квантовая механика реальна

В «странные» свойства квантовых частиц трудно поверить. Но эти квантовые свойства и результаты не только были проверены и доказаны, но они являются одними из самых проверенных и признанных научных теорий в мире. Они постоянно проверялись и оспаривались. Все эксперименты, которые были проведены, чтобы опровергнуть основные принятые теорией принципы квантовой механики, потерпели неудачу. Многие из неудач, в том числе и Эйнштейна, только в еще большей мере подтверждали квантовую теорию. Большинство Нобелевских премий по физике за последние 75 лет были присуждены ученым, которые улучшили наше понимание квантовой механики. В последние несколько десятилетий интерес к квантовой механике увеличивается, и наше понимание квантовой механики с каждым годом улучшается.

Хотя перечисленные в предыдущем разделе факты могут при первом прочтении показаться невероятными, подлинность квантовой физики оказывается для нас все большей и большей реальностью и становится в один ряд с такими фактами, как тот, что Солнце дает жизнь нашей планете, что любой раскаленный материал дает красное свечение, или фактами существования цифровых камер, оптоволоконных кабелей, лазеров, компьютерных чипов, носителей и коммуникаций интернета. Очень вероятно, что реальность как раз и состоит в том, что каждая составляющая этой реальности основана на квантовой механике.

Квантовая механика дает нам очень мощные компьютеры, которые раньше были немыслимы. Квантовые компьютеры и устройства изменят наш мир

многими невероятными способами, которые мы можем или не можем понять сейчас, так же, как это было для нынешнего поколения с интернетом, USB-накопителями и iPod'ами. Потенциальные квантовые изобретения значительно изменят нашу жизнь к лучшему, и самые важные из них появятся очень скоро.

Интересно, что хотя большая часть квантовой теории была подтверждена повторными наблюдениями, экспериментами и математикой, ученые до сих пор не знают, почему многие квантовые свойства таковы, какие они есть, или почему дают именно такие результаты. Физики-теоретики часто гадают о том, почему квантовая механика такова, какова она есть. Вы можете услышать предположения разного рода, обсуждаемые различные их *интерпретации* или *взгляды*, такие как *копенгагенская интерпретация* или взгляд «Много миров» (рассматривается позже в этой главе в разделе «Эффект наблюдателя»). Существует более десятка интерпретаций, каждая из которых пытается объяснить какую-то часть квантовой механики, даже не зная, точна эта интерпретация или нет.

Важно понимать, что независимо от предположения, почему или как какое-то квантовое действие или его результат происходит, действие или результат действительно происходят и всегда происходят ожидаемым образом, что экспериментально и математически доказано независимо от интерпретации. Никогда не было серьезного квантового предсказания, не подкрепленного достоверными экспериментами. Мы не всегда можем знать, почему поведение квантов – скажем точнее: квантовое действие – таково, но мы знаем, что оно реально происходит. Это может показаться магией, но это реально, даже если мы не можем объяснить это или «увидеть это» в общепринятом смысле.

Это беспокоит некоторых не ученых. Просить их поверить в то, чего они не видят или не чувствуют и что категорически противоречит интуиции и всему тому, чему их учили раньше, требует слишком многого. Это совсем не то, как они раньше привыкли оценивать науку. Например, они могут не понимать высказывания физика и математика относительно гравитации, но они могут «видеть это» и ее результат каждый раз, когда бросают мяч, спотыкаются и падают, смотрят, как яблоки падают с дерева, или наблюдают вращение Луны вокруг Земли. Они могут не понимать математику, но они понимают, как и почему работает гравитация... ну, хорошо, большинство из нас, это так. Многие люди спрашивают, как мы можем верить, что все, о чем говорит наука, существует, не зная, как или почему это произошло. Как мы можем верить во что-то, чего не можем увидеть своими глазами, особенно что-то, что звучит столь невероятно и нелогично?

То, что скептики обычно не знают, – так это то, что большая, если не самая большая часть прогресса в науке в прошлом веке, особенно в физике, и особенно в квантовой физике, почти всегда сначала была обязана доказательствам экспериментами и/или с помощью математики без понимания, почему и как. Много раз ученые, имея только очень смутные теории, для того чтобы поддержать то, что можно было лишь поверхностно наблюдать, сумели доказать математически. Отсюда и появился термин «физик-теоретик». Он часто начинается с реальных событий и поддержки рискованной интеллекту-

альной теории, чтобы объяснить то, что наблюдает. Если он (или кто-то еще) может предоставить математическое уравнение, которое последовательно описывает наблюдаемое явление, то большинство ученых будут полагаться на математику как на убедительное доказательство существования такого поведения или события. Это вовсе не то представление, в которое верит физик. Математика даже важнее, чем это представление или прямое наблюдение физика. Кто-то однажды сказал: «Единственная абсолютная истина в мире – это математика». Имелось в виду, что все остальное, кроме хорошо поддерживаемого математического уравнения, подвержено личным взглядам и интерпретациям. Либо математика поддерживает что-то, либо нет. Либо математика подтверждает что-то, либо нет. Это не предмет мнений наблюдателей. Если ученый видит какое-то необъяснимое ранее явление и может последовательно поддерживать его соответствие математической формуле и если каждый эксперимент подтверждает результат, точно описанный математикой, то научный факт считается доказанным. Математика является доказательством. Прямое, убедительное, подтверждающее наблюдение необязательно.

Неоспоримое наблюдаемое событие, которое большинство не ученых считало бы доказательством, часто происходит спустя десятилетия или даже столетия. Обычно к тому времени вовлеченные ученые и их последователи продолжительное время имели существовавшую до этого теорию, верили в нее и рассматривали событие как достоверный факт, подтвержденный математическим доказательством. В их сознании это последнее неоспоримое, физическое доказательство считается почти ненужной формальностью.

Многие прошлые научные постулаты, как очень маленькие, так и очень большие, включая открытие атомов, электронов и черных дыр, были сначала обнаружены учеными, создающими теории и разрабатывающими математику относительно ранее необъяснимых наблюдаемых явлений. В предыдущих наблюдениях черных дыр и недавно обнаруженных планет Солнечной системы наблюдатели заметили тонкие отклонения в орбитах тел и излучении света, которые, как они понимали, можно было объяснить только неизвестными ранее сторонними эффектами. Теория черных дыр появилась в 1784 году благодаря Джону Митчеллу (John Mitchell) и математически была поддержана общей теорией относительности Эйнштейна в 1915 году. Дальнейшие, в течение следующей половины столетия, связанные с ними наблюдения подтвердили математически и существование черных дыр, даже притом, что их не могли «увидеть». С 1970-х годов ученые воспринимают реальность черных дыр как данность. Первая картина, та, которую многие не ученые могут считать первым «реальным доказательством» черных дыр, не существовала до апреля 2019 года (<https://phys.org/news/2019-04-scientists-unveil-picture-black-hole.html>).

История квантовой механики идет по тому же пути. В ней участвуют сотни блестящих физиков, наблюдающих очень маленькие объекты, поведение которых они не могли бы объяснить, используя традиционную (т. е. классическую) физику. С появлением математических уравнений они стали наблюдать и изучать новые, странные явления, наличие которых, казалось, все больше подтверждалось. Они делали предположения о том, почему и как что-то происходило, а затем проводили эксперименты, чтобы доказать или

опровергнуть свои догадки. Со временем дополнительные эксперименты и наблюдения создали ныне известные постулаты квантовой механики. Некоторые блестящие умы, такие как Эйнштейн, ошибались относительно некоторых фактов, а ранее малоизвестные физики сделали карьеру (и получили Нобелевские премии), приведя доказательства других. В целом вклады сотен отдельных ученых и их скептицизм создали квантовую механику такой, какую мы знаем сегодня, временами кажущуюся странной и необъяснимой.

Основные свойства квантовой механики

В этом разделе я расскажу о популярных свойствах квантовой механики, таких как фотоэлектрический эффект, двойственность волна–частица, вероятности, принцип неопределенности, спиновые состояния, туннельный эффект, суперпозиция, эффект наблюдателя и квантовая запутанность.

Примечание Итак, что такое квант в квантовой физике? Когда физики используют термин *quantum* или *quanta* (от латинского корневого кванта, что означает количество или сколько), они заявляют, что все, что они описывают, является наименьшей возможной единицей чего-либо (например, света или энергии) и не может быть разделено на более мелкие единицы. И любой математический расчет с участием квантов не может разделить кванты на что-то меньшее, чем целое число.

Квантовая механика или *квантовая физика* состоит из свойств и действий квантовых частиц и взаимодействия. Так называется также то, что является областью исследований с участием квантовых свойств и частиц. Почти всегда эти слова используются как взаимозаменяемые.

Хотя вся наша реальность состоит из квантовых частиц и их взаимодействия, квантовая механика существует на микроскопическом уровне для очень, очень малых элементарных объектов, таких как фотоны, кварки, электроны и атомы. Если элементный объект проявляет квантовые свойства, он известен как *квантовая частица*. Самые маленькие известные частицы обычно проявляют квантовые свойства. Квантовые свойства могут распространяться и на более крупные объекты, на так называемом *макроскопическом уровне*, но наука еще не продвинулась настолько, чтобы понять однозначно, происходит это или нет, и если происходит, то как. Понимание того, как свойства очень маленьких объектов передаются большим объектам и воздействуют на них, – конечная цель весьма популярной так называемой *Всеобщей теории (Theory of Everything)*.

