МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. А.Н. Косыгина (ТЕХНОЛОГИИ. ДИЗАЙН. ИСКУССТВО)» (ФГБОУ ВО «РГУ им. А.Н. Косыгина»)

Мокряков А.В., Горшков В.В.

Основы квантовых вычислений

Учебное пособие

Допущено к изданию редакционно-издательским советом университета в качестве электронного учебного пособия для подготовки магистров по направлению 01.04.02 – Прикладная математика и информатика

Объем 1,2 МБ, тираж 10

Редакционно-издательский отдел ФГБОУ ВО «РГУ им. А.Н. Косыгина»
115035 Москва, ул. Садовническая, 33, стр. 1
тел. 8-495-811-01-01 доб. 1099
e-mail: riomgudt@mail.ru

Москва
ФГБОУ ВО «РГУ им. А.Н. Косыгина», 2022

Copyright © 2022 ФГБОУ ВО «РГУ им. А.Н. Косыгина»
All Rights Reserved

Copyright © 2022 Мокряков А.В., Горшков В.В.
All Rights Reserved

ISBN 978-5-00181-197-8

УДК 530.145(075)
ББК 22
М 74

М 74 Мокряков А.В., Горшков В.В.
Основы квантовых вычислений: учебное пособие – М.: ФГБОУ ВО «РГУ им. А.Н. Косыгина», 2022.– 1,2 МБ.

В работу включено краткое изложение основ квантовых вычислений и базовых квантовых алгоритмов, также даётся описание кубитов в их математическом и физическом представлениях. Большое внимание уделено рассмотрению текущих мировых исследований в данной области для расширения кругозора молодых учёных. Перед пособием стоит цель познакомить магистров с квантовыми вычислениями в доступной форме, описывая сложные математические понятия простым языком.

Пособие предназначено для обучающихся по направлениям подготовки 01.04.02 Прикладная математика и информатика всех форм обучения и будет использовано при изучении дисциплины «Квантовые алгоритмы и анализ их сложности».

Минимальные системные требования: ПЭВМ, работающая под управлением Windows; оперативная память – 512 Мб; необходимо на винчестере – 512 Мб; операционные системы- Windows XP/Vista/7/8/10/11; дополнительные программные средства – Adobe Acrobat Reader.

Работа подготовлена на кафедре прикладной математики и программирования ФГБОУ ВО «РГУ им. А.Н. Косыгина».

Copyright © 2022 ФГБОУ ВО «РГУ им. А.Н. Косыгина»
All Rights Reserved
Copyright © 2022 Мокряков А.В., Горшков В.В.
All Rights Reserved

СОДЕРЖАНИЕ

1. ПРОГРЕСС В ВЫЧИСЛЕНИЯХ

В последнее время в популярной прессе регулярно появляются истории о разработке малогабаритных квантовых компьютеров и их потенциальных возможностях, в значительной степени обусловленные быстрым продвижением текущих общественных исследований в этой области, началом корпоративных инвестиций и заботой о будущем масштабирование производительности традиционных компьютеров [1-4]. Хотя прогресс в области квантовых вычислений был впечатляющим, существует много открытых вопросов о потенциальных применениях такой системы, о том, как можно создавать такие типы компьютеров и когда эта технология разрушит сегодняшнюю вычислительную парадигму и изменит ли она её.

Цель этого пособия — рассказать о квантовых вычислениях и показать спектр современных исследований, которые относятся к вопросам создания квантового компьютера общего назначения. Прежде чем приступить к изучению возможностей этой новой технологии, полезно рассмотреть происхождение и возможности современных коммерческих вычислительных технологий, экономические факторы, которые стимулировали их развитие, и ограничения, с которыми они начинают сталкиваться. Эта информация обеспечит контекст для понимания уникального потенциала квантовых вычислений наряду с потенциальными проблемами для разработки любой новой и конкурентоспособной вычислительной технологии и послужит сравнительной основой для понимания прогресса в практическом квантовом компьютере.

1.1. Происхождение современных вычислений

Прогресс в одной области науки и техники часто катализирует или ускоряет открытия в другой, создавая новые пути как для новой науки, так и для разработки и внедрения новых технологий. Такие взаимосвязи особенно заметны в развитии вычислительных технологий, которые возникли благодаря тысячелетнему прогрессу в математических и физических науках и положили начало революционной индустрии в середине 20-го века. Менее чем за сто лет исследования, разработки и внедрение практических вычислительных технологий изменили науку, технику и общество в целом.

До середины 20-го века практическими «компьютерами» были не машины, а люди, которые выполняли математические вычисления с помощью простых инструментов, таких как счёты или логарифмическая линейка. Сегодня мы обычно определяем компьютер как сложную машину, которая может решать многие проблемы

быстрее, точнее или точнее, чем человек, путём манипулирования абстрактными представлениями данных, воплощёнными в некоторой физической системе, с использованием набора чётко определенных правил. При соответствующем входе и правильном наборе инструкций компьютер может выдать ответы на множество задач. В начале 1800-х годов Чарльз Бэббидж разработал механический компьютер, «разностную машину», для печати астрономических таблиц, а позже предложил более сложную механическую вычислительную машину, «аналитическую машину». Из-за отсутствия практических технологий производства ни один из них в то время не был построен, но этот двигатель был первой концепцией универсального программируемого компьютера. Современная концепция компьютера получила дальнейшее развитие в 1930-х годах благодаря работам Алана Тьюринга. Его абстрактная математическая модель простого компьютера, способного имитировать любое другое вычислительное устройство, «машина Тьюринга», описывала основные возможности всех цифровых компьютеров.

В то время как вычисления основаны на тысячелетнем исследовании математических принципов, практические устройства требуют конкретной физической реализации абстрактных и теоретических идей. Первые успешные реализации таких устройств появились во время Второй мировой войны. Алан Тьюринг построил специальный электромеханический компьютер для криптоанализа «Бомба» и разработал подробную спецификацию для «автоматического вычислительного механизма», настоящего универсального компьютера с хранимой программой. В Германии в рамках отдельной разработки Конрад Цузе создал Z1, первый программируемый компьютер, использующий электромеханические реле. После войны так называемая архитектура фон Неймана — переосмысление универсальной машины Тьюринга в терминах модели вычислений с хранимой программой — стала доминирующей архитектурой для большинства компьютерных систем.

В последующие десятилетия, в основном благодаря военному финансированию, производительность и возможности компьютеров продолжали улучшаться. Физические компоненты, используемые для создания компьютеров, также со временем улучшались. Поскольку зарождающаяся компьютерная индустрия была слишком мала, чтобы стимулировать развитие технологий, её разработчики использовали технологии (вакуумные лампы, затем транзисторы и, наконец, интегральные схемы), которые были разработаны для поддержки радио, телевидения и телефонии, которые были движущими

коммерческими приложениями день. Со временем компьютерная индустрия стала намного больше, чем военный сектор, с которого она началась, и стала достаточно большой, чтобы поддерживать разработку индивидуальных технологий. Сегодня вычисления являются одним из крупнейших коммерческих двигателей разработки интегральных схем, и многие другие области используют интегральные схемы, разработанные для вычислительной отрасли, для своих нужд. В результате современные электронные компьютеры — от мобильных устройств и ноутбуков до суперкомпьютеров — являются плодами огромного прогресса в понимании человеком физических материалов и систем и в контроле над ними.

1.2. Квантовые вычисления

В то время как современные вычислительные машины используют тонкий контроль над природой для создания конструкций невероятной сложности, представление и логическую обработку информации в этих машинах можно объяснить с помощью законов классической физики (в то время как законы квантовой механики должны применяться для проектирования или объяснения процессов). работы полупроводниковых материалов, ширина запрещённой зоны которых позволяет реализовать сегодня широко распространённые обычные компьютерные логические вентили, сама природа логической обработки информации основана на потоке классической модели заряженной частицы). Эти классические описания электромагнетизма и ньютоновской физики обеспечивают интуитивное и детерминистическое объяснение физической вселенной, но они не могут предсказать все наблюдаемые явления. Это осознание, сделанное на рубеже 20-го века, привело к самой важной трансформации в физике: открытию принципов квантовой механики. Квантовая механика (или квантовая физика) — это теория физического мира, которая является не детерминированной, а вероятностной, с присущей ей неопределённостью. Хотя динамика, которую он описывает в малом масштабе, экзотична и противоречит здравому смыслу, он точно предсказывает широкий спектр наблюдаемых явлений, которые не могла дать классическая физика, и воспроизводит правильные классические результаты для более крупных систем. Развитие этой области изменило то, как учёные понимают природу. Очень маленькие системы, поведение которых не может быть адекватно аппроксимировано уравнениями классической физики, часто называют «квантовыми системами».

В то время как классическая физика часто является хорошим приближением наблюдаемых явлений, вся материя в своей основе является квантово-механической, включая материалы, из которых построены современные компьютеры. Однако несмотря на то, что конструкция их аппаратных компонентов все больше определяется квантовыми свойствами материалов, а постоянно сокращающийся размер этих компонентов означает, что квантовые явления вводят больше ограничений на их конструкцию, принципы и операции, которые реализуют эти компьютеры. остались классическими.

Несмотря на невероятную мощь современных компьютеров, есть приложения, которые им трудно вычислить, но которые, кажется, легко «вычисляются» квантовым миром: оценка свойств и поведения квантовых систем. В то время как современные классические компьютеры могут моделировать простые квантовые системы и часто находят полезные приближенные решения для более сложных, для многих таких задач объем памяти, необходимый для моделирования, растёт экспоненциально с размером моделируемой системы.

В 1982 году физик Ричард Фейнман предположил, что явления квантовой механики сами по себе могут использоваться для моделирования квантовой системы более эффективно, чем простое моделирование на классическом компьютере [5, 6]. В 1993 году Бернстайн и Вазирани показали [7], что квантовые компьютеры могут нарушать расширенный тезис Чёрча-Тьюринга — основополагающий принцип информатики, согласно которому производительность всех компьютеров лишь полиномиально выше, чем у вероятностной машины Тьюринга [8, 9]. Их квантовый алгоритм предлагал экспоненциальное ускорение по сравнению с любым классическим алгоритмом для определенной вычислительной задачи, называемой рекурсивной выборкой Фурье. Другой пример квантового алгоритма, демонстрирующего экспоненциальное ускорение для другой вычислительной задачи, был предоставлен в 1994 году Дэном Саймоном [10]. Квантовые вычисления на сегодняшний день являются единственной моделью вычислений, которая нарушает расширенный тезис Черча-Тьюринга, и, следовательно, только квантовые компьютеры способны к экспоненциальному ускорению по сравнению с классическими компьютерами.

В 1994 году Питер Шор показал, что несколько важных вычислительных задач в принципе можно было бы решить значительно эффективнее с помощью квантового компьютера — если бы такую машину удалось построить. В частности, он вывел алгоритмы факторизации больших целых чисел и быстрого решения дискретных

логарифмов — задач, на решение которых даже самому мощному сегодняшнему компьютеру могут уйти тысячи или миллионы лет — или даже время жизни Вселенной. Это было поразительное открытие, потому что оно также предполагало, что любой, у кого есть реальный квантовый компьютер, может взломать криптографические коды, которые используют эти проблемы, ставя под угрозу безопасность зашифрованных сообщений и зашифрованных хранимых данных и потенциально раскрывая защищенные секреты или личную информацию. Эти результаты вызвали интерес у исследователей к разработке других квантовых алгоритмов с экспоненциально более высокой производительностью, чем у классических алгоритмов, и к попыткам создать основные квантовые строительные блоки, из которых можно было бы построить квантовый компьютер.

За последние несколько десятилетий эти исследования продвинулись до такой степени, что были построены очень простые квантовые компьютеры, и появляется позитивный прогноз, основанный на предположении, что сложность этих машин будет расти экспоненциально со временем, аналогично росту, который было достигнуто в производительности классических компьютеров. Учитывая важность этого предположения о масштабировании для будущего квантовых вычислений, понимание факторов, влияющих на масштабирование, имеет решающее значение.

1.3. Закон Мура

В то время как первые компьютеры были огромными, дорогими и энергоёмкими устройствами, часто финансируемыми государством, сегодняшние компьютеры значительно меньше, дешевле, эффективнее и мощнее в результате усовершенствований в аппаратном, программном обеспечении и архитектуре. Современные смартфоны, компьютеры, помещающиеся в карман, обладают такой же вычислительной мощностью, как самые быстрые суперкомпьютеры 20-летней давности. Низкая стоимость компьютерного оборудования привела к проникновению компьютеров в различные среды и позволила объединить от десятков до сотен тысяч компьютеров, которые предоставляют услуги веб-вычислений, от которых многие стали зависеть. В настоящее время компьютеры широко используются во все большем количестве промышленных товаров, от стиральных машин до поющих поздравительных открыток. В этом разделе описывается, как это произошло, что раскрывает несколько уроков и проблем для любой новой вычислительной технологии.

Процесс, используемый для создания интегральных схем, ключевых компонентов современных компьютеров, возник как незапланированный шаг вперёд на фоне усилий 1960-х годов по улучшению процесса промышленного производства транзисторов. Транзисторы — это небольшие электрические устройства, которые можно использовать в качестве электронных переключателей или усилителей. В то время они использовались в различных электронных устройствах, включая радиоприёмники, телевизоры, аудиоусилители и ранние компьютеры. Усилия по повышению качества транзисторов и производительности производства (что снижает затраты) привели к нескольким изобретениям в Fairchild Semiconductor, начинающей компании по производству транзисторов. Первым был метод изготовления транзисторов, называемый «планарным процессом», который позволял транзисторам работать после изготовления на поверхности плоского куска кремния. Раньше материал снаружи транзистора нужно было вытравливать, создавая «массу» кремниевого транзистора. Планарные процессы позволили изготовить множество транзисторов на данном куске кремния, который затем можно было разрезать, чтобы отделить их друг от друга. Второе изобретение заключалось в соединении нескольких таких транзисторов вместе через металлический слой на поверхности кремния для создания полной схемы. Поскольку эта транзисторная схема была интегрирована в один кусок кремния, результат получил название «интегральная схема» или ИС. Эта концепция соединения нескольких устройств на одной подложке была продемонстрирована годом ранее Джеком Килби из Texas Instruments на грубом германиевом прототипе, также с целью снижения стоимости и повышения надёжности транзисторных схем.

Производственный процесс создания интегральной схемы, который со временем становился все более сложным, можно рассматривать как тип многослойного процесса печати. Транзистор можно создать путём последовательной «печати» различных форм в ряду слоёв. Для интегральной схемы формы всех транзисторов схемы «печатаются» одновременно, слой за слоем, на куске кремния. Процесс занимает одинаковое количество времени независимо от количества транзисторов в схеме; дальнейшее снижение затрат может быть достигнуто за счёт одновременного изготовления нескольких копий схемы на большом куске кремния, называемом пластиной. В результате стоимость производства ИС определяется размером кремния, который она занимает (который определяет, сколько схем может быть изготовлено при обработке одной пластины), а не количеством транзисторов в схеме.

В 1964 году Гордон Мур, также работавший в Fairchild, изучил затраты на создание интегральных схем. Он заметил, что из-за усовершенствований конструкции и обработки количество транзисторов, которые можно было экономично напечатать на каждой схеме, со временем увеличивалось в геометрической прогрессии, удваиваясь примерно каждый год. Мур предположил, что технология изготовления ИС будет продолжать совершенствоваться с экспоненциальным ростом количества транзисторов на интегральную схему, и в статье 1964 года он размышлял о том, как мир будет использовать все эти устройства. В последующие десятилетия его гипотеза об экспоненциальном росте подтвердилась как точная и теперь её обычно называют «законом Мура».

Закон Мура — это не физический закон; это просто эмпирическая производственная тенденция для отрасли интегральных схем из-за ее бизнес-цикла. В то время как экспоненциальный рост возможностей интегральных схем обычно рекламируется, затраты, которые поддерживают этот рост, часто упускаются из виду. За последние 50 лет доходы индустрии компьютерного оборудования также росли в геометрической прогрессии, увеличившись более чем в тысячу раз, и сегодня составляют чуть менее полутриллиона долларов США в год. За тот же период доля этих доходов, реинвестированных в отраслевые исследования и разработки (НИОКР), оставалась примерно постоянной, а это означает, что финансовые затраты на технологические усовершенствования, лежащие в основе закона Мура, также экспоненциально росли. Интересно, что в дополнение к этому экспоненциальному росту, как стоимость строительства завода по производству ИС, так и стоимость разработки конструкции, которая будет производиться, также демонстрировали экспоненциальный рост.

Это иллюстрирует важный момент: закон Мура является результатом благотворного цикла, когда усовершенствования в производстве интегральных схем позволяют производителю снизить цену на свой продукт, что, в свою очередь, заставляет его продавать больше продуктов и увеличивать свои продажи и прибыль. Этот увеличенный доход затем позволяет им снова улучшить производственный процесс, что на этот раз сложнее, поскольку более простые изменения уже были сделаны (это одна из причин так называемого закона Рока, который гласит, что стоимость строительства новых мощностей по производству полупроводников удваивается каждые 4 года). Ключом к этому циклу является создание растущего рынка для своего продукта. Для интегральных схем новая доступность заставляет разработчиков многих продуктов общего назначения

заменять некоторые существующие механизмы на ИС, потому что это делает продукт лучше или дешевле (например, замена замка с ключом на электронный замок), что увеличивает рынок ИС, создавая растущий доход, необходимый для дальнейшего масштабирования их сложности.

Трудно достичь такого типа экспоненциального масштабирования без такого благотворного цикла. Это видно из исторического примера попыток изготовления транзисторов из материала, отличного от кремния. Поскольку транзисторы, изготовленные из арсенида галлия (GaAs), обладают более высокой производительностью, чем кремниевые транзисторы, исследователи полагали, что компьютеры, построенные на микросхемах GaAs, будут иметь более высокую производительность, чем компьютеры, построенные с использованием кремниевых микросхем. Учитывая это обещание, к середине 1970-х годов многие исследовательские группы, а позже и компании, работали над созданием интегральных схем с использованием GaAs-транзисторов. Однако к тому времени, когда эти усилия начались, отрасль кремниевых ИС была большой, и компании уже начали реинвестировать часть своих доходов в усовершенствование своего производственного процесса. Процесс производства GaAs существенно отличался от процесса производства кремния, поэтому разработчикам потребовалось разработать новые этапы изготовления, специфичные для GaAs. Это событие поставило производителей GaAs в ситуацию «Уловка-22»: чтобы финансировать свои производственные исследования и разработки, им нужны были стабильные продажи; чтобы добиться стабильных продаж, им требовались самые современные технологии производства, чтобы конкурировать с кремниевыми альтернативами, которые постоянно совершенствовались. Промышленность так и не смогла разорвать этот цикл, и попытки создать коммерчески успешные микросхемы на основе GaAs в конечном итоге потерпели неудачу; цифровые GaAs – информационные системы общего назначения так и не стали конкурентоспособными.

Благотворный цикл, лежащий в основе закона Мура, носит не только финансовый характер. Это также зависит от наличия динамичной экосистемы для поддержки роста рынка. Во многих отношениях индустрия интегральных схем создала — а затем стала зависеть от неё — Силиконовую долину, которая позже стала глобальной и заняла сегодняшнее положение. Растущие возможности и рынок компьютерного оборудования привлекли венчурное финансирование, вспомогательные отрасли и, что наиболее важно, таланты в этой области. Затем это растущее сообщество смогло решить

ранее неразрешимые проблемы, что ещё больше способствовало прогрессу и росту отрасли, что, в свою очередь, привлекло в этот район ещё больше людей. Результат этого благотворного цикла поразителен. В современных технологиях цифровой вентиль, простой строительный блок компьютера, стоит около нескольких миллионных долей пенни (100 000 000 вентилей за доллар), и каждый вентиль может вычислить свой результат менее чем за 10 пикосекунд (то есть за одну сотую доли секунды). миллиардная доля секунды) при достаточно низком уровне мощности для работы в сотовом телефоне.

Вывод: Закон Мура для интегральных схем стал результатом благотворного цикла, в котором улучшенная технология приносила экспоненциально растущий доход, позволяя реинвестировать в исследования и разработки и привлекать новые таланты и отрасли, чтобы помочь внедрять инновации и масштабировать технологию до следующего уровня.

1.4. Преобразование транзисторов в дешёвые компьютеры

Закон Мура о масштабировании технологии примерно вдвое снижает стоимость изготовления транзистора каждые два года. За последние полвека это привело к снижению затрат более чем в 30 миллионов раз. Хотя это снижение стоимости транзисторов сделало производство ИС с возрастающей сложностью транзисторов экономически выгодным, проектирование этих сложных ИС становится все более сложным. Спроектировать схему с 8 транзисторами несложно; разработка схемы со 100 миллионами транзисторов — это совсем другая история. Чтобы справиться с этой растущей сложностью, разработчики вычислительного оборудования создали новые способы мышления о транзисторных схемах, которые позволили им рассуждать о меньшем количестве объектов. Первоначально они думали о соединении отдельных транзисторов, но вскоре они начали думать о «логических вентилях» — наборах транзисторов, которые можно было представить и смоделировать с помощью булевой логики (правила, объединяющие сигналы, которые могут быть либо ложными (представленными как 0), либо или true (представлено как 1) через операции, которые дают определенные выходные данные). Поскольку сложность продолжала расти, логические элементы были сгруппированы в более крупную схему, такую как сумматор или блок памяти, что снова уменьшило сложность, с которой должен был работать разработчик. Эти разные уровни мышления о дизайне, которые позволяют людям создавать системы, не задумываясь о каждой детали сразу, называются «абстракциями».

Абстракции позволяют концептуально сгруппировать основные компоненты компьютера по форме или функции.

Компьютер — ещё одна дизайнерская абстракция. Он представляет собой транзисторную схему, функция которой управляется набором инструкций, считываемых из подключённой памяти. Как только стало возможным создавать сложные интегральные схемы, стало возможным интегрировать небольшой компьютер в одну ИС, создавая «микрокомпьютер» или «микропроцессор». Эта конструкция значительно упростила использование дешёвых транзисторов; новые приложения больше не требовали проектирования и изготовления ИС для конкретного приложения, а вместо этого могли быть реализованы путём изменения инструкций, предоставляемых существующему микропроцессору, для создания желаемого решения. Простота разработки и развёртывания компьютерных решений в сочетании со снижением стоимости вычислений значительно увеличили спрос на устройства этого типа. Таким образом, вездесущность вычислений обеспечивается (за счёт более дешёвых вычислений) и позволяет (за счёт более высоких доходов) закону Мура. Вычислительная техника — это один из способов, с помощью которого индустрия создаёт продукты, которые люди хотят покупать, из все более дешёвых транзисторов.

Дальнейшие выгоды от экспоненциально падающей стоимости транзисторов потребовали создания множества уровней абстракции, подобных описанным выше, а также нового программного обеспечения (компьютерных программ) и сред проектирования. Хотя разработка этих программ и сред проектирования была дорогостоящей, их стоимость поддерживалась потоками доходов от предыдущих продуктов и прогнозируемыми доходами от будущих продуктов, которые они дадут. Тем не менее, даже с этой дополнительной поддержкой, разработка современного чипа по-прежнему стоит дорого, более 100 миллионов долларов. Поскольку стоимость каждого устройства складывается из производственных затрат плюс амортизированная стоимость проектирования, вычисления на основе ИС дёшевы только в том случае, если они продаются в достаточно больших объёмах (обычно 10 миллионов единиц или более), гарантируя, что амортизированная стоимость проектирования не будет преобладать над общей стоимостью. стоимость производства. Именно амортизация затрат на проектирование делает массовые вычислительные устройства намного более бюджетными, чем специализированные компьютеры.

Новые вычислительные подходы, такие как квантовые вычисления, которые изменяют фундаментальные строительные блоки компьютера, потребуют создания не только нового типа аппаратных строительных блоков, но и новых уровней абстракции, программного обеспечения и сред проектирования, чтобы позволить разработчикам создавать и использовать эти систем, если их сложность должна будет масштабироваться с течением времени. Затраты на создание этих новых аппаратных и программных инструментов важны для новых технологий, поскольку цена первых машин должна быть достаточно высокой, чтобы начать возмещать часть затрат. Эта надбавка всегда наказывает новые подходы при конкуренции с признанным игроком.

1.5. Замедление в масштабировании

Хотя закон Мура отражает большой прогресс в классических вычислениях за несколько десятилетий, экспоненциальный тренд не может поддерживаться бесконечно из-за физических ограничений и конечного размера мирового рынка. Хотя существует много споров о том, когда именно это масштабирование прекратится, за последнее десятилетие признаки конца масштабирования стали более ясными. Поскольку закон Мура на самом деле касается стоимости транзисторов, одним из признаков проблем с масштабированием является тот факт, что стоимость транзисторов не снижается историческими темпами в самых передовых технологиях. консорциум, который был создан, чтобы помочь поддерживать масштабирование технологий в соответствии с законом Мура и устранить возможные препятствия на пути к этому, решил прекратить свои прогнозы масштабирования с размерами элементов 5-7 нанометров, ожидаемыми примерно в 2021 г.

Замедление роста также проявляется в тенденциях чистой выручки в отрасли интегральных схем, как показано на рис. 1.1. Этот полулогарифмический график дохода с течением времени показывает прямую линию, когда рост дохода является экспоненциальным. Данные показывают сильный экспоненциальный рост доходов до 2000 года, за которым следует снижение темпов роста. Этот график указывает на то, что благотворный цикл, когда каждое улучшение технологии приносило отрасли больше денег, начал замедляться. Это замедление роста доходов, вероятно, повлияет на циклы разработки технологий, что повлияет на масштабирование технологий. Замедление роста неудивительно: при доходе в 300–400 миллиардов долларов эта отрасль представляет собой несколько процентов вклада производственного сектора в мировой ВВП. Он не может вечно расти быстрее, чем мировой ВВП.

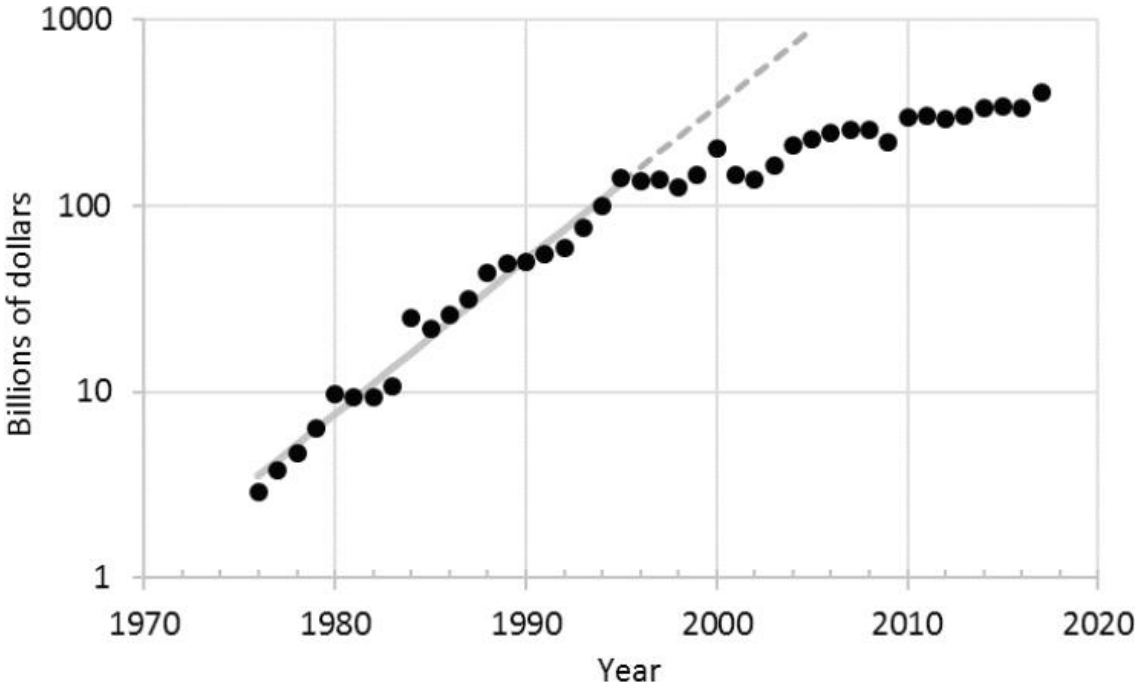


Рис 1.1. Общий годовой объем продаж полупроводников в мире в миллиардах долларов показан на полулогарифмическом графике с линией тренда. На этом графике показан почти экспоненциальный рост продаж примерно до 1995 г. (серая линия тренда соответствует экспоненциальному росту с годовым темпом роста 21 процент), за которым следует более скромный рост [11].