Примечание Макроскопический уровень включает в себя любой объект, превышающий микроскопический уровень атома и субатомные частицы, но часто интерпретирующийся как начинающийся с объектов, которые могут быть обнаружены невооруженным глазом. Большинство ученых сходятся во мнении, что человеческий глаз может обнаружить объект, равный ширине человеческого волоса (или 0,4 мм), или около 100 000 атомов элемента.

ФОТОНЫ И КВАНТОВАЯ МЕХАНИКА

Вы будете часто читать о фотонах (первоначально названных Эйнштейном *квантами энергии*), используемых в экспериментах по квантовой механике. *Фотон* является наименьшей из возможных делимых единиц света и квантового поведения. Они очень маленькие. Для среднего напряженного человеческого глаза регистрация очень слабого проблеска света, отправленного почти мгновенно, потребует не менее ста фотонов. Любой луч света или изображение, которое мы обычно видим, включает в себя от миллионов до триллионов фотонов.

Квантовые физики часто проводят эксперименты с использованием одиночных (или относительно небольших количеств) фотонов или других элементарных частиц, потому что, используя небольшие их количества, ученые могут удалить другие ненужные эффекты, которые в противном случае только усложняют эксперименты, результаты и математические доказательства. Доказательство квантовых свойств было впервые получено в экспериментах с использованием фотонов при исследовании излучения, электромагнитных волн и фотоэлектрического эффекта (за которое Эйнштейн был удостоен своей единственной Нобелевской премии в 1921 году). Работа Эйнштейна имела решающее значение для становления квантовой теории. Даже его работы по опровержению квантовой механики лишь улучшили ее понимание нами.

В течение долгого времени ученые смогли генерировать одиночные протоны, посылая их в экспериментах разными путями и измеряя то, что происходит, используя светочувствительное оборудование, так называемые фотоумножительные трубы (*photomultiplier tubes*). Фотоумножитель способен принять один обнаруженный фотон и размножить его в достаточно большом количестве других фотонов, которые могут создать электрический ток, чтобы можно было зарегистрировать и подтвердить начальное обнаружение одиночного фотона. Представьте себе это как падающее домино. Падение одной кости домино может вызвать падение многих других костей домино. По этой причине, когда вы будете читать о квантово-физических экспериментах, вы часто будете читать о фотонах (и подобных элементарных квантовых частицах). Распространенными также являются эксперименты с использованием отдельных электронов, атомов и молекул. Давайте обсудим, что доказали некоторые из этих экспериментов.

ФОТОЭЛЕКТРИЧЕСКИЙ ЭФФЕКТ

Понимание и количественная оценка фотоэлектрического эффекта в начале 1900-х годов (Планк, Эйнштейн и др.) послужили началом основ современной квантовой механики. Свет, который мы видим, – это только один тип и диапазон электромагнитного излучения того, что называется электромагнитным спектром. Электромагнитный спектр описывает все виды электромагнитного излучения, включая свет, который мы можем видеть, и все типы, которые мы видеть не можем (такие как рентгеновские лучи, микроволновые печи, гамма-волны и радиоволны). Различные типы элект-

ромагнитного излучения отличаются в первую очередь длиной волны (видимый свет имеет длину волны от 400 до 700 нанометров (нм), в качестве примера рентгеновские лучи имеют от 0,10 до 10 нм), частотой (нередко измеряется количеством циклов в секунду, называемых герц [Гц]), интенсивностью, направлением и другими свойствами. Все виды электромагнитного излучения движутся прямолинейно, если излучение ничем не ограничено (объектом, гравитацией и т. д.), со скоростью света (299 792 458 м/с в вакууме).

Примечание Частота и длина волны могут быть преобразованы друг в друга через скорость света, и по существу это одна и та же переменная.

У света есть импульс и энергия (но нет массы). Планк и Эйнштейн поняли, что когда свет (или другие формы электромагнитного излучения) падает на другой материал, материал часто испускает электроны (которые всегда заряжены отрицательно) в результате передачи энергии от фотона материалу, как показано на рис. 1.1. Чем выше интенсивность света, тем больше электронов испускается. Фотоэлектрический эффект возникает, когда свет попадает на большинство материалов, но наиболее легко наблюдается, когда он падает на металлы и другие хорошо проводящие материалы. Фотоэлектрический эффект – это когда энергия солнца преобразуется в электричество с помощью солнечных батарей. Фотоэлектрический эффект лежит также в основе работы цифровых камер и записи изображений.

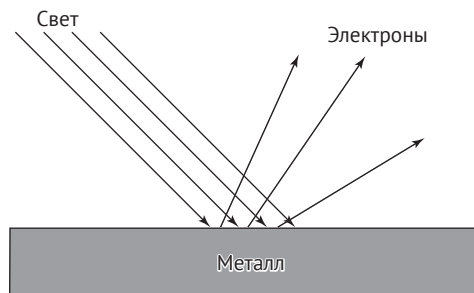


Рис. 1.1. Фотоны ударяются о металл, который затем испускает электроны
Стив Холцнер (Steven Holzner), рис. 1.3 из Quantum Physics For Dummies, Revised Edition; Wiley, 2013

Двойственность волна–частица

Сотни лет то, что ученые обнаруживали на микроскопическом уровне, классифицировалось или как частица, или как волна. *Частицы* – это (микроскопические) объекты, которые следуют четко определенным, легко обнаруживаемым физическим законам, объекты, которые мы можем наблюдать так же, как и повседневные макроскопические объекты (такие как камни или шары). Частицы путешествуют предсказуемыми путями, подвержены гравитации и могут взаимодействовать с другими частицами и объектами. Их довольно легко описать, предсказать и математически моделировать.

Волна – это непрерывное возмущение в поле, которое колеблется между различными точками пространства, или какая-то другая переменная. Волна может передавать энергию через основную среду, не нарушая другие объекты в среде. Это, например, происходит, когда плавающий объект, например лодка на воде, встречается с волной. Волна поднимает лодку вверх и вниз по мере прохождения, но не сильно нарушает ее общее положение на воде, если волна не настолько велика, что становится гребнем. Волны проявляют себя не только в том, что мы видим (например, океанские волны, рябь в озере или вибрации в струне), но также и в другом, что мы не видим (например, звук, радио, радиация и микроволны).

Примечание Волны могут осциллировать, как переменные, не меняя пространства или положения среды. Например, электромагнитные волны – это меняющиеся электрические и магнитные поля.

Волны колеблются в непрерывной, повторяющейся, связанной схеме. *Форма волны* каждого конкретного типа волн имеет верхний пик или гребень, за ним следует нижняя долина или впадина, и это повторяется снова и снова. Расстояние между вершиной и впадиной называется *амплитудой*. Число полных подъемов и впадин волны за определенный период времени определяет ее *частоту*.

Ученые думали, что частицы и волны обладают совершенно разными физическими свойствами. Частицы функционируют больше как камни или бейсбольные мячи. Они с трудом «огинают» предметы. Они ударяют с импульсом и силой. Их траектории при столкновении и возникающие при этом отскоки могут быть предопределены и рассчитаны заранее. Можно легко увидеть каждую отдельную часть составляющих большую массу частиц, как вид отдельных камней, составляющих кучу камней. Частица, ударившаяся в стену, похожа на жука, попавшего в лобовое стекло. Волны имеют противоположные свойства.

В середине 1800-х годов после многих теорий и экспериментов это было «устоявшейся наукой», в то время как свет и фотоны, которые составляют его, перемещались как волны. Но начиная с начала 1900-х годов, когда были обнаружены фотоны и другие электромагнитные частицы и использованы в большем количестве субатомных экспериментов, ряд ученых стали замечать, что фотоны и другие частицы вели себя и как волна, и как частица (то есть проявляли двойственность волна–частица). В то время это считалось чуть ли не научным кощунством. Однако Эйнштейн подтвердил эту новую точку зрения, продемонстрировав, что свет действует так же, как частица, и получил за это открытие свою единственную Нобелевскую премию по физике. Эйнштейн писал о своем открытии:

Кажется, мы должны использовать иногда одну теорию, иногда другую, а иногда можем использовать и обе. Мы столкнулись с новым видом трудностей. У нас есть две противоречивые картины реальности. Отдельно ни одна из них полностью не объясняет явления света, но вместе они это делают.

Один из лучших способов думать о двойственности волновых частиц – это представить, что у вас есть резиновый шарик, который, когда ведет себя как частица, подпрыгивает и отпрыгивает назад и вперед, ударяясь о другие объекты, в зависимости от его траектории и свойств материала, о который он ударяется. Теперь представьте, что шар падает в озеро и исчезает (под поверхностью). Его энергия немедленно превращается в волны в виде ряби на поверхности. Затем волновая рябь ударяется о доковую станцию, находящуюся в воде. Резиновый шар в этот момент появляется на доке, а волны исчезают. Это и есть двойственность волна–частица в зависимости от ситуации. Фотон действует иногда как волна, а иногда как частица. За эту прекрасную аллегория надо сказать спасибо Доминику Воллиману (Dominic Walliman).