1.6. Кванты: новый подход к вычислениям

Именно на этом фоне появились теория и прототипы квантовых вычислений. Как отмечалось в разделе 1.2, квантовые вычисления используют совершенно другой подход к вычислениям, используя некоторые необычные свойства квантового мира. Когда идея была официально предложена в 1980-х, а новые алгоритмы были открыты в 90-х, никто не знал, как на самом деле построить машину такого типа. За последние два десятилетия усилия по созданию работающего квантового компьютера достигли заметного прогресса, возродив интерес к потенциалу этой технологии. Ещё неизвестно, смогут ли или будут ли практические квантовые компьютеры разрабатываться таким образом, чтобы поддерживать рост вычислительных возможностей по закону Мура. Неудачный эксперимент с ИС на основе арсенида галлия иллюстрирует сложность попытки выйти на устоявшийся рынок с существующим доминирующим игроком. Тем не менее, квантовые вычисления являются единственной действительно новой моделью вычислений, которая была предложена в том смысле, что она не связана расширенным тезисом Черча-Тьюринга. Как более общая модель

вычислений — во многом так же, как квантовая механика является более общей моделью физики, чем классическая механика, — квантовые вычисления обладают теоретическим потенциалом для решения некоторых проблем, с которыми не может реально справиться ни один классический компьютер. Это «квантовое преимущество», которое может проявляться скорее, как подрывная, а не постепенная инновация, делает квантовые вычисления такими интересными и мотивирует коммерческий интерес к квантовым вычислениям.

В следующей главе описываются физические явления, лежащие в основе квантовых вычислений, и сравниваются связанные с ними принципы работы с принципами работы обычных компьютеров. В последующих главах описываются задачи, в которых квантовые компьютеры потенциально могут превзойти классические компьютеры, их значение для криптографии, аппаратное и программное обеспечение, необходимое для создания работающего квантового компьютера, а также сильные и слабые стороны лежащих в основе физических технологий для создания квантовых компьютеров. Пособие завершается оценкой возможности практического внедрения квантового компьютера, соответствующими сроками и необходимыми ресурсами, а также вехами и показателями, которые можно использовать для отслеживания будущего прогресса.

2. КВАНТОВЫЕ ВЫЧИСЛЕНИЯ: НОВАЯ ПАРАДИГМА

Современные компьютеры работают, преобразовывая информацию в последовательность двоичных цифр или битов и оперируя этими битами с помощью интегральных схем (ИС), содержащих миллиарды транзисторов. Каждый бит имеет только два возможных значения, 0 или 1. Благодаря манипуляциям с этими так называемыми двоичными представлениями компьютеры обрабатывают текстовые документы и электронные таблицы, создают удивительные визуальные миры в играх и фильмах и предоставляют веб-сервисы, к которым многие пришли. зависеть.

Квантовый компьютер также представляет информацию в виде последовательности битов, называемых квантовыми битами или кубитами. Как и обычный бит, кубит может быть либо 0, либо 1, но в отличие от обычного бита, который может быть только 0 или 1, кубит также может находиться в состоянии, когда он находится в обоих состояниях одновременно. При распространении на системы многих кубитов эта способность находиться во всех возможных бинарных состояниях одновременно приводит к потенциальной вычислительной мощности квантовых вычислений. Однако правила, управляющие квантовыми системами, также затрудняют использование этой силы. Как лучше всего использовать квантовые свойства — и характер улучшений, которые эти свойства делают возможными — не является ни тривиальным, ни очевидным.

Эта глава представляет собой введение в некоторые уникальные свойства квантового мира, показывая, как одни из них обеспечивают вычислительные преимущества, а другие ограничивают возможности использования этих преимуществ. Механизмы управления классическими и квантовыми битами сравниваются и противопоставляются, чтобы проиллюстрировать уникальные проблемы и преимущества квантовых вычислений. Глава завершается описанием типов квантовых компьютеров, которыми в настоящее время занимаются исследователи, и даёт первый взгляд на прогресс, который будет оцениваться в следующей главе.

2.1. Неинтуитивная физика квантового мира

Первоначально представленная в начале 20-го века, квантовая механика является одной из наиболее хорошо проверенных моделей для объяснения физического мира. Теория — то есть лежащие в основе абстрактные правила и их математические представления — описывает поведение частиц на очень малых расстояниях и в энергетических

масштабах. Эти свойства являются основой для понимания физических и химических свойств всей материи. Квантовая механика даёт те же наблюдаемые и интуитивные результаты, которые мы ожидаем для больших объектов, но её описания мелкомасштабного поведения субатомных частиц, хотя и точные, экзотичны и неинтуитивны (этот простой обзор квантовых явлений призван обеспечить контекст для обсуждения квантовые вычисления. Фундаментальная теория и научная история в этой области увлекательны и обширны, и полностью не могут быть переданы в этом пособии.

Согласно теории, квантовый объект обычно не существует в полностью детерминированном и познаваемом состоянии. На самом деле каждый раз, когда кто-то наблюдает за квантовым объектом, он выглядит как частица, но, когда его не наблюдают, он ведёт себя как волна. Этот так называемый корпускулярно-волновой дуализм приводит ко многим интересным физическим явлениям.

Например, квантовые объекты могут одновременно существовать в нескольких состояниях, причём каждое из состояний суммируется и интерферирует, подобно волнам, определяя общее квантовое состояние. В общем случае состояние любой квантовой системы описывается в терминах «волновых функций». Во многих случаях состояние системы может быть выражено математически как сумма возможных влияющих состояний (строго говоря, каждое из влияющих состояний также называется «волновой функцией»; состояние любой когерентной квантовой системы определяется волновая функция), каждая из которых масштабируется комплексным[1] коэффициентом, отражающим относительный вес состояния. Такие состояния называются «когерентными», потому что содействующие состояния могут конструктивно и деструктивно интерферировать друг с другом, подобно волновым фронтам[2].

Однако при попытке наблюдать квантовую систему наблюдается только один из её компонентов с вероятностью, пропорциональной квадрату абсолютного значения её коэффициента. Для наблюдателя

---

[1] Волнообразная природа волновой функции означает, что коэффициенты могут описывать как амплитуду, так и фазу этого состояния. В этом использовании «комплексное» означает число, которое представлено двумя действительные числа, одно из которых определяет амплитуду, а другое — фазу. Это часто представляется как $Ae^{i\theta}$, где A — амплитуда, а θ — фазовый сдвиг. Фазовый сдвиг $\pi/2$ или 90 градусов записывается как i и фазовый сдвиг на π или 180 градусов равен -1.

[2] Квантовые системы, которые не являются полностью когерентными, должны быть представлены с использованием «матрицы плотности», которая определяет классическую вероятность того, что система находится в каком-то конкретном квантовом состоянии — в этом случае возможные содействующие состояния не мешают друг другу.

система всегда будет выглядеть классической при измерении. Наблюдение за квантовым объектом (или квантовой системой, т. е. системой квантовых объектов), формально называемое «измерением», происходит при взаимодействии объекта с некоторой более крупной физической системой, извлекающей из него информацию. Измерение коренным образом разрушает квантовое состояние: оно «сворачивает» аспект волновой функции, который был измерен, в одно наблюдаемое состояние, что приводит к потере информации. После измерения волновая функция квантового объекта соответствует состоянию, которое было обнаружено, а не состоянию до измерения.

Чтобы визуализировать это, представьте себе обычную монету на столе. В классическом мире, с которым мы сталкиваемся ежедневно, её состояние либо «Орёл вверху» (U), либо «Орёл вниз» (D). Квантовая версия монеты будет существовать в комбинации или «суперпозиции» обоих состояний одновременно. Волновую функцию квантовой монеты можно представить как взвешенную сумму обоих состояний, масштабированную с помощью коэффициентов C_U и C_D. Однако попытка наблюдать за состоянием квантовой монеты приведёт к тому, что она окажется только «орлом вверх» или «орлом вниз» — при измерении она окажется только в одном из двух состояний с вероятностью, пропорциональной квадрату соответствующего коэффициент.

Поскольку пара обычных монет имеет четыре возможных состояния (UU, UD, DU и DD), пара квантовых монет может существовать как суперпозиция этих четырёх обычных состояний, каждое из которых взвешивается собственным коэффициентом, C_{UU}, C_{UD}, C_{DU}, C_{DD} — и так далее для больших коллекций квантовых монет.

При измерении пара квантовых монет будет выглядеть как пара классических монет — только в одной из четырёх возможных конфигураций на столешнице. Точно так же система из n квантовых монет будет наблюдаться только в одном из 2^n возможных состояний.

При некоторых обстоятельствах два или более квантовых объекта в системе могут быть неразрывно связаны, так что измерение одного диктует возможные результаты измерения для другого, независимо от того, насколько далеко друг от друга находятся два объекта. Свойство, лежащее в основе этого явления, известное как «запутанность», является ключом к потенциальной мощи квантовых вычислений.

Эволюция любой квантовой системы определяется уравнением Шредингера, которое описывает, как волновая функция системы изменяется в зависимости от энергетического окружения, в котором

она находится. Эта среда определяется так называемым гамильтонианом системы, математическим представлением энергий, являющихся результатом всех сил, действующих на все элементы системы[3]. Следовательно, чтобы управлять квантовой системой, необходимо тщательно контролировать её энергетическую среду, как путём изоляции системы от остальной части Вселенной (которая содержит силы, которые нелегко контролировать), так и путём преднамеренного применения энергетических полей в области изоляции, чтобы вызвать желаемое поведение. На практике полная изоляция невозможна, хотя взаимодействие с окружающей средой можно свести к минимуму; квантовая система в итоге будет обмениваться некоторой энергией и информацией с более широкой средой с течением времени, процесс, известный как «декогеренция». Это можно представить себе как среду, постоянно производящую небольшие случайные измерения системы, каждое из которых вызывает частичный коллапс волновой функции.

Уникальные свойства, описанные выше и кратко изложенные во вставке 2.1, были выявлены в результате основополагающих научных открытий. При тщательном контроле эти неотъемлемые характеристики материи также представляют собой новые потенциальные парадигмы для инженерии, в частности, для кодирования, манипулирования и передачи информации.

2.2. Ландшафт квантовой технологии

За последние несколько десятилетий был достигнут значительный прогресс в исследованиях и разработках по управлению и использованию мощности квантовых систем, раскрывая потенциал преобразующих квантовых технологий. Хотя область квантовых вычислений была, пожалуй, наиболее заметной в глазах общественности, важно признать, что спектр приложений квантовых явлений шире, чем только квантовые вычисления. Под общим заголовком квантовой информатики области квантовой связи и сетей, а также квантового зондирования и метрологии также являются процветающими областями фундаментальных научных исследований с определенными технологическими целями. Хотя эти области находятся на разных уровнях технологической зрелости, границы между ними не всегда легко определить, потому что все области

[3] Строго говоря, гамильтониан — это математическое описание среды, которое для квантовой -механическая система, принимает форму оператора, однако этот термин часто также используется для обозначения самой окружающей среды.

Вставка 2.1.

Уникальные свойства квантового мира.

Теория квантовой механики представляет собой математическое описание мира в очень малых масштабах и является наиболее точной теорией для понимания и предсказания свойств физической вселенной. Квантовые взаимодействия совершенно не похожи на те, с которыми люди сталкиваются каждый день. Некоторые из определяющих принципов квантовой механики описаны ниже.

Корпускулярно-волновой дуализм. Квантовый объект обычно обладает как волновыми, так и свойствами частицы. Хотя эволюция системы следует волновому уравнению, любое измерение системы вернёт значение, согласующееся с тем, что она является частицей.

Суперпозиция. Квантовая система может находиться в двух или более состояниях одновременно, что называется «суперпозицией» состояний или «состоянием суперпозиции». Волновую функцию для такого состояния суперпозиции можно описать как линейную комбинацию участвующих состояний с комплексными коэффициентами. Эти коэффициенты описывают величину и относительные фазы между участвующими состояниями.

Когерентность. Когда состояние квантовой системы может быть описано набором комплексных чисел, по одному для каждого базисного состояния системы, состояние системы называется «когерентным». Когерентность необходима для квантовых явлений, таких как квантовая интерференция, суперпозиция и запутанность. Небольшие взаимодействия с окружающей средой вызывают медленную декогерентность квантовых систем. Взаимодействия с окружающей средой делают даже комплексные коэффициенты для каждого состояния вероятностными.

Запутанность. Особое свойство некоторых (но не всех) состояний многочастичной суперпозиции, когда измерение состояния одной частицы приводит к коллапсу состояния других частиц, даже если частицы находятся далеко друг от друга и не могут взаимодействовать. Это возникает, когда волновые функции для разных частиц неразделимы (в математических терминах, когда волновая функция для всей системы не может быть записана как произведение волновых функций для каждой частицы). Классического аналога этому явлению нет.

Измерение. Измерение квантовой системы коренным образом меняет её. В случае, когда измерение даёт чётко определенное значение, система остаётся в состоянии, соответствующем измеренному значению. Это обычно называют «схлопыванием волновой функции».

Контролируемое использование этих свойств создаёт новые потенциальные парадигмы для инженерии.

основаны на одних и тех же основных явлениях и сталкиваются со многими одинаковыми проблемами [12]. Все они используют уникальные свойства квантовых систем, основаны на одной и той же базовой физической теории и используют много общих аппаратных средств и лабораторных методов. В результате их прогресс является взаимозависимым.

Область квантовой информатики обычно исследует, как информация может быть закодирована в квантовой системе, включая связанную статистику, ограничения и уникальные возможности квантовой механики. Эта область обеспечивает большую часть основы для квантовых вычислений, связи и зондирования.

Исследования и разработки в области квантовой связи сосредоточены на передаче или обмене информацией путём её кодирования в квантовую систему. Протоколы квантовой связи, вероятно, будут необходимы для квантовых вычислений — будь то для передачи информации от одной части аппаратного обеспечения квантового компьютера к другой или для обеспечения связи между квантовыми компьютерами. Подобластью квантовой связи является квантовая криптография, в которой квантовые свойства используются для разработки систем связи, которые не могут быть перехвачены наблюдателем. Наиболее ярким примером является квантовое распределение ключей (КРК), основанный на квантовых измерениях метод распределения криптографических данных). Самый известный протокол, называемый BB84, был разработан Чарли Беннеттом и Жилем Брассаром в 1984 г. Этот протокол был экспериментально опробован как по оптоволоконным кабелям, так и для работы через спутник. Это даже привело к созданию нескольких компаний и коммерческих продуктов. Хотя КРК и квантовая криптография в целом не устраняют риск атак по побочным каналам и в настоящее время обходятся дороже, чем классические методы защиты, теоретические и экспериментальные исследования в данной области продолжают развиваться.

Квантовое зондирование и метрология включают изучение и разработку квантовых систем, чья чрезвычайная чувствительность к возмущениям окружающей среды может быть использована для измерения важных физических свойств (таких как магнитные поля, электрические поля, гравитация и температура) с большей точностью, чем это возможно с помощью классических методов. технологии. Квантовые датчики обычно основаны на кубитах и реализуются с

использованием многих одних и тех же физических систем[4], используемые в экспериментальных квантовых компьютерах.

Квантовые вычисления, которым уделяется основное внимание в этом пособии, используют квантово-механические свойства интерференции, суперпозиции и запутанности для выполнения вычислений, которые примерно аналогичны (хотя они работают совершенно иначе) тем, которые выполняются на классическом компьютере. В общем, квантовый компьютер определяется как физическая система, состоящая из набора связанных кубитов, которыми можно управлять и которыми можно манипулировать для реализации алгоритма, такого, что измерение конечного состояния системы даёт ответ на интересующую проблему с высокой вероятностью. Сами кубиты квантового компьютера должны быть достаточно изолированы от окружающей среды, чтобы их квантовое состояние оставалось когерентным на протяжении всего вычисления.

Таким образом исследования в области квантовой механики уже привели к фундаментальным достижениям в физике и к многообещающим новым технологиям, например, к квантовым датчикам. Такие достижения и приложения, вероятно, будут стимулировать дальнейшую работу, которая поможет углубить человеческое знание квантовых явлений и приведёт к улучшению методов квантовой инженерии.

В следующих разделах сравниваются основы классических и квантовых вычислений, чтобы проиллюстрировать фундаментальные различия между их компонентами и дать общий обзор свойств квантовых вычислений.

2.3. Биты и кубиты

Чтобы дать представление о том, как квантовые свойства обеспечивают новую вычислительную парадигму и как решать возникающие проблемы, в этом разделе представлен краткий обзор основ классических вычислений, включая то, как машины обрабатывают информацию, представленную битами. Затем представляются аналогичные квантовые системы, и их свойства сравниваются и сопоставляются.

[4] Например, захваченных ионов, сверхпроводящих цепей, нейтральных атомов, вакансий азота в алмазе.

2.3.1. Классические вычисления: от аналоговых сигналов к битам и цифровым вентилям

Существующие сегодня мощные классические вычислительные системы основаны на надёжном фундаменте из надёжных физических компонентов. Транзисторы, основные строительные блоки интегральных схем (ИС) в классических компьютерах, взаимодействуют друг с другом с помощью электрических «сигналов». Эти сигналы являются «аналоговыми» по своей природе, что означает, что их значения могут плавно изменяться, как при изменении температуры или скорости[5]. В схеме транзисторы соединены проводами, которые передают электрические сигналы от одного устройства к другому. К сожалению, эти электрические сигналы также взаимодействуют с окружающей средой, и это взаимодействие может нарушить или «нарушить» их значение. Такое возмущение называется «шумом», и его можно разбить на две составляющие. Первый, «фундаментальный шум», возникает в результате флуктуаций энергии, спонтанно возникающих внутри любого объекта, температура которого выше абсолютного нуля. Второй, «систематический шум», возникает из-за взаимодействий сигналов, которые теоретически могли быть смоделированы и скорректированы, но либо не смоделированы вообще, либо смоделированы неправильно, либо намеренно оставлены без коррекции на аппаратном уровне. Этот систематический шум возникает из многих источников. Например, абстракции используются для уменьшения сложности проектирования, что очень важно при создании сложных систем. Тем не менее, эти абстракции часто вносят систематический шум, поскольку, скрывая детали реализации, разработчики не знают точных деталей реализации, которую они используют. Даже когда сокрытие информации не является проблемой, систематический шум все равно возникает из-за производственных отклонений. В то время как разработчик может учитывать номинальное взаимодействие сигналов, изменения в производственном процессе, который на практике не является абсолютно точным, могут создать систему, немного отличающуюся от спроектированной. Эти остаточные различия также вызывают систематический шум. Для правильной работы схема должна быть устойчива к шуму, который вызывают эти изменения.

Когда схема является аналоговой (то есть, когда небольшие изменения на её входе или параметрах вызывают небольшие изменения

[5] По аналогии, чтобы разогнаться до 60 миль в час в автомобиле с места, скорость автомобиля непрерывно увеличивается от 0 до 60 миль в час и достигает всех скоростей между этими пределами.

на её выходе), эффекты шума обычно аддитивны, накапливаясь по мере прохождения сигнала через каждую последующую цепь. Хотя шум, добавляемый на каждом этапе, может быть достаточно мал, чтобы не нарушать заданный процесс, кумулятивный шум может в итоге стать достаточно большим, чтобы повлиять на точность (или достоверность) результата. Следовательно, электронные аналоговые компьютеры никогда не были очень популярными или очень сложными, и они вышли из употребления после 1950-х и 1960-х годов.

Чтобы обойти проблему шума в аналоговых схемах, в большинстве ИС используются транзисторы для создания схем, которые работают с цифровыми двоичными сигналами (называемыми «битами»), а не с аналоговыми сигналами. Эти схемы, называемые «цифровыми вентилями» или просто «вентильными элементами», рассматривают электрический сигнал как двоичное значение, как 0 или 1, а не как действительное число, плавно изменяющееся от 0 до 1. Некоторые вентили, называемые «регистры» или «память» хранят значение бита, в то время как другие обрабатывают ряд входных битовых значений для создания нового выходного значения. Ограничивая набор значений, которые может нести сигнал, вентили могут подавлять шум, добавленный к сигналу, обеспечивая так называемую «помехоустойчивость». Это достигается за счёт обработки всех сигналов, которые имеют электрические значения, близкие к номинальному уровню 0, как нуля, а сигналов около уровня 1 - как единицы, и обеспечивает выходное значение, которое не зависит от точного входного напряжения.

Построение интегральных схем (ИС) полностью из цифровых вентилей значительно упрощает процесс проектирования цифровых систем за счёт создания надёжной схемной структуры, нечувствительной к большинству вариантов изготовления или дизайна. Таким образом, разработчики могут игнорировать все проблемы схемы и думать о вентилях просто как о функциях (известных как логические функции), которые принимают двоичные значения и выводят двоичные значения. Типы функций, которые работают таким образом, полностью описываются общепринятыми правилами булевой алгебры. Эти правила описывают, как любую сложную булеву функцию можно разложить на небольшой ряд более простых операций, таких как перечисленные в таблице 2.1. Этот перевод позволяет сегодняшним разработчикам оборудования описывать свои разработки на относительно высоком уровне абстракции и использовать инструмент автоматизированного проектирования для сопоставления их с требуемыми логическими вентилями — процесс, называемый

«логическим синтезом». Поскольку количество основных строительных блоков ограничено, все производители ИС предоставляют набор предварительно разработанных и протестированных логических элементов, свою «стандартную библиотеку ячеек», которые могут быть включены в конструкцию микросхемы и встроены в кремний с использованием их технологии производства.

Использование как цифровой логики, так и стандартных библиотек для этих логических вентилей также делает конструкции надёжными, то есть они имеют пренебрежимо малую частоту ошибок. Производители ИС предоставляют инструменты проверки, которые анализируют проект, чтобы убедиться, что его систематический шум меньше, чем запас по шуму их вентилей, гарантируя, что логическая абстракция может быть реализована базовыми компонентами.

Таблица 2.1 Базовые булевы операции.

Логическая операция	Входной сигнал		Выходной сигнал	Обозначение операции
	X	Y		
И (AND)	0	0	0	$x \wedge y$
	0	1	0	
	1	0	0	
	1	1	1	
ИЛИ (OR)	0	0	0	$x \vee y$
	0	1	1	
	1	0	1	
	1	1	1	
Исключающее ИЛИ (XOR)	0	0	0	$x \oplus y$
	0	1	1	
	1	0	1	
	1	1	0	
НЕ (NOT)	0		1	$\sim x$ или $\bar{x}$
	1		0	

Даже с большим запасом по шуму в цифровых вентилях шум иногда может быть достаточно большим, чтобы нарушить логические значения, хранящиеся в памяти. Чтобы получить высокую плотность и высокую производительность, эти структуры обычно имеют более крупные вариации устройства и меньший запас по шуму, поэтому иногда шум бывает достаточно большим, чтобы исказить цифровой выход. Чтобы исправить это, добавляется уровень защиты от ошибок.

Данные «кодируются» с использованием кода исправления ошибок (ECC), добавляя некоторые биты, которые добавляют избыточность к значениям, хранящимся в памяти. Этот код проверяется при каждом чтении, что позволяет обнаруживать ошибки памяти. Были разработаны эффективные ECC, которые с небольшими служебными данными (добавление 8 битов к 64-битному значению, что составляет менее 15 процентов служебных данных) могут обнаруживать и исправлять любые однобитовые ошибки в операциях с памятью и обнаруживать двухбитовые ошибки. Эффективные схемы исправления ошибок имеют решающее значение для успеха и надёжности современных классических вычислительных систем. Этот тип алгоритмической коррекции ошибок ещё более важен в квантовых вычислениях, поскольку квантовые вентили имеют небольшую внутреннюю помехоустойчивость, как будет показано в следующем разделе.

Поток цифрового проектирования также помогает с другими аспектами дизайна, такими как тестирование и удаление ошибок из проекта, процесс, обычно называемый «отладкой». В микросхемах есть два типа ошибок, с которыми необходимо иметь дело: ошибки проектирования и производственные дефекты. Учитывая сложность современных систем, в проектировании неизбежно возникают ошибки (баги), поэтому методы поиска этих ошибок и их исправления являются ключевым аспектом любой стратегии проектирования. Когда схема встроена в небольшой кусочек кремния, трудно или невозможно посмотреть на внутренние сигналы, чтобы попытаться отследить ошибку. Чтобы смягчить это, инструменты синтеза, которые отображают высокоуровневое описание проекта в вентили, добавляют в проект дополнительное оборудование, чтобы обеспечить внутренние контрольные точки, которые позволяют отладку этого типа проекта. Эти внутренние тестовые точки также позволяют инструментам автоматически генерировать тесты, которые могут подтвердить, что изготовленный чип выполняет точно такую же логическую функцию, как указано в проекте, что значительно упрощает производственные тесты.

Как будет показано в следующих разделах, хотя квантовые компьютеры имеют битоподобные структуры (называемые «кубитами») и вентили, они ведут себя совершенно иначе, чем классические биты и цифровые вентили. Кубиты обладают как цифровым, так и аналоговым характером, что обеспечивает их потенциальную вычислительную мощность. Их аналоговая природа подразумевает, что, в отличие от классических вентилей, квантовые

вентили не имеют запаса по шуму (входные ошибки передаются непосредственно на выход вентиля), но их цифровая природа позволяет устранить этот критический недостаток. Таким образом, подход к цифровому проектированию и абстракции, разработанные для классических вычислений, нельзя использовать непосредственно для квантовых вычислений. Квантовые вычисления могут заимствовать идеи из обычных вычислений; однако в конечном итоге ему потребуется собственный метод для смягчения последствий изменений обработки и шума, и ему придётся разработать собственный подход к отладке проектных ошибок и производственных дефектов.

2.3.2 Квантовый бит или «Кубит»

При создании обычных ИС разработчики прилагают большие усилия, чтобы свести к минимуму влияние квантовых явлений, которые обычно проявляются в виде шума или других ошибок, влияющих на работу транзистора, особенно по мере того, как устройства становятся все меньше и меньше. Квантовые вычисления во всех их формах используют совершенно другой подход, охватывая, а не пытаясь минимизировать квантовые явления, используя квантовые, а не классические биты.