Это частица

Ученые продемонстрировали двойственность волна–частица с помощью простого эксперимента с использованием высокоинтенсивного (лазерного) света, фона и промежуточного блокирующего материала с одной и двумя прорезями в нем. Ученые направили пучок фотонов сквозь щель блокирующего материала и затем посмотрели, куда попали фотоны на заднем фоне. Когда использовалась одна щель и пучок фотонов был пропущен через нее, фотоны, пройдя через щель, попали на задний фон почти прямо по направлению пучка. Отдельные фотоны расположились довольно близко друг к другу, имитируя форму щели. Картина напоминала выстрел меткого стрелка и путь пули при выстреле сквозь щель. Если винтовка находилась каждый раз в одном и том же положении, можно было ожидать, что пуля попадет почти в то же место, с небольшими отклонениями в зависимости от опыта стрелка, точности винтовки, индивидуальных параметров пули и любых других внешних мешающих факторов. Если винтовка была направлена при стрельбе под разными углами, пули могли располагаться более спонтанно. Это как раз и происходило, когда пропускался пучок фотонов. Фотоны демонстрировали свойства частицы.

Интерференция волн

Нечто удивительное случилось, когда в промежуточном блокирующем материале добавили вторую щель. Когда был пропущен один фотон, он все еще попадал на заднем плане за щелями, со следом одной частицы (то есть как пулевое отверстие), но уже не прямо за прорезями. Когда же пучок фотонов содежал все большее и большее их количество, казалось, фотоны попадали в области, которые не были расположены непосредственно позади щели. Были области с различными предпочтениями – кластеры областей с большим количеством совокупных попаданий, и области, в которые попадало меньше фотонов. Создавалось чередование светлых и темных вертикальных полос (как показано на рис. 1.2).

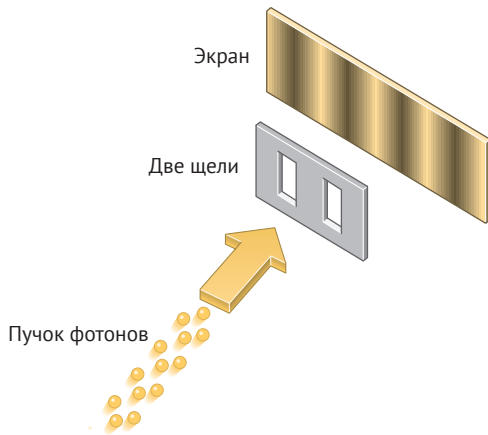


Рис. 1.2. Эксперимент с двумя щелями и источником света, подтверждающий двойственность волна–частица
 Давид Янг (David Young) и Шейн Стадлер (Shane Stadler),
 рис. 29-1 из Cutnell & Johnson Physics, 11th Edition; Wiley, 2018

Ученые сразу поняли, что то, что они видят, являлось результатом действия пущенных одновременно фотонов, перемещающихся как волна (и падающих на задний план как частица). Полосы появлялись потому, что когда фотон перемещается как волна, он попадает в обе щели и создает две результирующие волны по другую сторону каждой щели, с которой взаимодействует каждая часть оригинальной одиночной волны, проходившая через щель. По другую сторону две результирующие волны перемешивались друг с другом, формируя полосы. Но фотон, падающий на задний фон, являлся следом частицы (как показано в видео из Википедии: https://upload.wikimedia.org/wikipedia/commons/e/e4/Waveparticle_duality.ogv). Это была замечательная находка.

Полоса на экране создается взаимодействующими друг с другом волнами. Если одна световая волна, находящаяся на вершине гребня, встречает в какой-то момент другую световую волну на вершине ее гребня, то это создает максимально возможную комбинированную, синхронизированную световую волну, которая имеет наиболее яркий свет. Это также означает, что их объединенные впадины создают темные полосы. Любая другая комбинация, отличная от совпадения двух наибольших вершин и двух наибольших впадин, будет создавать менее смешанные волны – менее яркие или менее темные.

Вначале, когда это было обнаружено, ученые просто не могли поверить утверждениям, математике и результатам. Потребовались десятилетия, чтобы наука окончательно признала, что свет ведет себя и как частица, и как волна одновременно. Теперь мы без сомнения знаем, что все субатомные частицы, составляющие всю материю, действуют с двойственностью волна–частица. Этот вывод укрепил решимость ученых более полно исследовать квантовую механику и попытаться «связать» ее с остальным нашим большим миром. Сегодня любой может выполнить простой эксперимент, чтобы увидеть эту двойственность волны и частицы света.

Ваш эксперимент с двумя щелями

Приятно иметь возможность воссоздать один из ранних экспериментов по двойственности частиц и волн и непосредственно наблюдать работу квантов. Вы можете дублировать этот эксперимент, используя лазерную указку, фольгу и сплошной фон, например стену. Используйте сильную однотонную (не белую) лазерную указку. Чем она более мощная, тем лучше. Белый свет – это смесь всех цветов света, и это затрудняет эксперимент, потому что отдельные цвета, из которых состоит белый свет, имеют разные частоты. Поместите фольгу на поверхности разделочной доски и вырежьте рядом две равные по длине вертикальные прорезы длиной около 1 дюйма, так близко, насколько это возможно (речь идет о расстоянии в миллиметры). Затем в затемненной комнате осветите лазерным лучом указки эти две прорезы на расстоянии фута или более от фольги, отстоящей от поверхности заднего фона также на расстоянии фута или более. Возможно, вам придется поэкспериментировать с расстояниями, на которых отстоят друг от друга лазерная указка, промежуточный материал и стена, но если все сделано правильно, вы увидите полосы. Вероятно, это будет не так резко, как это видно в серьезных физических экспериментах с лучшим лабораторным оборудованием, но вы получите полосы.

Природа частиц света доказана при проведении такого же эксперимента, хотя мы не можем с уверенностью увидеть это без специальной аппаратуры обнаружения, потому что каждый отдельный запущенный фотон будет обнаружен как одна частица непосредственно на щелях или при попадании на поверхность заднего фона. Применение для обнаружения частиц фотонных детекторов подтвердит, что каждый фотон проходит через щель и ударяет в фоновую поверхность как частица. Когда измерениям подвергаются все излучаемые фотоны при проведении многих и многих экспериментов, эффектом всегда является наличие светлых и темных чередующихся полос, подтверждая волновые свойства света в очередной раз. Этот эксперимент доказывает, что свет (как и все квантовые частицы и молекулы) имеет двойственность волна–частица.

Примечание Если вы хотите увидеть реальные примеры этого эксперимента, просто зайдите на YouTube и найдите в поисковике «волновой эксперимент с двумя щелями» или что-то в этом роде. Вы, как правило, найдете десятки видео, демонстрирующих эксперимент. Один такой отличный, анимированный пример эксперимента размещен на странице <https://www.youtube.com/watch?v=fwXQjRBLwsQ>.

Обнаружение странности

Теперь все становится действительно странным. Когда ученые помещают детекторы фотонов на одну или обе щели, чтобы установить, через какие щели фотон действительно проходит, фотон действует как частица и все волнообразное поведение немедленно исчезает. Позвольте мне повторить это. Перед тем как детекторы ставятся перед двумя щелями или сзади двух щелей, фотоны действуют как волны. А после того как детекторы установлены

и включены, по пока не понятной до конца причине, фотоны сразу начинают действовать как частицы, как будто щель одна. Это как будто частицы сами видят процесс обнаружения и изменяют свое поведение. Ученые даже провели эксперименты, в которых они не включают детекторы до тех пор, пока фотоны не прошли через щель, и когда они включают детекторы, оказывается, что фотоны ведут себя как частицы (когда, казалось бы, они должны были пройти через щели как волны). Как будто фотон задним числом корректирует в будущем свое начальное поведение в прошлом, основанное на начальном обнаружении. Мы не можем сказать, это действительно происходит (то есть изменение прошлого) или к какому времени это относится, прошлому или реальному. Что происходит и как, никто не знает. Мы знаем только то, что изменение поведения происходит каждый раз, когда используется детектор, а что происходит, нам пока понять трудно. Это явление известно как часть эффекта наблюдателя, который более подробно описан далее и является объяснением той истории изменения представления о свете, с которого начиналась эта глава.

Принцип вероятности

Понимание того, как электроны вращаются вокруг ядра, привело к лучшему пониманию того, как устроен наш мир, особенно на квантовом уровне. Например, будучи еще школьниками, мы все, наверное, узнали, что каждый атомный элемент состоит из электронов, протонов и нейтронов. Каждый атом (самая маленькая единица обычного вещества) состоит из ядра (состоящего из положительно заряженных фотонов) и (без заряда) нейтронов, окруженных отрицательно заряженными электронами. Электроны «вращаются» вокруг ядра из-за электромагнитного притяжения. В начальной школе большинство из нас узнало, что электроны кружатся в орбитальных полосах, известных как оболочки.