Квантовый бит, или кубит, имеет два квантовых состояния, аналогичных классическим бинарным состояниям. Хотя кубит может находиться в любом состоянии, он также может существовать в «суперпозиции» двух состояний (как описано ранее на примере квантовой монеты). Эти состояния часто представляются в так называемой нотации Дирака, где метка состояния пишется между | и ⟩. Таким образом, двухкомпонентные или «основные» состояния кубита обычно записываются как $|0\rangle$ и $|1\rangle$. Любая данная волновая функция кубита может быть записана как линейная комбинация двух состояний, каждое из которых имеет свой собственный комплексный коэффициент a_i: $|\psi\rangle = a_0|0\rangle + a_1|1\rangle$.

Поскольку вероятность прочтения состояния пропорциональна квадрату величины его коэффициента, $|a_0|^2$ соответствует вероятности обнаружения состояния $|0\rangle$ и $|a_1|^2$ к вероятности обнаружения $|1\rangle$. Сумма вероятностей каждого возможного выходного состояния должна равняться ста процентам, математически выражаясь в этом случае как $|a_0|^2 + |a_1|^2 = 1$.

В то время как классический бит полностью определяется как 1 или 0, кубит определяется континуумом значений a_0 и a_1, которые на самом деле являются аналоговыми, то есть относительный вклад каждого возможного состояния может быть любым значением между 0

и 1, если общая вероятность равна единице. Конечно, это богатство возможностей существует до того, как состояние кубита будет измерено или «считано». Результат измерения выглядит точно так же, как классический бит, 0 или 1, с соответствующей вероятностью получения каждого значения, пропорционального квадрату абсолютного значения коэффициента соответствующего состояния, $|a_0|^2$ или $|a_1|^2$.

Кроме того, при измерении коэффициент кубита (или амплитуда) становится единицей в считываемом состоянии и нулём в другом; вся информация об амплитудах уничтожается при измерении. Однако если бы кто-то инициализировал кубит в определенном состоянии произвольное количество раз и каждый раз измерял его, можно было бы создать гистограмму количества раз, когда измерение даёт каждый результат, что позволило бы статистически аппроксимировать относительные вероятности, связанные с каждым состоянием, и, таким образом, вывести абсолютное значение коэффициента (эквивалентно квадратному корню из вычисленной вероятности). Результаты измерений для одного кубита перечислены в таблице 2.2 и более подробно описаны во вставке 2.2.

Таблица 2.2. Результаты измерения и вероятности для одного кубита с учётом его начального состояния для нескольких примеров

Состояние перед измерением (волновая функция) кубита	Результат измерения	Вероятность исхода, %	Состояние кубита после измерения
$\|\psi\rangle = \|0\rangle$	0	100	$\|\psi\rangle = \|0\rangle$
$\|\psi\rangle = \|1\rangle$	1	100	$\|\psi\rangle = \|1\rangle$
$\|\psi\rangle = \frac{1}{\sqrt{2}}\|0\rangle + \frac{1}{\sqrt{2}}\|1\rangle$	0	50	$\|\psi\rangle = \|0\rangle$
	1	50	$\|\psi\rangle = \|1\rangle$
$\|\psi\rangle = \frac{1}{2}\|0\rangle + \frac{\sqrt{3}}{2}\|1\rangle$	0	25	$\|\psi\rangle = \|0\rangle$
	1	75	$\|\psi\rangle = \|1\rangle$
$\|\psi\rangle = \frac{1}{2}\|0\rangle + \frac{\sqrt{3}e^{-\frac{i\pi}{4}}}{2}\|1\rangle$	0	25	$\|\psi\rangle = \|0\rangle$
	1	75	$\|\psi\rangle = \|1\rangle$

2.3.3 Мультикубитные системы

Рассмотрим систему из двух битов. Классически два бита могут существовать в четырёх возможных конфигурациях: 00, 01, 10 и 11. Чтобы вычислить вывод двухбитовой булевой функции для каждого из этих возможных входов с использованием классической схемы, нужно

было бы сгенерировать каждый соответствующую пару сигналов и либо посылать каждый по очереди в вентиль, соответствующий функции, либо направлять каждый сигнал в собственную копию четырёх идентичных вентилей, соответствующих интересующей функции.

Вставка 2.2

Измерение одного кубита.

Когда кубит находится в состоянии $|\psi\rangle = |0\rangle$, результатом измерения будет 0 с вероятностью 100 %, что мало чем отличается от того, что происходит с классическим битом. Точно так же измерение кубита в состоянии $|\psi\rangle = |1\rangle$ даст результат 1 с вероятностью 100 %. Для кубита в состоянии суперпозиции результат менее прост — результат измерения, даже известного состояния, нельзя предсказать с уверенностью.

Например, состояние суперпозиции $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ имеет равную вероятность (50 %) получения любого результата (вероятность равна квадрату амплитуды или 0,5). Повторная подготовка и измерение этого состояния дадут случайную последовательность результатов, приближающуюся к равной частоте каждого из них по мере увеличения числа испытаний, как при классическом подбрасывании монеты. Соответственно, это состояние можно рассматривать как «квантовую монету». После измерения определенного значения кубит остаётся в состоянии, соответствующем этому значению. Например, если результат измерения равен 1, кубит после измерения находится в состоянии $|\psi\rangle = |1\rangle$, независимо от того, в каком состоянии он находился до измерения.

С другой стороны, если бы кто-то использовал квантовый компьютер, все четыре возможности могли бы быть закодированы в состояние двух кубитов посредством суперпозиции четырёх квантовых базисных состояний $|00\rangle$, $|01\rangle$, $|10\rangle$ и $|11\rangle$. Вычисление может быть выполнено с использованием одного квантового вентиля, который будет работать со всеми состояниями параллельно и в одно и то же время. Легко понять, почему мультикубитная система может быть мощной. Однако, как упоминалось ранее — и как будет показано в следующих двух разделах — извлечь любое соответствующее значение из квантовой системы сложно.

Ещё один способ оценить потенциальную мощь набора кубитов — посмотреть на количество информации, необходимой для полного

описания состояния системы кубитов. Обычная цифровая двухбитная система требует два бита информации для представления своего состояния. Напротив, двухкубитная система существует в суперпозиции четырёх состояний (|00⟩, |01⟩, |10⟩ и |11⟩), требующих четырёх комплексных констант (a_{00}, a_{01}, a_{10} и a_{11}) для полностью описывают квантовое состояние, а не два бита. Различные значения четырёх коэффициентов кодируют результаты всех возможных типов предыдущих операций, выполненных над этими двумя кубитами, а также вероятность оказаться в каждом состоянии, если система измеряется.

Для системы с тремя кубитами требуется восемь коэффициентов для определения вкладов от базисных состояний (|000⟩, |100⟩, |010⟩, |001⟩, |110⟩, |101⟩, |011⟩ и |111⟩) к трехкубитной волновой функции. Следуя этой логике, система с n кубитами требует указания 2^n коэффициентов a_i, а не n битов, как в классическом компьютере. Это экспоненциальное масштабирование квантового состояния — это то, что позволяет 32 кубитам представлять все 2^{32} возможных выхода 32-битной функции и иллюстрирует богатство квантового компьютера и трудности классического моделирования этих машин по мере их увеличения в размерах.

Эта точка зрения также указывает на то, что, хотя в названии кубитов есть слово «бит», они не являются ни цифровыми, ни чисто бинарными. Состояние системы кубитов закодировано в значениях коэффициента a_i, наборе аналоговых сигналов (фактически комплексных чисел), которые не устойчивы к шуму. В цифровой системе только с двумя допустимыми уровнями, скажем, 0 и 1, легко удалить шум в системе, так как все значения будут близки к 0 или 1 с небольшими отклонениями. Например, значение входного сигнала 0,9 почти наверняка равно 1, поэтому гейт может «удалить» шум, обработав это входное значение как 1 перед вычислением своего выхода. В аналоговом сигнале, для которого любое значение от 0 до 1 может быть значимым и разрешённым, невозможно узнать, является ли сигнал правильным или он искажён шумом. Например, 0,9 может означать 1 с некоторой ошибкой или 0,9 без ошибки. В этой ситуации наилучшее предположение (которое приводит к наименьшей чистой ошибке) всегда состоит в том, чтобы предположить, что ошибка равна нулю, и интерпретировать зашумлённое значение как фактический сигнал. Это означает, что шум в физической реализации системы кубитов искажает фактические значения ai и влияет на «точность» результирующих квантовых вычислений. Квантовые вентили не имеют запаса шума, поскольку их входы (начальные значения a_i) и их выходы

(конечные значения a_i) являются аналоговыми значениями. Поскольку ни один аналоговый вентиль полностью не соответствует своим спецификациям (абсолютно точным быть невозможно), каждая операция вентиля также будет добавлять шум в общую систему в количестве, которое зависит от точности операций вентиля.

Обычно отсутствие помехозащищённости означает, что «глубина вычислений» — количество последовательных операций, которые могут быть выполнены точно — квантового компьютера будет ограничена, как и любого аналогового компьютера. Однако квантовые вентили не являются полностью аналоговыми: измерение кубита всегда возвращает двоичное значение. Эта цифровая связь между входами и выходами означает, что логическая коррекция ошибок может применяться к квантовым машинам, которые используют квантовые вентили в качестве своих основных операций. Эти алгоритмы называются квантовой коррекцией ошибок (QEC), и их можно запускать на шумном квантовом компьютере на основе вентиля, чтобы уменьшить количество ошибок и эмулировать бесшумную систему. Как и в случае классических кодов с исправлением ошибок, упомянутых в разделе 2.3.1, QEC должен добавлять избыточность, и в квантовом случае эта избыточность должна быть переплетена с остальным состоянием системы, чтобы восстановиться после ошибки. В отличие от классических кодов, которые имеют небольшие накладные расходы, коды QEC, как правило, имеют очень высокие накладные расходы и могут увеличить количество кубитов, необходимых для выполнения безошибочного вычисления, на много порядков. Алгоритмы QEC более подробно описаны в разделе 3.2.

2.4. Вычисления с кубитами

Аналоговая природа состояний кубитов и квантовых вентилей кардинально меняет необходимые подходы к проектированию и архитектуру схем для квантовых компьютеров. Основные части, необходимые для создания и запуска квантового компьютера, на примере частей современной системы сверхпроводящих кубитов: чип кубита помещён в большую структуру, которая позволяет охлаждать его до 20 мК, поддерживая при этом необходимую проводку управления. Затем эту большую структуру помещают в криостат, который охлаждает кубитовый чип. Затем управляющие провода подключаются к набору тестового и измерительного оборудования (оборудование из лаборатории Уилла Оливера), которое приводит в движение кубиты. Это тестовое оборудование управляется уровнем

процессора управления, который может состоять из нескольких процессоров в случае большого квантового компьютера. Процессор управления подключён к более крупному компьютерному серверу (показан как часть центра обработки данных Google), который обеспечивает доступ пользователя к квантовому компьютеру и необходимые службы поддержки программного обеспечения.

В традиционной компьютерной конструкции устойчивость цифрового сигнала позволяет легко оптимизировать конструкцию для повышения производительности, т. е. максимизировать количество операций, которые могут выполняться параллельно (в одно и то же время). Одна ИС может содержать сотни миллионов вентилей, расположенных в разных местах. Каждый провод соединяет выход вентиля (1 или 0) с вентилями, которые используют этот электрический сигнал в качестве входа. В то время как производственные вариации делают каждый затвор немного другим, а электрические сигналы на проводах могут взаимодействовать друг с другом и вносить систематический шум друг в друга, помехозащищённость используемых цифровых затворов достаточна, чтобы свести на нет влияние всех этих источников шума. Таким образом, даже при параллельной работе миллионов логических элементов результирующая система ведёт себя так, как предполагалось, производя тот же результат, что и булева модель проекта.

Поскольку квантовые сигналы являются аналоговыми и чувствительными к шуму, при проектировании квантовых систем используется совершенно другой подход. Здесь ключевая цель разработки состоит в том, чтобы свести к минимуму введение шума в кубит, что исключает отправку состояния кубита через зашумлённые каналы, такие как длинный провод[6]. Таким образом, эти системы обычно сосредотачиваются на создании кубитов или контейнеров для кубитов, а также связанных вспомогательных схем, необходимых для выполнения различных операций с состояниями кубитов, включая запутывание кубитов с другими кубитами, находящимися поблизости. В квантовых системах операции (вентили) имеют тенденцию поступать к кубитам, в то время как в классических машинах биты поступают к вентилям.

Помимо этой разницы в архитектуре, поскольку квантовые компьютеры работают с другими типами значений, чем классические компьютеры, они не могут использовать те же абстракции логических

[6] Кубиты также должны подчиняться правилу запрета клонирования, что также исключает отправку состояния кубита к двум разным вентилям одновременно (это будет обсуждаться далее в разделе 2.5).

вентилей, которые были разработаны для манипулирования классическими битами. Требуются новые абстракции для вычислений с использованием кубитов, обеспечивающие способ реализации определенных изменений в квантовых состояниях. Как и во всех квантовых системах, состояние кубита можно изменить, изменив его энергетическое окружение, что является физическим проявлением его гамильтониана.

Существует два основных подхода к квантовым вычислениям. Первый генерирует желаемый результат, инициализируя состояние квантовой системы, а затем используя прямое управление гамильтонианом для развития квантового состояния таким образом, который имеет высокую вероятность ответа на интересующий вопрос. В этих системах гамильтониан часто плавно изменяется, поэтому квантовые операции являются действительно аналоговыми по своей природе и не могут быть полностью исправлены[7] и будет называться «аналоговые квантовые вычисления». Этот подход включает адиабатические квантовые вычисления (AQC), квантовый отжиг (QA) и прямое квантовое моделирование. Второй подход, называемый «квантовыми вычислениями на основе вентилей», похож на современные классические подходы в том, что проблема разбивается на последовательность нескольких очень простых «примитивных операций» или вентилей, которые имеют чётко определенные «цифровые вычисления». результаты измерения для определенных входных состояний. Это цифровое свойство означает, что в схемах такого типа в принципе может использоваться коррекция ошибок на системном уровне для достижения отказоустойчивости. Однако, как отмечалось выше, набор примитивных квантовых операций отличается от классических примитивов.

2.4.1 Квантовое моделирование, квантовый отжиг и адиабатические квантовые вычисления

Аналоговые квантовые вычисления включают систему кубитов в начальном квантовом состоянии и изменяют гамильтониан таким образом, что проблема кодируется в конечном гамильтониане, а конечное состояние соответствует ответу. Если система остаётся в основном состоянии изменяющегося гамильтониана, такой подход называется адиабатическими квантовыми вычислениями (AKB). Когда

[7] В то время как методы уменьшения влияния шума были разработаны и развёрнуты для аналоговых КК, теория аналогового КК QEC был предложен только для AQC; ожидается, что это не будет легко достигнуто, а полное исправление ошибок потребует безграничных ресурсов. Таким образом, для аналоговых КК не существует практического метода достижения безошибочной машины. Эти вопросы рассматриваются далее. в разделе 3.2.

это требование ослабляется — например, если квантовому компьютеру также разрешено взаимодействовать с тепловым окружением или если ему разрешено развиваться слишком быстро — этот протокол называется «квантовым отжигом». При достаточно сложном выборе гамильтонианов AQC формально эквивалентна по вычислительной мощности модели квантовых вычислений на основе вентилей. Для существующих устройств квантового отжига выбор гамильтонианов ограничен, и эти устройства формально не эквивалентны универсальным квантовым компьютерам. Прямое квантовое моделирование — это когда гамильтониан между кубитами задается для моделирования интересующей квантовой системы, поэтому его эволюция моделирует эту систему.

Как упоминалось выше, в этих подходах к аналоговым квантовым вычислениям не только значения кубитов являются аналоговыми, но и квантовые операции выполняются путём плавного изменения гамильтониана. Этот недискретный набор квантовых операторов сбивает с толку традиционные подходы к исправлению ошибок на системном уровне. Хотя модель QEC была предложена, в частности, для AQC [13-17], её было бы сложно реализовать на практике, поскольку для устранения всех ошибок потребуются неограниченные ресурсы. В результате пытаются минимизировать влияние шума в таких системах с помощью квантовой ошибки и подавления шума [18, 19].

Декогеренция играет совсем другую роль в цифровых квантовых компьютерах и аналоговых квантовых компьютерах. В цифровых квантовых компьютерах декогеренция редко бывает желательной[8]. В случае аналогового квантового компьютера и, в частности, квантового отжигателя декогеренция играет более тонкую роль. С одной стороны, релаксация (диссипация) энергии желательна, потому что она позволяет системе найти основное состояние, необходимое для того, чтобы метод давал правильные результаты. Для более масштабных задач отжиг почти наверняка покинет своё основное состояние во время протокола отжига либо в результате слишком быстрого изменения гамильтониана, либо из-за теплового возбуждения из окружающей среды. В этих случаях рассеяние в окружающую среду явно выгодно, так как оно имеет тенденцию возвращать отжиг в исходное состояние. Однако если диссипация слишком велика, система больше не будет вести себя квантово-механически и, таким образом, перестанет быть квантовым компьютером. Кроме того, фазовая когерентность также необходима для «когерентного совместного

[8] За исключением, возможно, времени подготовки состояния и проективного измерения.

туннелирования», квантового процесса, который обеспечивает более эффективную релаксацию в основное состояние за счёт скоординированного переключения кубитов. На практике необходимо достичь баланса, чтобы отжиг был эффективным. Аналоговые квантовые вычисления более подробно обсуждаются в главе 3.

2.4.2 Квантовые вычисления на основе вентилей

В основанном на вентилях подходе к квантовым вычислениям каждая примитивная операция (вентиль) выполняется путём точного изменения гамильтониана одного или нескольких кубитов в течение определенного времени, необходимого для достижения желаемого преобразования. Это делается путём изменения физической среды, например, с помощью лазерного импульса или приложения какого-либо другого электромагнитного поля, в зависимости от способа построения кубитов. Поскольку эти примитивные операции аналогичны логическим вентилям в классических вычислениях, системы, построенные с использованием такого подхода, называются «цифровыми квантовыми компьютерами».

Правила квантовой механики ограничивают набор возможных операций квантовых вентилей несколькими интересными способами. Во-первых, операции должны быть «без потерь», то есть они не должны рассеивать какую-либо энергию, поскольку рассеяние энергии означает, что система связана с окружающей средой для отвода тепла, что привело бы к неприемлемой декогерентности. Поскольку потеря информации рассеивает энергию [20], квантовые вентили должны быть обратимыми, а это означает, что вы можете не только вычислять выходы вентиля из его входов, вы также можете вычислять входы вентиля из его выходов (вычисления вентиля могут выполняться в обратном порядке или наоборот). наоборот). Чтобы быть обратимой, функция всегда должна иметь столько же выходов, сколько и входов.

Во-вторых, хотя операции изменяют коэффициенты или «амплитудное распределение» различных возможных состояний, сумма квадратов их абсолютных значений (сумма их вероятностей) всегда остаётся единицей. Один математический способ визуализировать работу квантовых вентилей состоит в том, чтобы представить состояние «n» кубитов в виде вектора в многомерном пространстве (2^n комплексных измерений), где значение вектора в каждом измерении определяется комплексными коэффициентами a_i. Сохранение вероятности заставляет длину вектора быть постоянной и равной 1, поэтому состояние системы может быть любым местом на единичной гиперсфере (расширение сферы до более высоких

измерений). Все квантовые вентили представляют собой простые повороты вектора состояния в новое положение на гиперсфере. По мере увеличения числа кубитов размерность пространства растёт экспоненциально, но вектор состояния остаётся единичной длины, а операции остаются различными возможными поворотами гиперсферы (все они обратимы). Операции, сохраняющие длину вектора, называются «унитарными». Вставка 2.3 показывает сферу, созданную одним кубитом.

Как и в классической логике, вентили с большим количеством входов создать сложно, но их можно сконструировать или «синтезировать», используя ряд более простых вентилей, каждый из которых принимает меньшее число входов. На практике квантовые вентили обычно предназначены для работы на входах одного, двух или трех кубитов. Также, как и в классической логике, небольшое количество базовых квантовых вентилей можно использовать для создания всех возможных функций квантовых вентилей. Общий набор основных квантовых вентилей и их представления показан в таблице 2.3. Особое значение имеют вентили Адамара для суперпозиции, которые превращают кубит в $|0\rangle$ состояние равной суперпозиции $|0\rangle$ и $|1\rangle$, где оба имеют одинаковую относительную фазу $\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)$, и развивают $|1\rangle$ до чётной суперпозиции $|0\rangle$ и $|1\rangle$, но с противоположными фазами $\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)$. Двухкубитный вентиль CNOT выполняет логическую операцию XOR, но он должен передать один из входов на выход, чтобы сделать вычисления обратимыми.

Поскольку квантовые вентили отображают начальный $a_i s$ набора входных кубитов в новый набор $a_i s$, эти вентили часто математически записываются в виде матрицы. В этом представлении a_i для каждого из входных состояний накладываются друг на друга, чтобы сформировать вектор, а результат умножения вектора матрицы приводит к вектору, который представляет собой ai выходного состояния. Логическая операция с n входами, или «вентиль», может быть математически описана как унитарная матрица $2^n \times 2^n$, которая работает с n входными кубитами (кодирует начальные 2^n $a_i s$) и производит n выходных кубитов (кодирует 2^n новых $a_i s$).

Известно, что вентили T, Адамара и CNOT, где T — поворот на π/4 (90 градусов), образуют универсальное множество вентилей [21] (т. е. любая унитарная функция может быть аппроксимирована с произвольной точностью с помощью компьютер, построенный только из вентилей из этого множества) [22].

Вставка 2.3

Визуализация состояния кубита.

Состояние одного кубита представлено символом $|\psi\rangle = a_0|0\rangle + a_1|1\rangle$. Условие вероятности $|a_0|^2 + |a_1|^2 = 1$ ограничивает значения, которые могут принимать a_0 и a_1. Мы можем учесть это ограничение, установив величину a_0 на $\cos\frac{\theta}{2}$ и величину a_1 на $\sin\frac{\theta}{2}$: $\left(\sin\frac{\theta}{2}\right)^2 + \left(\cos\frac{\theta}{2}\right)^2 = 1$. Учёт фазовой составляющей комплексного числа означает, что $a_0 = e^{i\alpha}\cos\frac{\theta}{2}$ и $a_1 = e^{i(\alpha+\varphi)}\sin\frac{\theta}{2}$. В результате состояние кубита можно представить с помощью трёх независимых действительных чисел α, θ и φ: $|\psi\rangle = e^{i\alpha}\left(\cos\frac{\theta}{2}|0\rangle\right) + e^{i\varphi}\left(\sin\frac{\theta}{2}|1\rangle\right)$. Оказывается, глобальная фаза α не имеет никакого физического смысла, а однокубитное состояние можно полностью описать двумя действительными числами $0 \leq \theta < \pi$ и $0 \leq \varphi < 2\pi$. Описание произвольного состояния одного кубита может быть отображено на точку на поверхности единичной сферы (называемой «сферой Блоха»), где северный и южный полюса соответствуют состояниям $|0\rangle$ и $|1\rangle$ соответственно. θ указывает широту, а φ — долготу положительного значения квантового состояния на сфере Блоха, как показано на рис. 2.1.

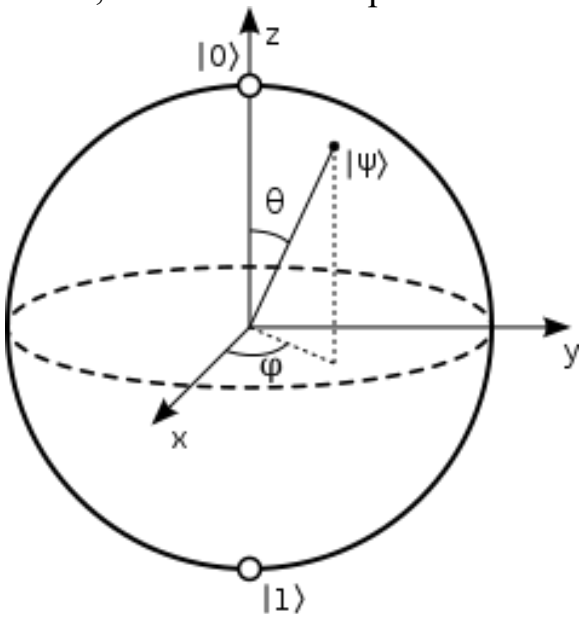
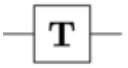
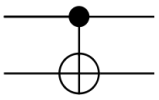
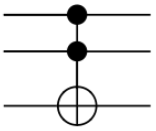
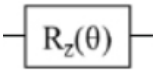


Рис. 2.1 Изображение сферы Блоха, которая представляет набор всех возможных состояний для одного кубита. Однокубитовые вентили поворачивают состояние кубита в другую точку на этой сфере. (Smite-Meister, https://commons.wikimedia.org/w/index.php?curid=5829358).

Таблица 2.3 Обычно используемые кубитные квантовые вентили.

Название вентиля	Число кубит	Обозначение вентиля	Унитарная матрица	Описание
Адамара	1		$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$	Преобразует базовое состояние в равномерную суперпозицию двух базовых состояний.
T	1		$\begin{bmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{bmatrix}$	Добавляет относительный фазовый сдвиг $\pi/4$ между содействующими базисными состояниями. Иногда его называют воротами числа $\pi/8$, потому что диагональные элементы можно записать как $e^{i\pi/8}$и $e^{-i\pi/8}$.
CNOT	2		$\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$	Контролируемое отрицание; обратимый аналог классического вентиля XOR. Вход, подключённый к сплошной точке, проходит через него, чтобы сделать операцию обратимой.
Тоффоли (CCNOT)	3		$\begin{bmatrix}1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1\\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\end{bmatrix}$	Универсальный контролируемый обратимый вентиль; вентиль с тремя кубитами, который переключает третий бит для состояний, в которых первые два бита равны 1 (т. е. переключает $\|110\rangle$ на $\|111\rangle$ и наоборот).
Паули-Z	1		$\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$	Добавляет относительный фазовый сдвиг π между базисными состояниями. Отображает $\|0\rangle$ в себя и $\|1\rangle$ в $-\|1\rangle$. Иногда называется «переворотом фазы».
Z-вращение	1		$\begin{bmatrix}e^{-i\theta/2} & 0\\ 0 & e^{i\theta/2}\end{bmatrix}$	Добавляет относительный фазовый сдвиг (или поворачивает вектор состояния вокруг оси Z на) θ.
NOT	1		$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$	Аналогично классическому вентилю НЕ; переключает$\|0\rangle$ на $\|1\rangle$ и наоборот.

Для поворота на общий угол θ повороты одного кубита не могут быть точно выражены в этом наборе вентилей; таким образом, необходимо разложить искомую операцию на последовательность операций. Такая «декомпозиция» данной операции на последовательность простых элементов также позволяет составить

общую схему в виде последовательности более простых элементов-примитивов, которые легче реализовать аппаратно.