В начальной школе, вероятно с целью упрощения, электронные орбитальные оболочки (см. рис. 1.3) показываются на атомном уровне, как совершенные круги или, возможно, овалы, часто идеальные орбиты, подобные орбитам планет, но квантовая физика показала нам, что движение электронов не происходит по идеальным кругам или даже овалам. Электронные оболочки идеального круга являются плодом чьего-то раннего воображения и сегодня используются исключительно для того, чтобы продемонстрировать наличие электронных оболочек, не углубляясь в детали. Но это не то, что действительно происходит. Электроны вращаются вокруг ядра по более сложным схемам, продиктованным принципами квантовой механики и вовлеченным в процесс энергией. На рис. 1.4 показан двумерный репрезентативный пример орбит электронов вокруг ядра на определенном энергетическом уровне. Эти области вероятной орбиты известны как *атомные орбиты*, или *электронные облака*. Вероятностный характер процесса очень важен в квантовой механике и более подробно будет объяснен в следующем разделе.

Ситуацию несколько усложняет то, что никто не может заранее сказать, где конкретный электрон может оказаться на орбите в некоторый момент времени, можно только судить о вероятности того, что он окажется в опре-

деленных (прогнозируемых) атомных орбитальных областях. Не существует математического уравнения, которое могло бы с уверенностью сказать, что любой электрон будет точно в точке А в какое-то определенное время. Лучшее, что квантовая механика может сказать, – это то, что когда вы попытаетесь найти эту точку А, выяснится, что электрон может оказаться в ней только с определенной вероятностью. И если вы проведете измерение много раз, появление этого электрона в точке А может быть предсказано лишь в процентах вероятности.

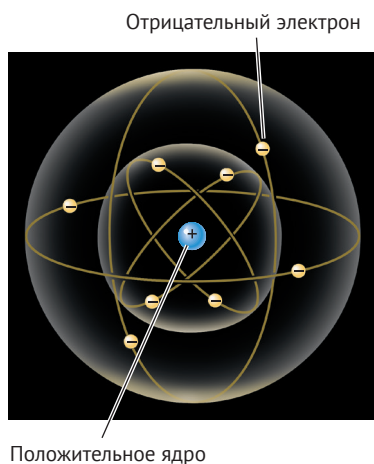


Рис. 1.3. Ядро атома, окруженное упрощенными орбитами электронов
 Давид Янг (David Young) и Шейн Стадлер (Shane Stadler), рис. 30-1 из Cutnell & Johnson Physics, 11th Edition; Wiley, 2018Ш

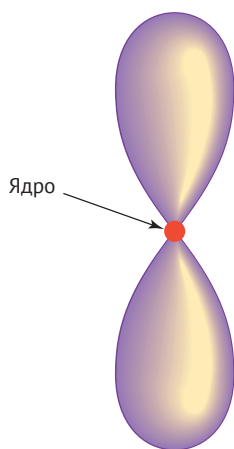


Рис. 1.4. Двумерная орбита атома для электронов, вращающихся по орбите

Принцип вероятности применим к любому свойству квантовой частицы, а не только к электронам. Нельзя угадать заранее не только состояние, их

конкретные свойства или положение, но при измерении их состояние или положение является во время любого одного измерения абсолютно случайной величиной в широких пределах вероятностного предсказания. И эта случайность конкретного ответа или состояния вовсе не случайна. Она является фундаментальным принципом, присущим квантовой механике. Ключевое отличие квантовой механики от традиционной классической физики состоит в том, что точное состояние или положение квантового объекта или свойства не может быть точно предсказано заранее. В классической физике $A + B = C$ и всегда будет равно C . Более того. Если я знаю A и C , я могу предсказать B .

Но в квантовой механике точное место электрона на орбите, или свойства кванта, или размещение любой квантовой частицы может быть описано вероятностями и только вероятностями. Никто не знает заранее, каким будет какой-то один ответ при измерении. Лишь то, что будет одним из ряда возможных ответов, и если проводить измерения много раз, измеренные результаты будут соответствовать прогнозируемой вероятности. Это лучшее, что может сказать любой человек, завершая измерения.

Эти найденные и измеренные возможные области ответов и *вероятность* того, что электрон находится в определенном месте или с определенным квантовым свойством, могут быть точно предсказаны. Если вы запустите конкретный электронный эксперимент снова и снова (скажем, тысячу раз), чтобы точно определить, где электрон был точно в определенный момент времени, вы не сможете предсказать положение какого-либо конкретно измеряемого электрона в одном из этих измерений. Квантовая механика говорит, что любое одно измерение будет случайным событием. Но совокупность мест вокруг ядра, где в конечном итоге находился электрон, найденная и измеренная во многих экспериментах, создаст графическую диаграмму, подобную соответствующим предсказаниям атомных орбит.

Несмотря на то что мы не можем знать точный ответ, диапазон возможных ответов измерения известен. Когда известна вероятность конкретного квантового состояния дискретной квантовой системы, это состояние описывается математической формулой, известной как *волновая функция*. Физики используют волновые функции для описания и предсказания того, что произойдет в широком диапазоне вероятностей при конкретном квантовом взаимодействии или конкретном свойстве. Конкретный ответ для одного измерения неизвестен, но известен диапазон вероятных ответов и соответственно вероятность каждого возможного ответа. Волновая функция математически описывает все, что мы знаем о квантовой частице, включая все ее свойства, какими могут быть эти свойства и вероятность их появления при измерении. Волновая функция представляет для физиков полную карту квантовой частицы. Используя волновую функцию, ученые могут предсказать, что произойдет, когда различные частицы будут взаимодействовать друг с другом.

Этот принцип вероятности квантовой физики важен, потому что он означает, что мы не можем предсказать, каким будет какое-либо конкретное состояние квантового свойства до его измерения. В качестве очень упрощенной (не квантовой) иллюстрации предположим, что мы пытались определить, какого цвета была собака, черной или белой. С квантовой точки зрения, мы не

можем определить заранее, до измерения, какого она была цвета. Мы могли бы предсказать возможные ответы (например, черная или белая) и даже вероятность того, что каждый ответ явится наблюдаемым ответом на основе некоторой заранее определенной математики (скажем, 50 % времени собака будет белой, а 50 % – черной, если мы проведем эксперимент много раз). Но нам придется подождать, пока собака не появится, чтобы увидеть, какого же цвета собака действительно наблюдалась и измерялась. И не только это, но и цвет собаки, определяемый в любой конкретный момент времени, будет случайным.

Примечание Это своеобразное квантовое свойство расстраивает физиков, склонных к классике, и делает квантовую механику столь настораживающей. В традиционной физике, когда вы знаете все о вовлеченных объектах, их свойства и их взаимодействие, вы всегда сможете заранее найти ответ или результат. Когда эксперимент закончится или результат будет получен, он будет соответствовать предсказанному ответу в соответствии с ранее полученными математическими соотношениями. «Это наука! Вот как она работает!» Квантовая механика, напротив, говорит, что независимо от того, насколько хорошо вы знаете математику, объекты и как они взаимодействуют, вы никогда не сможете предсказать конкретный ответ или квантовый результат в одном каком-либо эксперименте. Лучшее, что вы вообще сможете сделать, – это предсказать вероятность различных ответов.

Ситуация даже сложнее. «Ответ», который дает нам квантовый компьютер сегодня (в 2019 году), может быть неправильным, и часто мы получаем неправильный ответ. Помните, квантовые ответы – это только ответы внутри данного диапазона вероятностей. Но если мы сможем запустить квантовый сценарий и получить квантовый ответ большое количество раз, мы можем получить правильный (вероятностный) ответ, так как получим правильный ответ чаще и последовательно в последовательном цикле экспериментов. По сути, чтобы получить правильный ответ, вычисления необходимо запускать снова и снова, пока возвращаемый вероятностный ответ не будет настолько статистически достоверным, что это должно и стать правильным ответом. Приведем макроскопическую аллегорию. Предположим, что шестигранный кубик имеет смещенный центр масс так, что будет давать один какой-либо ответ при подбрасывании чаще, чем любой другой ответ (так называемый «загруженный» кубик). Вы знаете, что смещение центра существует, но вы не знаете, в каком направлении относительно его поверхностей. Когда вы бросаете кубик один раз, он может лечь или не лечь в соответствии со смещением в сторону поверхности. Но когда вы подбрасываете его много раз, тот, скорее всего, более часто выпадет определенное число, чем любое другое число, подтверждая смещение с высокой достоверностью. Допустим, вы планируете подбрасывать загруженный кубик десять раз. Первый раз, когда вы бросаете, он дает два. Теперь у вас есть ответ, но только с уверенностью 10 % (1 из 10 бросков). Вы подбрасываете его во второй раз и получаете единицу. Теперь у вас есть другой ответ, но только с уверенностью 10 % (1 из

10 бросков). На третьем броске вы снова получаете единицу и имеете 20 % уверенности (2 из 10 бросков). На четвертом броске вы получаете пять. Затем в следующие пять подбрасываний получаете единицу, что дает вам 70 % уверенности (7 из 10 бросков были единицей). И при последнем подбрасывании вы получаете тройку. Всего у нас будет четыре разных возможных ответа, но одна сторона кубика была ответом наибольшее количество раз, и любой разумный человек придет к выводу, что сторона кубика с единицей была той стороной, в которую смещен центр тяжести. В квантовом компьютере количество измерений и полученных ответов, скорее всего, будет много больше, чем десять раз, и соответственно будет получена максимальная вероятность правильного ответа.

Для любого отдельного измерения всегда, однако, велика вероятность, что оно дает неправильный ответ. И как бы настораживающе это не звучало, так работают все квантовые измерения. И вы уже живете и выживаете в такой действительности с самого дня рождения.

Принцип неопределенности

Принцип неопределенности Гейзенберга гласит, что чем точнее измеряется положение квантовой частицы, тем менее точно может быть известен ее импульс, и наоборот. Неопределенность также применима к другим зависимым парам квантовых свойств (известных как *сопряженные переменные*), но не ко всем свойствам. Могут быть пары свойств, которые вы можете измерить одновременно, просто не у всех пар. Некоторые пары связаны друг с другом таким образом, что это мешает точно измерить оба свойства одновременно. Это не из-за некоторого изъяна в том, как человечество может или не может точно измерить что-либо. Это квантовый закон природы, проистекающий из двойственности волна–частица и принципа вероятности. Один из этих законов квантовой механики гласит, что вы не можете точно измерить обе позиции или импульс квантовой частицы в одно и то же время, и, когда вы пытаетесь более точно измерить одну величину, измерение другой величины этой зависимой пары становится менее точным.

Давайте воспользуемся еще одной макроскопической аллегорией – попыткой измерить скорость автомобиля. В макроскопическом классическом мире скорость автомобиля – это просто измерение пройденного расстояния за определенный временной период. Если машина проехала 100 километров ровно за 1 час, вы бы сказали, что скорость в среднем составляет 100 км/ч. Но в квантовом мире, глядя на квантовые свойства очень маленьких частиц, обе переменные времени и расстояния вообще не фиксируются. Они меняются в диапазоне вероятностей, и любое одно измерение может привести к другому ответу из этого диапазона. Это делает измерение сложным с самого начала.

В нашем примере измерения скорости машины есть очень похожая аллегория, если в любом отрезке пути, по которому вы провели измерение, автомобиль движется быстрее и медленнее, чем 100 км/ч. Это действительно маловероятно, что какой-либо сложный объект с автономным питанием будет двигаться с одинаковой скоростью во все моменты времени. Чтобы

определить скорость, с которой автомобиль двигался одну секунду, надо учитывать сопротивление ветра, изменения в состоянии дорожного покрытия, изменения температуры и сотни факторов внутри самого двигателя, определяющие мощность и крутящий момент, которые он развивает в данный момент времени. Хотя если в конечном итоге было получено 100 км/ч в течение всего пути, то, конечно, его скорость, вероятно, была ровно 100 км/ч чаще, чем любая другая скорость.

Это и составляет принцип вероятности. Если измерять радаром скорость машины, то можно обнаружить, что в каждой точке пути машина имеет разную скорость, однако при окончательном результате 100 километров ровно за 1 час существует вероятность того, что скорость машины, равная 100 км/ч, была больше любой другой скорости в большинстве точек пути. Впрочем, всегда есть вероятность, что машина шла половину пути со скоростью ровно 98 км/ч, а затем другую половину пути со скоростью ровно 101 км/ч, хотя это и менее вероятно.

Принцип неопределенности гласит, что чем большее время затрачивается для точного измерения скорости, тем одновременно менее точно может быть измерено расстояние, и нет никакого способа это исправить. В квантовом мире нет такого параметра, как высокая точность скорости. Как концепция он не существует. Это закон природы. Чтобы продолжить нашу скоростную аллегорию, предположим, наши спортивные судьи захотели быть сверхточными, и для этого они решили запечатлеть лучшую в мире фотовспышку, чтобы фотографировать машину, когда она пересекает финишную черту. Чтобы получить тот момент, когда машина пересекла черту, затвор камеры должен был открыться и закрыться очень быстро. В эту микросекунду автомобиль будет «заморожен» во времени. На картинке в тот самый момент, когда она пересекла черту, машина, кажется, не двигалась вообще. Финишную линию камера может запечатлеть точно в момент, когда машина пересекает линию, но в этот момент машина не будет двигаться (или двигаться очень сильно). Камере, пытаясь получить точный момент, когда время истекло, придется удалить скорость из измерения. И если бы вы имели другую камеру, которая измеряла истинную скорость автомобиля, она была бы не в состоянии точно запечатлеть момент, когда машина пересекла линию.

Усложним дело. Что собой представляет линия? Любая линия на макроуровне выглядит как прямая линия. Но увеличьте любую нарисованную или начерченную линию, и при увеличении проявятся ее отдельные, крошечные волнистости. Чтобы быть наиболее точным, вам нужно сделать снимок или нажать на секундомер точно в момент, когда автомобиль пересек первый атом нарисованной линии. И ваш глаз, и линза камеры должны будут щелкнуть точно, когда машина пересекла этот первый атом, а мы ведь не можем знать, в какой момент машина на самом деле пересекла первый атом финишной линии, пока этот момент не пришел к сетчатке глаза или линзе камеры. А это определяют фотоны и скорость света.

К тому времени, когда первый записывающий фотон придет, машина уже будет за первым атомом относительно тех измерений, которые будут сделаны. Мы знаем, что этот первый атом состоит из субатомных частиц – электронов, протонов и нейтрино. Чтобы быть наиболее точным, вам при-

дется остановить секундомер или запустить камеру тогда, когда автомобиль встретит первый электрон на внешней орбите электронной оболочки первого атома, а мы, согласно квантовой теории, не знаем, где будет находиться этот первый электрон, а при одном измерении он может находиться где угодно и оказаться не там, где будет его наиболее вероятное местоположение. В конечном итоге вы не сможете сделать действительно точный расчет скорости, потому что вам нужно получить наибольшую точность атрибута (то есть электрона), который движется, а частица движется как волна в соответствии с волновой функцией. Пытаясь получить большую точность, вы понимаете, что просто невозможно получить действительно точную меру чего-либо, тем более для сопряженных пар параметров, поскольку определение одного зависит от другого. Все движется во все времена (даже камень состоит из движущихся электронов), все является частицей и волной, все ведет себя по-разному, каждый ответ во время конкретного измерения является случайным, и это может быть даже не «правильный» (наиболее вероятный) ответ. И с сопряженными парами точное измерение одного значения зависит от другого, который по определению должен измеряться менее точно. В нашем примере концепция «километр/час» (то есть положение и импульс) на самом деле на квантовом уровне не существует. Просто не существует. Это принцип неопределенности.

Вы должны понимать, что неопределенность в парах измерений не связана с отсутствием возможностей измерительного оборудования. Многие люди, впервые услышав о принципе неопределенности, думают, что это связано с проблемами с измерительной аппаратурой, которая недостаточно точна. Они полагают, что это связано с недостатком измерительных приборов. Это не так. Мы могли бы иметь самое точное измерительное оборудование, которое может очень точно (для наших человеческих чувств) измерить время и расстояние, но это не имеет значения. Это не измерение, которое является неточным. Это связано с (квантовыми) законами природы, которые определяют, насколько точно мы можем измерить любое квантовое состояние, которое зависит от двух зависимых сопряженных переменных. Поскольку мы измеряем одну сторону зависимой пары более точно, просто невозможно так же точно измерить другую часть уравнения. Фактически это просто гарантированная инверсия отношения.

Примечание Принципы вероятности и неопределенности не должны быть истолкованы как означающие, что квантовая механика и квантовые свойства не могут быть математически точными. Наоборот, математика и результаты квантовой механики невероятно точны и имеют непревзойденный большинством других наук уровень доверия. Принцип неопределенности также не следует смешивать с эффектом наблюдателя, который обсуждается далее.

Спиновые состояния и заряды

Есть 12 фундаментальных квантовых частиц (также известных как элементарные), которые составляют всю материю во Вселенной. Фундаментальные частицы, как мы знаем, не могут быть разбиты на более мелкие, цельные

частицы. Познакомьтесь с ними, если вы не знали о них раньше. Некоторые из этих частиц имеют несколько странные на слух имена. Основными квантовыми частицами являются электрон, мюон (*muon*), тау (*tau*), электронное нейтрино (*electron neutrino*), тау-нейтрино (*tau neutrino*), мюон-нейтрино (*muon neutrino*) (все части семейства *лептонов*, *lepton family*) и *вверх* (*up*), *вниз* (*down*), *верхний* (*top*), *нижний* (*bottom*), *очарование* (*charm*), *странный* (*strange*) (последние шесть являются частью семейства *кварков*, *quark family*). Фундаментальные квантовые частицы составляют все другие субатомные частицы. Например, каждый протон состоит из двух кварков *up* и одного кварка *down*. Нейтрон состоит из двух кварков *down* и одного кварка *up*. Электрон сам является элементарной частицей и не состоит из чего-либо. Электрон не содержит субатомных частиц, на которые его можно было бы разбить. Электроны, протоны и нейтроны составляют атомы, атомы составляют элементы и молекулы и т. д.

Примечание Мы никогда не можем быть уверены, что обнаружили каждую элементарную частицу или даже что существующие лептоны и кварки элементарны, хотя современная наука очень непреклонна в том, что это частицы с наименьшим общим знаменателем. Но из истории известно, что то же самое раньше говорили о клетках, атомах и протонах. Итак, кто знает, что мы обнаружим, когда попытаемся до конца разгадать ту грандиозную головоломку, которой является наша реальность?