Стоит отметить, что известные алгоритмы для некоторых приложений, например, в вычислительной химии, в значительной степени полагаются на общие угловые повороты; в частности, для этих случаев очень важно иметь методы, которые могут создавать или синтезировать эти операции, используя небольшое количество примитивных вентильных операций. Более совершенные алгоритмы синтеза генерируют целевые элементы из меньшего числа примитивных элементов.

В отличие от унитарных операций, лежащих в основе реализации квантового алгоритма, операция измерения сильно связывает квантовое состояние с измерительным устройством, которое выдаёт двоичный вывод и не является обратимым. Измерение необходимо для извлечения информации из квантового компьютера; однако измерение коллапсирует волновую функцию системы и возвращает только n битов информации из n-кубитного квантового регистра, то есть возвращает один классический результат. Результаты измерения системы с двумя кубитами показаны в таблице 2.4 и обсуждаются во вставке 2.4.

2.5 Ограничения при проектировании квантового компьютера

Как упоминалось в предыдущих разделах, большая потенциальная мощность квантового компьютера связана с четырьмя основными ограничениями. Первое серьёзное ограничение заключается в том, что количество коэффициентов, необходимых для описания состояния квантового компьютера, экспоненциально возрастает с увеличением количества кубитов только тогда, когда все кубиты запутываются друг с другом. Хотя добавление кубита в систему удваивает количество квантовых состояний, если этот кубит не взаимодействовал с остальной системой, описание квантового состояния может быть факторизовано и представлено как произведение состояния добавленного кубита, умноженное на состояние остальной части системы. Это факторизованное состояние требует всего два дополнительных коэффициента (состояние добавленного кубита) по сравнению с исходной квантовой системой. Чтобы получить мощность квантовых вычислений, кубиты должны быть запутаны, то есть состояние любого кубита должно быть соотнесено с состояниями других кубитов. Чтобы образовалась такая зависимость между двумя кубитами, им необходимо прямо или косвенно взаимодействовать через промежуточную квантовую систему — будь то фотон, фонон или

другой кубит, — которая в какой-то момент взаимодействует с каждым запутываемым кубитом.

Если кубит A запутывается с кубитом B, а через какое-то время кубит B запутается с кубитом C, вполне вероятно, что кубит A теперь также запутан с кубитом C. Чтобы увидеть это, предположим, что все кубиты начинаются в состоянии $|0\rangle$, а кубит A находится в запутанном состоянии. затем управляется вентилем Адамара. Это управляющий вход вентиля CNOT для кубита B, а затем кубит B является управляющим терминалом для кубита C. Измерение A, B или C даст 0 в 50% случаев. Но как только один из кубитов будет измерен, состояние других кубитов будет известно со 100 % вероятностью.

Несмотря на то, что генерация прямого взаимодействия между кубитами, которые физически разделены (то есть несмежны) внутри квантового процессора, как сложные вентили, может быть труднодостижимой[9] его можно разложить на ряд более простых примитивов операции ворот напрямую поддерживаются аппаратным обеспечением. Эта непрямая связь может быть выполнена через цепочку операций с использованием промежуточных кубитов или других квантовых систем для облегчения взаимодействия. Однако, как и в классических вычислениях, эта непрямая связь создаёт дополнительную нагрузку на машину, что является первым серьёзным ограничением конструкции. Эта стоимость связи хорошо известна в классических вычислениях и способствует очень большому числу вентилей в современных машинах. Во многих реализациях квантовых вычислений генерация этого дальнодействующего взаимодействия будет потреблять часть кубитов в машине, а количество полезных кубитов будет меньше, чем количество физических кубитов в машине. Эта необходимость разрушить дальнодействующие взаимодействия также означает, что некоторые операции с двумя кубитами, взятые из набора универсальных вентилей, потребуют для выполнения нескольких примитивных вентильных операций. Эти накладные расходы наиболее значительны на ранних стадиях развития технологии, когда операции с кубитами и вентилями ограничены.

Второе ограничение связано с тем, что невозможно сделать копию квантовой системы из-за так называемого принципа запрета клонирования [23, 24]. Хотя состояние набора кубитов можно переместить в другой набор кубитов, это приведёт к удалению этой информации из исходных кубитов; произвольная квантовая

[9] Чтобы предотвратить взаимодействие энергии кубита с окружающей средой, она удерживается в локализованные, хорошо изолированные пятна. Распределение энергии по широкой области для взаимодействия двух кубитов также подвергает эти кубиты воздействию окружающей среды, что в современных технологиях значительно сокращает время когерентности.

информация может быть перемещена, но не скопирована. Поскольку создание и хранение копий промежуточных состояний или частичных результатов в памяти является неотъемлемой частью классических вычислений и того, как мы думаем о программировании, квантовые компьютеры требуют другого подхода к разработке алгоритмов. Кроме того, вычислительные задачи часто требуют возможности доступа к хранимым данным, а многим квантовым алгоритмам требуются средства для доступа к сохранённым классическим битам таким образом, чтобы было видно, какие биты запрашиваются и загружаются в квантовую память.

Таблица 2.4 Результаты измерений и вероятности некоторых возможных состояний двухкубитной системы при заданном её начальном состоянии

Состояние перед измерением (волновая функция) системы кубитов	Результат измерения	Вероятность исхода, %	Состояние системы кубитов после измерения
$\|\psi\rangle = \|00\rangle$	00	100	$\|\psi\rangle = \|00\rangle$
$\|\psi\rangle = \|01\rangle$	01	100	$\|\psi\rangle = \|01\rangle$
$\|\psi\rangle = \frac{1}{\sqrt{2}}\|00\rangle + \frac{1}{\sqrt{2}}\|11\rangle$	00	50	$\|\psi\rangle = \|00\rangle$
	11	50	$\|\psi\rangle = \|11\rangle$
$\|\psi\rangle = \frac{1}{2}\|01\rangle + \frac{\sqrt{3}}{2}\|10\rangle$	01	25	$\|\psi\rangle = \|01\rangle$
	10	75	$\|\psi\rangle = \|10\rangle$
$\|\psi\rangle = \frac{1}{2}(\|00\rangle + \|10\rangle + \|01\rangle + \|11\rangle)$	00	25	$\|\psi\rangle = \|00\rangle$
	01	25	$\|\psi\rangle = \|01\rangle$
	10	25	$\|\psi\rangle = \|10\rangle$
	11	25	$\|\psi\rangle = \|11\rangle$

Третье основное ограничение связано с отсутствием помехозащищённости квантовых операций. Поскольку небольшие дефекты во входных сигналах или операциях вентилей не устраняются основными операциями вентилей, как в классических логических вентилях, эти небольшие ошибки со временем будут накапливаться, нарушая состояние системы. Эти ошибки влияют на точность вычислений и, когда они достаточно велики, могут привести к ошибкам измерения или даже к потере квантовой когерентности (и, следовательно, к потере любого квантового преимущества). Этот шум возникает из-за несовершенной изоляции от окружающей среды, неисправленных изменений в физической подготовке или производстве самих кубитов (или устройств, которые

Вставка 2.4

Измерение и запутанность в двухкубитной системе.

Волновые функции для многокубитных систем строятся как линейные комбинации всех возможных классических состояний, которые на языке линейной алгебры служат так называемыми базисными. Для двухбитовой системы возможны четыре классических состояния, поэтому волновая функция такой системы имеет общий вид

$$|\psi_{ij}\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle,$$

где квадрат величины коэффициента состояния соответствует вероятности его измерения.

Рассмотрим состояние, в котором только a_{00} отличен от нуля, $|\psi\rangle = |00\rangle$. Измерение первой частицы даёт 0 со 100 % уверенностью, то же самое и со второй частицей. В этом случае каждый кубит может быть описан независимо своей волновой функцией: $|\psi_i\rangle = |0\rangle_i$. и $|\psi_j\rangle = |0\rangle_j$. Вся система может быть записана как произведение отдельных кубитов $|\psi\rangle = |\psi_i\rangle \cdot |\psi_j\rangle = |0\rangle_i|0\rangle_j$, что равнозначно написанию $|\psi_{ij}\rangle = |00\rangle$.

Теперь рассмотрим состояние суперпозиции $|\psi_{ij}\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. Что произойдёт, если измерить первый кубит? Если результат равен 1, волновая функция коллапсирует в комбинацию только тех состояний с этим значением для первого кубита, или $|\psi_{ij}\rangle = |11\rangle$. Следовательно, второй кубит со 100 % вероятностью будет найден в том же состоянии. С другой стороны, измерение первого кубита как 0 гарантирует, что второй кубит будет таким же, в соответствии с той же логикой. Дальнейшая проверка покажет, что независимо от того, какой кубит измеряется первым, измерение второго всегда будет давать то же самое значение, которое наблюдалось для первого. Частицы неразрывно связаны между собой в том смысле, что состояние одной зависит от другой, и измерение одной внутренне определяет состояние другой — независимо от того, измеряется вторая или нет. Это состояние называется «запутанностью» и по своей сути является квантово-механическим. С математической точки зрения, запутанность возникает, когда нет возможности записать многокубитную волновую функцию как произведение однокубитных волновых функций. Это конкретное состояние является примером «состояния Белла», особой категории запутанного состояния. Запутанные состояния по своей сути являются квантово-механическими и являются ключом к мощности квантовых вычислений.

их содержат или поддерживают), а также несовершенства сигналов, используемых для выполнения требуемых операций с кубитами. В совокупности эти несовершенства обычно ухудшают качество работы кубита. Эти эффекты остаются значительными даже при использовании стратегий минимизации и предотвращения шума, который приводит к ошибкам.

Вставка 2.5

Определение и количественная оценка достоверности / частоты ошибок кубитов.

Квантовые компьютеры требуют высокой точности кубитов и вентилей для успешной работы. В данном пособии частота ошибок вентилей будет использоваться как мера точности кубитов компьютера. Частота ошибок вентиля — это показатель, который характеризует надёжность работы шлюза с учётом широкого набора источников ошибок. По сути, это мера того, насколько близко фактические вентили соответствуют — в среднем — теоретически идеальным версиям этих вентилей. Частота ошибок логического элемента в 1 процент указывает на то, что данный тип вентиля даст правильный результат при измерении в среднем 99 из 100 попыток.

Эти ошибки возникают из-за ряда различных механизмов, которые добавляют «шум» к кубиту. Одним из источников шума является потеря когерентности кубита, а поскольку состояние кубита состоит как из величины, так и из фазы, «шум» может влиять на оба аспекта состояния кубита. Невозможно полностью изолировать какую-либо систему от окружающей среды, поэтому со временем энергия кубита будет стремиться уравновеситься с окружающей средой — возбуждённые состояния будут терять энергию и станут основным состоянием, если окружающая среда холодная. Это означает, что вероятность (квадрат амплитуды) возбуждённого состояния уменьшается со временем. Физические процессы также со временем добавляют к квантовому состоянию случайные фазовые сдвиги, что снижает фазовую когерентность состояний кубита. Поскольку квантовые операции требуют фазового выравнивания для правильной работы, эта фазовая декогерентность также со временем приводит к ошибкам кубитов. Для простого шума релаксация энергии и фазовая декогерентизация происходят посредством экспоненциального затухания с постоянными времени, обозначаемыми как T_1 и T_2 соответственно. Поскольку энергетическая релаксация также является процессом фазового разрыва, время когерентности T_2 охватывает процессы как релаксации энергии, так и дефазировки, и T_2 должно быть намного

больше, чем время, необходимое для реализации необходимого количества квантовых вентилей для создания полезного квантового компьютера.

В дополнение к фундаментальным ошибкам когерентности кубитов, учитывая аналоговые управляющие сигналы, используемые для выполнения операций вентиля кубита, каждая операция вентиля не идеальна, и выполнение этой операции может повлиять на другие состояния кубита в системе (эти помехи называются «перекрёстными помехами»). Это означает, что в последовательности операций вентиля есть вероятность, что сгенерированный вывод будет неправильным, и что эти операции увеличат частоту ошибок для будущих операций. Вероятность генерации правильного результата (правильное выполнение всех вентильных операций для создания результата) снова экспоненциально уменьшается с их количеством. Таким образом, из измеренной частоты системных ошибок можно извлечь среднюю частоту ошибок на вентиль. Вентили кубитов с двумя входами более сложны, чем операции с одним кубитом, поскольку в этой операции состояния двух кубитов должны взаимодействовать, что приводит к более высокому уровню ошибок. Для более полной картины часто приводятся частоты ошибок как для одно-, так и для двухкубитных вентилей. Когда частота ошибок используется в качестве метрики точности, эта частота учитывает декогерентность, которая возникает во время операции, и любые другие ошибки, вызванные работой вентиля.

Учитывая, что пользователь квантового компьютера заинтересован в оценке достоверности результатов, извлечение эффективных коэффициентов ошибок логического элемента с использованием процесса рандомизированного бенчмаркинга (RBM) имеет большое значение. В общем, RBM реализует случайный набор вентилей и сравнивает результирующее состояние с предсказанным состоянием для этой последовательности. Ошибка в конечном состоянии увеличивается по мере увеличения длины последовательности, при этом скорость роста ошибки на элемент обеспечивает меру частоты ошибок для выбранной группы элементов. Interleaved RBM стремится охарактеризовать частоту ошибок конкретного элемента путём периодического ввода этого элемента в случайный набор и сравнения полученной ошибки с тем же набором без интересующего нас элемента. RBM и его вариации обеспечивают относительно эффективное средство для оценки средней частоты ошибок квантовых операций в конкретном устройстве. Эти оценки не искажены наличием каких-либо ошибок инициализации и измерений. Однако следует отметить, что RBM предоставляет только частоту ошибок устройства, не раскрывая конкретных каналов ошибок.