Каждая элементарная квантовая частица имеет массу, заряд и спин. Все понимают, что такое масса, так что давайте быстро обсудим два других. *Заряд* – это величина тока по сравнению с электроном. Например, у кварка *up* есть две трети заряда электрона, а у кварка *down* есть отрицательная треть заряда электрона. Поскольку у протона есть два кварка *up* и один кварк *down*, протон имеет $\frac{2}{3} + \frac{2}{3} - \frac{1}{3} = \frac{3}{3}$ заряда электрона, или точно равен заряду одного электрона. По этой причине в большинстве стабильных атомов число протонов в ядре равно числу орбитальных электронов. Элементарные частицы также имеют *спин*, который обратно пропорционален числу оборотов частицы, которые частица должна сделать, чтобы вернуться к своей первоначальной ориентации. Все элементарные частицы имеют спин половину (*one-half*), что означает, что они должны провернуться дважды, чтобы вернуться в исходное положение. Почему я рассказываю вам о квантовых зарядах и спинах? Потому что ответы, которые мы получаем от квантовых компьютеров, часто являются результатом зарядов и спинов. Как мы увидим в главе 2 «Введение в квантовые компьютеры», для получения ответов в различных типах квантовых компьютеров используются различные квантовые свойства и состояния.

Квантовое туннелирование

Квантовое туннелирование – это необъяснимая способность квантовых частиц проходить через барьеры, что классическая физика признает невозможным. Общий макроскопический подобный пример – шар, находящийся

у подножия холма или стены. Предположим, что человек пытается бросить мяч через стену, но у него не хватает физических сил, чтобы перебросить мяч через стену. Он безуспешно пытается снова и снова. Классическая физика, изучив руку человека и силу всего тела, говорит, что человек никогда не сможет этого сделать. Но по причинам, которые невозможно объяснить, иногда бросок мяча заканчивается тем, что мяч оказывается по другую сторону стены. Некоторые теории говорят, что мяч просто необъяснимо поднимается над стеной. Другие говорят, что при одном каком-то броске стена опускается или что мяч проходит через стену, не оставляя след точки входа или выхода.

Мы еще не знаем, как это работает или когда именно субатомная частица добьется успеха, вопреки всем своим предыдущим неудачным попыткам, но это существует и является основой всей известной жизни. Туннелирование – это то, как наше Солнце генерирует тепло и свет с помощью термоядерного синтеза. Туннелирование – это то, как распадается радиоактивный элемент. Туннелирование является основой фотосинтеза, который поддерживает жизнь большинства растений на Земле и затем поддерживает человеческую жизнь. Квантовое туннелирование используется в некоторых типах квантовых вычислений.

Суперпозиция

Суперпозиция является квантовым свойством, которое говорит, что частица может существовать во всех возможных состояниях, пока состояние, наконец, не наблюдается и измеряется, чтобы дать один ответ. Например, скажем, конкретная математическая задача, на которую вы не знаете ответа, возможно, имеет ответ или А, или В. Суперпозиция говорит, что до тех пор, пока ответ находится в квантовом состоянии, до того, как его можно наблюдать или измерить, он является в одно и то же время и А, и В. Это не А или В. Это и то, и другое.

Это связано с тем, что, как обсуждалось выше, при любом конкретном измерении квантового свойства измеренное свойство может быть любым возможным ответом. И фактически полученный ответ при любом одном измерении может быть случайным образом любым из этих возможных ответов. В классическом мире А – это А, а В – это В. Одна буква не может случайно быть иногда А и иногда В. Но в квантовом мире это именно то, что происходит.

Возможно, вы слышали о знаменитой квантовой головоломке Эрвина Шредингера. Шредингер создал сценарий (лишь мысленный эксперимент), в котором кота помещают в закрытую коробку с закрытой бутылкой смертельного яда, радиоактивного элемента и счетчика Гейгера. Радиоактивный элемент мог распасться или не распасться. Радиоактивный распад является квантовым событием, и в момент, когда какой-либо конкретный атом элемента решает распасться – это случайное событие. Если счетчик Гейгера обнаруживает излучение (от радиоактивного распада), он вызовет разрушение бутылки, содержащей яд, который убил бы кота.

Шредингер приводил этот мысленный эксперимент в качестве примера квантовой суперпозиции, наблюдаемой как макроскопическое событие,

чтобы продемонстрировать, насколько странной суперпозиция может быть, если представить ее на макроскопическом уровне. Шредингер пытался продемонстрировать, насколько курьезной выглядела в его времена квантовая механика при ее описании. Он проводил мысленный эксперимент не для поддержки квантовой механики. Он делал это, чтобы показать, насколько она абсурдна, и показать, что мы не понимаем, что происходит на самом деле. Если бы он был жив сегодня, то, вероятно, посмеялся бы над тем, что его намеренно абсурдный мысленный эксперимент на самом деле является наиболее часто используемым наглядным примером того, как в действительности работает квантовая механика, потому что это было совсем не тем, что он тогда собирался продемонстрировать.

До открытия коробки для наблюдения за котом принцип суперпозиции гласит, что радиоактивный элемент и распался, и не распался. Кот для нас одновременно и жив, и мертв. В классическом физическом (реальном) мире кот в любой конкретный момент времени будет либо жив, либо мертв – или одно, или другое. То, что квантовая физика доказала на квантовом уровне, – это что до того, пока мы не посмотрим, открыв коробку, кот (в результате радиоактивного распада) и жив, и мертв одновременно, а не находится в каком-то половинчатом состоянии, при котором кот отравлен, но не полностью. Нет, это означает, что он и на 100 % здоров, и на 100 % мертв в одно и то же время. Что кажется бессмысленным на макроскопическом уровне, является абсолютной реальностью на квантовом уровне.

Если вы собираетесь понять квантовую механику и квантовые компьютеры, то должны воспринять понятие суперпозиции. Вы должны расстаться с тем, что вы иначе видите и понимаете мир, потому что на квантовом уровне мир будет именно таким. У меня заняло много времени, чтобы понять последствия мысленного эксперимента Шредингера. Я полагал, что когда мы открыли коробку, кот был жив или мертв, либо одно, либо другое, и так было с какого-то определенного предыдущего момента времени. Но это не то, что говорит суперпозиция. Суперпозиция, которая была снова и снова доказана, говорит, что кот был и жив, и мертв, и пребывает в обоих состояниях, пока, наконец, не будет наблюдаться и измеряться. После того как «состояние» кота измерено, кот либо постоянно жив, либо мертв с этого момента и далее, это и будет результатом измерения при данном наблюдении. Этот результат ошеломил величайшие научные умы, которые когда-либо существовали и все еще существуют. Тем не менее эксперимент за экспериментом подтверждает, что суперпозиция на квантовом уровне – это реальность.

Квантовая механика и, как следствие, квантовые компьютеры мгновенно генерируют все возможные ответы сразу, и пока не будет замечено и измерено, «правильными» ответами являются все возможные ответы. Как только мы наблюдаем или измеряем ответ, только один ответ становится для нас постоянной реальностью.

Чтобы усложнить ситуацию, как обсуждалось ранее, никто не может предсказать, каким будет окончательный этот наблюдаемый ответ. Никто не может сказать: «Конечно, кот мертв!» или «Конечно, кот жив!» – и всегда будет истиной только то, что кот до измерения и жив, и мертв, и что кот будет жив

или мертв при измерении, но только в пределах определенной вероятности результатов и среди возможных вариантов конкретный результат является при измерении случайным. Если чье-то предположение верно, то только потому, что ему повезло (или сыграли вероятности). Если это сбивает с толку или вредит вашей голове, мы еще даже не дошли до самых странных мест. Так что «оставайтесь на линии».

Эффект наблюдателя

В квантовом мире простое наблюдение квантовой системы меняет ее, хотя квантовые физики не знают, почему, или не согласны в этом друг с другом. Как и все квантовые свойства, обсуждаемые в этой главе, десятилетия экспериментов показали, что это свойство является реальным и точным. Ученые не задаются вопросом, правда ли это, а ищут ответ на вопрос, почему или как это происходит. Например, в каждом эксперименте с двумя щелями, когда ученые помещают фотонный детектор, чтобы измерить, через какую щель проходит фотон, фотон всегда ведет себя только как частица (и результирующие волновые полосы не возникают). Если они выключат детектор, волновые полосы возвращаются. Как будто природа видит, что происходит измерение, оберегает и меняет то, что происходит. Возможно, это не то, что происходит на самом деле, но это то, как мы описываем происходящее на основе наших экспериментальных наблюдений и результатов, потому что у нас нет других способов передать то, что мы видим. Мы еще не знаем, что происходит.

Это привело ко многим различным конкурирующим интерпретациям. Одна интерпретация говорит, что это невозможно наблюдать за системой без какого-либо вмешательства в нее. Например, просто чтобы наблюдать за чем-то, часто требуется свет (то есть фотон) или какое-либо искусственно установленное оборудование для получения результата, и эти дополнения влияют на возможные квантовые результаты. На примере фотона: фотон должен «ударить» по тому, что измеряет, и отскочить назад к детектору (или нашему главному яблоку), чтобы мы могли обнаружить это, и этот «удар» должен вызвать какое-то взаимодействие.

Другая популярная интерпретация (*копенгагенская интерпретация*) говорит, что когда квантовая волновая функция многих вероятных возможностей наконец наблюдается и измерена, волновая функция «ломается» (известно под названием *коллапс волновой функции*) и переходит в конечное состояние. Наблюдение, создающее в результате коллапс, является помехой. Чтобы понять копенгагенскую интерпретацию, вы должны еще раз убедиться, что вы понимаете и верите в суперпозицию, в то, что любой квантовый ответ или состояние из всех ответов или состояний до измерения является возможным одновременно. Акт измерения квантового сценария сводит все состояния или ответы в единый окончательный ответ или состояние. Это измерение сворачивает все одновременно возможные ответы в один окончательный, постоянный ответ (который может являться или не являться вероятностным «правильным» ответом и может не быть тем же самым ответом, если измеряется или наблюдается как угодно по-другому).

Копенгагенская интерпретация имеет наибольшую поддержку в квантовом мире для объяснения, почему наблюдение чего-то меняет его. Хотя странность, присущая созданному Шредингером мысленному эксперименту «Парадокс кота в коробке», была именно тем, что он хотел продемонстрировать: насколько противоречащей интуиции была копенгагенская интерпретация относительно того, чему мы верили ранее. Мало ученых знало, что копенгагенская интерпретация не была даже близко к тому объяснению, в которое трудно поверить.

Другая интерпретация «Много миров» гласит, что все возможные ответы относительно коллапса волновой функции принадлежат теперь другим вселенным и что каждый квантовый коллапс создает ряд новых вселенных, равных всем возможным ответам вероятностной волновой функции перед коллапсом. Вот это да! Теперь, учитывая, что вероятны триллионы и триллионы квантовых результатов каждую секунду, это создаст множество вселенных в огромном море многовариантности (*мультиверсов, multiverses*). Сумасшествием кажется то, что были проведены некоторые базовые эксперименты, включая этот, о котором стало известно в 2019 году (<https://www.iflscience.com/physics/quantum-experiment-sees-two-versions-of-reality-existing-at-the-same-time/>) и который поддерживает идею, что нельзя исключить квантовые мультиверсы. Большинство людей не верят тому, что объяснение множественностью вселенных является правильным, но поскольку математика пока этого не исключает, кто знает?

Эффект наблюдателя оказывает огромное влияние на квантовые вычисления. Мы хотим, чтобы наши квантовые компьютеры дали нам замечательные ответы на чрезвычайно трудные для решения другим способом задачи, но они должны быть изготовлены и работать, минимизируя или утилизируя эффект наблюдателя, чтобы при желании мы могли получать точные ответы.

Теорема об отсутствии клонирования

Родственным принципом, который невероятно важен для квантовой информатики, является *отсутствие клонирования*. Это теорема, в которой говорится, что квантовые состояния не могут быть скопированы напрямую. Вспомним, что измерение квантового состояния приводит это квантовое состояние в классическое постоянное состояние. И в соответствии с эффектом наблюдателя простое наблюдение или измерение квантового состояния меняет его. Это не значит, что «копирование» не может быть сделано, но это должно делаться косвенно. Подробнее об этом – в следующих главах. Теорема об отсутствии клонирования имеет много последствий для квантовых вычислений. Отрицательной стороной является то, что вы не можете создать резервную копию квантового состояния в середине квантового вычисления, как вы можете это сделать при работе с классическим компьютером. Это явление затрудняет копирование и исправление ошибок в квантовых компьютерах и сетевых устройствах. Положительным является то, что это отличное свойство для квантовой криптографии, предотвращающее многие сценарии подслушивания, которые намного проще создавать в классическом мире.

Жуткая запутанность

Теперь пришло время обсудить квантовое свойство, которое часто считается самым странным и досаждало Эйнштейну в последние дни его жизни. Квантовые частицы могут «запутаться» таким образом, что когда квантовое свойство (такое как поляризация, спин, импульс или заряд) одной частицы из пары изменяется, свойства другой пары частиц также немедленно изменяются предсказуемым образом, даже если две частицы разделены очень большими расстояниями. Мы не знаем, почему это происходит или как и почему Эйнштейн назвал это явление «Жуткое действие на расстоянии» («Spooky action at a distance»).

Примечание Запутывание – это только процесс измерения и чтения. Ученые знают, что когда они измеряют свойство одной частицы в паре, другая частица в паре будет иметь то же измеряемое значение. Но если ученые пытаются каким-либо образом манипулировать запутанными частицами, чтобы получить конкретное желаемое новое состояние – скажем, изменить свойство частицы с «0» на «1», – запутывание немедленно прерывается. Мы можем читать информацию, но не передавать ее. Реализация определенного желаемого состояния требует измерения состояния, а измерение состояния нарушает квантовые свойства.

В природе запутывание – это естественный процесс. Это происходит всякий раз, когда любая квантовая частица взаимодействует с другой квантовой частицей. Это происходит все время. Запутанность растет с каждой встреченной частицей. Это нельзя просто остановить. В конечном итоге запутывание приводит к созданию объектов, состоящих из многих частиц, зависящих теперь друг от друга. С точки зрения физики, вы больше не можете говорить о любой запутанной частице как об одной частице. Каждое наблюдение должно быть получено из результатов измерения всех запутанных частиц, участвующих в этой запутанности. В реальном мире запутывания происходит много, и они происходят очень быстро. Квант частицы может легко запутаться с миллиардом других квантовых частиц за миллионные доли секунды.

Хотя квантовые частицы всегда запутываются сами по себе, для целей квантового тестирования ученые намеренно создают или запутывают лишь небольшое количество квантовых частиц. Это потому, что когда вы пытаетесь понять какой-то истинный результат в эксперименте, меньшее количество обычно дает больше. Рассчитывать выяснить что-то, что является результатом взаимодействия миллиардов частиц, – это просто замутить воду.

Таким образом, в экспериментах, где запутанность желательна, ученые будут усердно работать над тем, чтобы изолировать экспериментальную среду и предотвратить любое нежелательное запутывание, создав свои собственные запутывания в гораздо меньших масштабах. Экспериментальная запутанность может быть осуществлена многими разными способами, хотя один из самых распространенных методов – взять один фотон с большой энергией

и разделить его на две части – два фотона с более низкой энергией. Есть несколько других распространенных методов запутывания, но их технически слишком сложно описать, что неуместно для этой книги.

Что касается эксперимента, запутывание должно включать две очень близкие квантовые частицы. Ученым пока не удалось запутать две частицы, которые находятся далеко друг от друга, хотя расстояние все время увеличивается. Однажды запутавшиеся, две частицы могут быть перемещены очень, очень далеко друг от друга и все еще сохраняют переплетение их связей. Хотя когда расстояние увеличивается, существует вероятность того, что взаимодействие запутанных частиц с другими запутанными частицами будет увеличиваться, затрудняя ученым или делая невозможным измерить то, что они хотели от оригинальной частицы, – создать намеренное запутывание.

Ирландский физик Джон С. Белл усилил теорию квантовой запутанности в серии неоспоримых экспериментов, описание которых он опубликовал в 1987 году в своей основополагающей белой книге под названием «Описуемое и неопишуемое в квантовой механике» (Speakable and unspeakable in quantum mechanics, <https://web.archive.org/web/20150412044550/>; http://philosophyfaculty.ucsd.edu/faculty/wuthrich/GSSPP09/Files/BellJohnS1981Speakable_BertlmannsSocks.pdf). Белл исключил «скрытые локальные переменные», которые, как предположил Эйнштейн, были другим возможным, более вероятным объяснением запутанности. Белл доказал, что скрытые местные переменные отсутствуют, что значительно усилило теорию запутывания и всю квантовую физику.

С тех пор его эксперименты повторялись с одинаковым успехом каждый раз и на разных квантовых частицах. Жуткая запутанность была продемонстрирована в фотонах, электронах, нейтрино и даже более крупных молекулах, таких как «букиболлы» (buckyballs). Квантовая запутанность была даже продемонстрирована в макроскопических объектах, таких как алмазы (<https://news.yahoo.com/two-diamonds-linked-strangequantum-entanglement-190805281.html>). Хотя квантовым физикам вовсе не нужны картинки, чтобы поверить или доказать что-либо в квантовой механике, но тем не менее в июле 2019 года ученым удалось запечатлеть первую картину запутанных частиц (<https://phys.org/news/2019-07-scientists-unveil-first-ever-image-quantum.html>), которая одинаково сильно взволновала умы как ученых, так и не ученых.

Декогеренция

Последнее квантовое свойство, которое мы обсудим в этой главе, – это *декогеренция*. Это чрезвычайно важное в квантовой физике и вычислительной технике свойство. Это то, что мы и хотим иметь, и хотим избежать (до поры до времени). Когда квантовая частица или система находится в легко видимом наборе квантовых состояний, мы говорим, что она когерентна или находится в состоянии когерентности. Мы можем легко увидеть результаты ее квантового состояния, которое работает в соответствии со всеми вероятностными ответами волновой функции. Без жесткой изоляции среды любая квантовая частица или система начнет взаимодействовать и запутываться с другими квантовыми частицами. Фактически это миллиарды и миллиарды

взаимодействий в микросекунду. Это происходит даже в том случае, когда мы можем считать, что она находится в вакууме. Например, когда ученые создают искусственный вакуум внутри замкнутого пространства без света или других преднамеренно введенных квантовых частиц в нем, аппарат, используемый для создания вакуума, будет выщелачиваться в вакуум. Это неизбежно. Без экстремальных условий это происходит очень часто и очень быстро. При самых лучших условиях это все же еще случается. Этого нельзя предотвратить.

Каждое нежелательное взаимодействие вызывает запутанность, и теперь ученые, пытающиеся исследовать одну или несколько частиц либо свойств, должны иметь дело с результатами, полученными из более сложных сочетаний многих частиц, чего обычно они не хотели бы. Оригинальные частицы, с которыми они работают, присутствуют, но могут быть легко потеряны среди моря других запутанных частиц, и в таком случае ученым нелегко понять влияние или результаты для исходных частиц, которые они наблюдали и хотели измерить.

Представьте, что вы хотели последовать за одной каплей воды и она упала в океан. Или вы хотели следовать за одним фотоном на пляже в солнечный день. Капля воды все еще будет в океане, но теперь сразу рассеяна среди триллионов и триллионов других капель. Вы могли бы все еще следовать за исходной каплей, но это было бы очень сложно. Вы могли бы отслеживать свой оригинальный фотон на пляже, но только не тогда, когда он не только теряется среди триллиона других фотонов, но и взаимодействует с другими фотонами и другими, как микро-, так и макрочастицами (например, пыль, воздух, ветер). Для любых практических целей уже после нескольких взаимодействий было бы трудно отследить какую-либо отдельную частицу и выяснить, что вызывали или не вызывали все другие запутывания.

Из-за этого для квантовых экспериментов и внутри квантовых компьютеров и других устройств внутренние структуры должны быть очень хорошо изолированы от внешнего мира. Ученые, изучающие кванты, хотят предотвратить столько нежелательного запутывания от происходящего, сколько в человеческих силах. Используют стерильные поверхности с применением одного стабильного элемента, холодные температуры и предельную защиту от внешнего мира. Но когда ученые или механизмы теряют способность отслеживать исходную частицу или свойство/свойства частицы и выяснить первоначально желаемый результат (который всегда в конечном счете будет, несмотря ни на что, получен), квантовая частица или система рассматривается как декогерентная или находящаяся в состоянии декогеренции. Важно отметить, что квантовость частицы или системы не превратилась во что-то еще. Она ни в коей мере не стала неквантовой/классической. Просто отслеживание и понимание происходящего значимым образом стало слишком трудным для наших скудных умов и оборудования.

Иногда декогеренция нам необходима. В квантовой информатике, когда мы хотим получить квантовый ответ и можем записать и обозначить результат, мы должны измерить его, а его измерение все это запутывает и меняет. Каким бы ни было измерительное устройство, оно также состоит из квантовых частиц и свойств и должно взаимодействовать с измеряемой частицей

или свойством. Даже если измерение включает в себя только свет, а свет состоит из фотонов, для того чтобы фотон дал результат и сообщил об этом, он должен «ударить» частицы и отскочить назад. Теперь этот фотон запутан с тем, что он измерял. Таким образом, само по себе измерение будет декогерировать квантовую систему. Это не внезапное изменение квантового состояния в нечто неквантовое, просто это сразу добавляет сложность измерения.

Но тем не менее, чтобы записать квантовый результат конкретного эксперимента или вычисления, мы должны измерить его. Итак, мы хотим проводить измерения, когда и где декогеренция контролируется и минимизируется без того, чтобы измерительная аппаратура декогерировала эти измерения. Нам нужно провести измерения и декогеренцию, чтобы мы могли получить окончательное измерение и ответ. Мы не хотим, чтобы ответом было: иногда А, а иногда В. Нам нужно стабильное значение результата для записи. Можно себе представить, что каждый раз, когда нам нужен был ответ, мы могли бы просто сказать «это диапазон всех возможных ответов в пределах их вероятностей» и остановиться на этом? Мы не могли бы просто сказать, что машина движется со скоростью 100 км/ч. Мы должны были бы сказать, ну, это будет скорость где-то от 0 до 200 км/ч (или какой-либо возможной максимальной скорости), и представить вероятности. Это был бы бездумный способ описания мира, особенно когда все понимают, что машина, определенная как движущаяся со скоростью 100 км/ч, вероятно, не будет двигаться все время со скоростью 100 км/ч. Чтобы дать ответ, мы просто хотели бы получить наиболее вероятный «правильный» ответ, а не некий спектр ответов, соответствующих математике волновой функции. Следовательно, мы хотели бы преднамеренно декогерировать систему только на время необходимого измерения. Мы хотим избежать декогеренции системы до измерения, и как только получим необходимое измерение, она может иметь ту декогеренцию, которая ей нравится. Хотя ученые также хотели бы и пытаются делать несколько измерений без декогеренции системы. Одна из самых больших проблем, если не самая большая, при получении научной информации о квантах – система должна быть защищена от преждевременной декогеренции, пока не проведено окончательное измерение.

Существует много других свойств, принципов и теорий центральной квантовой механики, таких как контекстуальность, которую мы могли бы обсудить, но то, что мы уже обсудили, является отличной основой для главы 2 «Как работают квантовые компьютеры?».

Квантовые примеры в современном мире —

Хотя квантовая механика в основном проявляется на субатомном уровне, ни одна из реальностей нашей жизни не была бы возможной без реального существования и воздействия квантовой механики. Квантовая механика заставляет Солнце светить, является причиной, по которой материя составляет целое, и выступает основой большинства вещей, которые мы наблюдаем на макроскопическом уровне. Когда вы видите докрасна раскаленную печь, то это стало возможным только из-за наличия квантовых эффектов. Квантовая

механика отвечает за наши компьютерные микропроцессоры, транзисторы, резисторы и любые интегральные схемы. Дисковое хранилище и сетевые коммуникации возможны только из-за существования квантовой механики. Ваше соединение Wi-Fi работает только из-за существования квантовых свойств.

Вот другие макроскопические реальности, которые возможны лишь непосредственно в связи с существованием квантовой механики:

- волоконно-оптические кабели;
- лазеры;
- сверхпроводимость;
- сверхтекучие жидкости;
- атомные часы;
- магнитно-резонансная томография (МРТ), –

и не забудем главную причину появления этой книги: квантовые компьютеры и квантовая криптография.

Все эти замечательные вещи, да и вся наша реальность существует и действует только из-за всех невероятных и странных причуд квантовой механики. Я расскажу больше о том, как помогает нам квантовая механика, в главе 5 «Как будет выглядеть постквантовый мир?».

Для дополнительной информации

Область квантовой физики огромна. Темы, рассмотренные в этой главе, в действительности представляют собой только вершину айсберга. Каждая обобщенная тема была освещена в десятках официальных документов и книг, а иногда и сотнях документов и книг. Никакая книга, белая книга или учебник не могут продемонстрировать справедливость квантовой механики. Любой, кто хочет узнать больше, должен просто выбрать несколько источников и постепенно погружаться в них. Часто требуется, по крайней мере, несколько таких источников, внимательно прочитанных или просмотренных, прежде чем даже основы начнут проясняться. С учетом сказанного, вот некоторые из моих лично любимых ресурсов, с которых может начать любой новичок в области квантовой физики:

- *Aaronson Scott* (2013). *Quantum Computing Since Democritus*. Cambridge: Cambridge University Press.
- *Bell Philip* (2018). *Beyond Weird: Why Everything You Knew About Quantum Physics Is Different*. Chicago: University of Chicago Press.
- *Orzel Chad* (2009). *How to Teach [Quantum] Physics to Your Dog*. New York: Scribner.
- *Orzel Chad* (2018). *Breakfast with Einstein: The Exotic Physics of Everyday Objects*. Dallas, TX: BenBella Books, Inc.
- Dr. Mark G. Jackson's Articles for Popular Audiences. <http://physicsjackson.com/articles/>.
- Quantum Physics Blog. <https://www.techbubble.info/blog/quantum-physics>.
- Scott Aaronson Blog. <https://www.scottaaronson.com>.

- Dr. Scott Aaronson's Democritus online courses. <https://www.scottaaronson.com/democritus/>.
- YouTube. Quantum Theory—Full Documentary HD. https://www.youtube.com/watch?v=CBrsWPCp_rs.
- YouTube. Quantum Physics for 7 Year Olds. <https://www.youtube.com/watch?v=ARWBdfWpDyc>.
- YouTube. Neil deGrasse Tyson Explains Quantum Entanglement. <https://www.youtube.com/watch?v=q8CQAOWi2RI>.

Если вы хотите узнать больше о квантовой механике, перейдите на YouTube и/или Amazon и, чтобы увидеть сотни вариантов, просто введите «физика квантовой механики».

Резюме

Если это ваше первое знакомство с квантовой механикой, я надеюсь, что для начала мне удалось показать ее дивную странность. Не стесняйтесь вернуться к этой главе и перечитать ее, когда вы получите больше понимания квантовой механики в последующих главах. Квантовые компьютеры используют эти невероятные квантовые свойства, включая запутанность, неопределенность и суперпозицию, чтобы дать нам ответы, которые просто невозможно получить на традиционных бинарных компьютерах. В главе 2 «Введение в квантовые компьютеры» мы обсудим, как работают квантовые компьютеры и устройства, чтобы дать нам невероятные ответы и решения, на которые можно положиться, и каковы современные достижения в этой области.