Качество вентиля измеряется либо частотой ошибок, определяемой вероятностью того, что вентиль даёт неправильный результат, либо точностью, вероятностью того, что вентиль приводит к правильному результату (Вставка 2.5). Для современных систем в 2018 году наилучшие коэффициенты ошибок находятся в диапазоне от 10^{-3} до 10^{-6} для однокубитных вентилей [25-28] и в диапазоне от 10^{-2} до 10^{-3} для двухкубитных вентилей (запутывающих) [29-32] в сверхпроводящих кубитах и кубитах с захваченными ионами. В современных машинах это качество ухудшается по мере увеличения количества кубитов в машине.

Последним ограничением является невозможность фактически наблюдать полное состояние машины после того, как она завершила свою работу. Например, если квантовый компьютер инициализирует набор кубитов суперпозицией всех комбинаций кубит-состояние, а затем применяет функцию к этому входному состоянию, результирующее квантовое состояние будет иметь информацию о значении функции для каждого возможного входного значения. Однако прямое измерение этой квантовой системы не даст этой информации. Вместо этого, поскольку все входные варианты были равновероятными, измерение вернёт только один из 2^n возможных выходных данных. Ключом к успешному квантовому алгоритму является манипулирование системой таким образом, чтобы состояния, соответствующие искомому решению, имели гораздо более высокую вероятность измерения, чем любой другой возможный результат. Это условие присуще примитивам квантовых алгоритмов, таким как квантовое преобразование Фурье и усиление амплитуды, которые более подробно описаны в главе 3. Эти операции усиливают коэффициент состояния, индекс которого указывает на искомый ответ, так что осмысленный ответ сильно вероятно, будет наблюдаться при измерении считывания; однако они могут потребовать нетривиального количества времени, что снижает общее ускорение квантового алгоритма.

Характеристики квантовых явлений не только обеспечивают вычислительную мощность квантового компьютера, но и сильно ограничивают возможности его использования.

2.6 Потенциал функциональных квантовых компьютеров

Как отмечалось ранее, вычисления, основанные на квантовых, а не на классических взаимодействиях, открывают возможности для нового типа вычислительной машины. У него есть потенциал для решения некоторых вычислительных проблем, которые в настоящее

время неразрешимы даже на самых мощных суперкомпьютерах сегодня и на любом классическом компьютере будущего. Например, помимо интереса к потенциальным крипто-аналитическим приложениям, существует большой интерес к приложениям, связанным с моделированием квантовых систем, имеющих значение для химии, материаловедения и биологии, в частности, с потенциальными приложениями для разработки новых материалов.

Экспериментаторы по всему миру работают над созданием как вентильных, так и аналоговых компьютеров, которые могли бы выполнять полезные вычисления, используя ряд базовых технологий кубитов. В оставшейся части этого отчёта будет обсуждаться прогресс, достигнутый в разработке полезных приложений для этих машин, а также в создании аппаратных и программных платформ, необходимых для создания квантового компьютера. Поскольку устройства квантовых вычислений, как правило, находятся на ранних стадиях и поскольку возможности устройств будут зависеть от их типа и уровня зрелости, полезно определить несколько различных категорий квантовых компьютеров для удобства ссылок и сравнения, как указано ниже:

Аналоговый квантовый компьютер (квантовый отжиг, адиабатический квантовый компьютер, прямое квантовое моделирование). Такая система будет работать за счёт когерентного манипулирования кубитами путём изменения аналоговых значений гамильтониана системы без использования квантовых вентилей. Например, вычисления на «квантовом отжиге» проводятся путём подготовки набора кубитов в некотором начальном состоянии и медленного изменения энергии, которую они испытывают, до тех пор, пока гамильтониан не определит параметры данной задачи, так что конечное состояние кубитов соответствует, с большой вероятностью, ответу задачи. «Адиабатический квантовый компьютер» (AQC) работает, переводя кубиты в основное состояние начального гамильтониана, а затем изменяя гамильтониан достаточно медленно, чтобы система оставалась в основном состоянии наименьшей энергии на протяжении всего процесса. AQC, хотя и не основанный на вентилях, обладает той же теоретической вычислительной мощностью, что и квантовый компьютер на основе вентилей, но не имеет практических средств для полной коррекции ошибок.

Шумный квантовый компьютер промежуточного масштаба (NISQ) на основе вентилей [33]. Такая система будет работать через логические операции над когерентным набором кубитов без полной квантовой коррекции ошибок, необходимой для подавления всех

ошибок; расчёты должны быть спроектированы так, чтобы их можно было выполнять в квантовых системах с некоторым шумом, и выполнять их за несколько шагов (достаточно мелкая логическая глубина), чтобы ошибки вентиля и декогерентность кубитов не заслоняли результаты. В книге эти системы также будут называться «цифровыми компьютерами NISQ».

Квантовые компьютеры на основе вентилей с полной коррекцией ошибок. Такая система будет работать посредством операций над кубитами на основе вентилей, реализуя квантовую коррекцию ошибок для исправления любого системного шума (включая ошибки, вызванные несовершенными управляющими сигналами или изготовлением устройства, или непреднамеренной связью кубитов друг с другом или с окружающей средой), которые возникают во время работы. сроки расчёта. В таких системах вероятность ошибок снижается настолько значительно, что машина кажется надёжной для всех вычислений. Конструкция этих машин должна позволять им масштабироваться, чтобы вмещать тысячи этих полностью исправленных ошибок или логических кубитов.

Квантовые компьютеры на основе вентилей могут иметь множество физических реализаций. Однако любые реализации должны удовлетворять знаменитым критериям Ди Винченцо, согласно которым они обладают следующим [34]:

1. хорошо охарактеризованные квантовые двухуровневые системы, которые можно использовать в качестве кубитов;
2. возможность инициализировать кубиты;
3. время декогеренции, достаточное для выполнения вычислений или исправления ошибок;
4. набор квантовых операций над кубитами, известный как «квантовые вентили», который является универсальным для квантовых вычислений;
5. возможность измерять квантовые биты один за другим, не мешая остальным.

Квантовые отжиги нуждаются во всем вышеперечисленном, кроме пункта 4, так как они не используют вентили для выражения своих алгоритмов. Однако декогеренция (пункт 3) играет совсем другую роль в квантовом отжиге, чем в модели ворот — в частности, некоторая декогерентность допустима при квантовом отжиге [35, 36], и для успеха квантового отжига необходима некоторая релаксация энергии. [37, 38]. На сегодняшний день достигнут прогресс в создании аналоговых квантовых и цифровых компьютерных систем NISQ, в то время как системы с полным исправлением ошибок гораздо сложнее.

Чтобы построить функциональный квантовый компьютер, необходимо создать физическую систему, которая кодирует кубиты, контролирует и манипулирует этими кубитами именно для выполнения вычислений. Сегодня экспериментаторы строят и эксплуатируют эти системы в тщательно контролируемых условиях в лабораториях. Две ведущие технологии квантовых вычислений — захваченные ионы и сверхпроводящие кубиты — используют очень разные стратегии для воплощения кубитов и работы с ними. Системы с захваченными ионами используют два внутренних состояния атома в качестве основного квантового элемента. Каждый атом лишается внешнего электрона, оставляя его положительно заряженным, так что их положением можно управлять с помощью электрических полей в устройствах, называемых «ионными ловушками». И ионы, и ловушки содержатся в камерах сверхвысокого вакуума, чтобы свести к минимуму взаимодействие с окружающей средой, а лазеры используются для охлаждения движения ионов до очень низких температур (0,1–1 мК). Хотя ионные ловушки обычно работают при комнатной температуре, их также можно охлаждать до криогенных температур (4–10 К) для улучшения условий вакуума или уменьшения влияния собственного электрического шума на движение ионов.

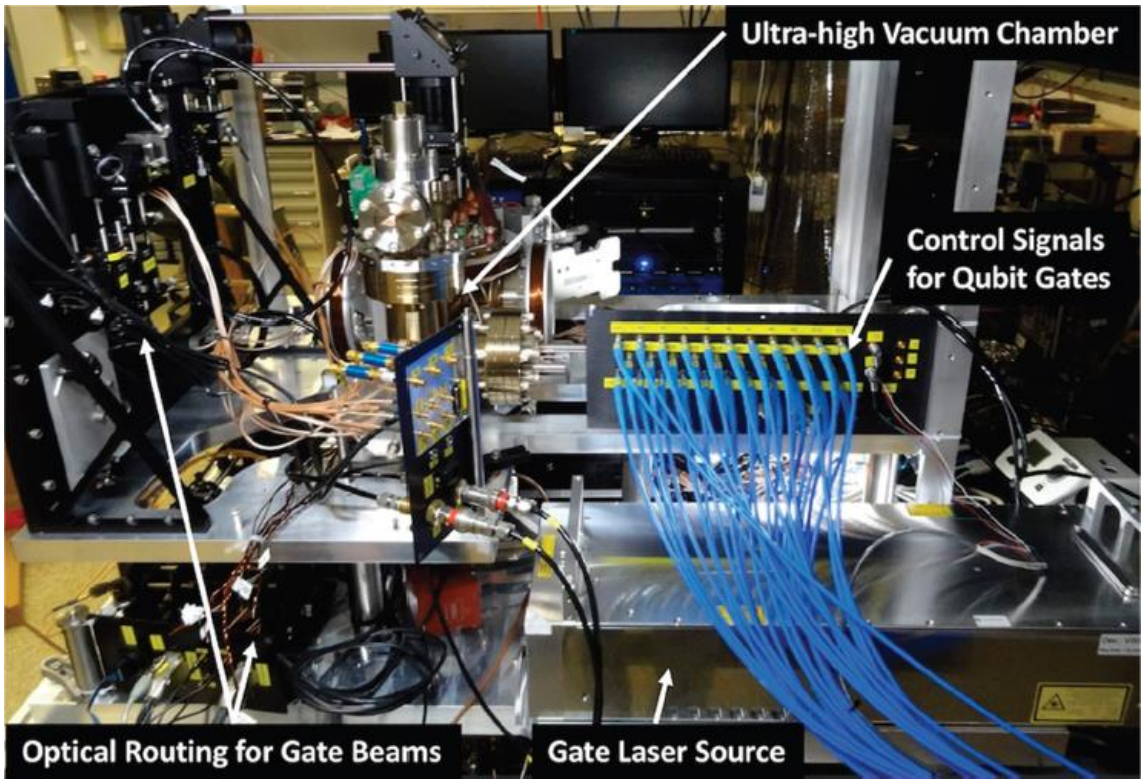


Рис. 2.2 Лабораторный прибор для современной системы ионной ловушки, работающий при комнатной температуре [39].

Состояние каждого иона можно изменить с помощью точно контролируемых лазерных импульсов или микроволнового излучения. Эти импульсы могут быть организованы так, чтобы соединять состояния двух или более ионов вместе, чтобы создать запутанность между ионами. Пример лабораторного оборудования, содержащего систему ионной ловушки и блоки управления, представлен на рис. 2.2. Здесь захваченные ионные кубиты размещены внутри камеры сверхвысокого вакуума. Квантовые логические вентили на кубитах осуществляются с помощью лазерных лучей от источника вентильного лазера, который модулируется управляющими сигналами (РЧ-сигналы, подаваемые по синим кабелям) и направляется на ионы с помощью оптической установки в системе.

Рис. 2.3. Лабораторное оборудование для современной системы сверхпроводящих кубитов [39].

Сверхпроводящие системы строятся с использованием совершенно другого подхода. Вместо использования естественной квантовой системы этот подход использует уникальные свойства сверхпроводящих материалов для создания схемы, которая действует как искусственный атом (эта схема по существу представляет собой нелинейный осциллятор, что означает, что, подобно атому, она поддерживает различные энергетические состояния, и разделение между энергетическими состояниями изменяется с уровнем энергии, так что промежуток между интересующими состояниями уникален, и интересующие состояния могут быть опрошены исключительно). Поскольку эту схему можно определить литографически как интегральную схему, можно построить массивы этих искусственных атомов, используя процесс, аналогичный тому, который используется

для изготовления ИС. Микроволновое излучение снова используется для манипулирования состоянием этих «атомов», а соседние «атомы» могут быть соединены электронным способом для создания запутанных состояний. К сожалению, уровни энергии в этих цепях все ещё очень малы, и эти цепи всегда находятся в контакте с материалом, на котором они построены. Следовательно, изоляция этих цепей требует их охлаждения примерно до 10 мК. На рис. 2.3 представлен снимок экспериментального сверхпроводящего квантового компьютера в лаборатории, включая часть оборудования, необходимого для поддержания температуры среды кубита и управления квантовой системой.

Развитие новых идей по построению вантовых компьютеров идёт постоянно. Даже пандемия Covid-19 не остановила дальнейших исследований в области построения квантовых компьютеров. Так в [40-41] описаны архитектурные элементы квантовых устройств, а работы [42-44] посвящены программному обеспечению для моделирования квантовых компьютеров.

Интерес к квантовым вычислениям возрос по мере улучшения времени когерентности и точности квантовых операций для базовых квантовых систем. В следующей главе мы рассмотрим потенциальные возможности квантового компьютера.

3. КВАНТОВЫЕ АЛГОРИТМЫ И ПРИЛОЖЕНИЯ

Основой области алгоритмов является принцип, согласно которому общее количество вычислительных шагов, необходимых для решения задачи, (приблизительно) не зависит от базовой конструкции компьютера — примечательно, что в первом приближении это называется одним шагом вычислений. является вопросом удобства и не меняет общего времени решения. Этот основной принцип, называемый расширенным тезисом Черча-Тьюринга, подразумевает, что для более быстрого решения вычислительной задачи можно (1) сократить время выполнения одного шага, (2) выполнить много шагов параллельно или (3) уменьшить общее количество шагов до завершения с помощью умного алгоритма.

Открытие того, что квантовые компьютеры нарушают расширенный тезис Чёрча-Тьюринга [10, 45] — решая определенные вычислительные задачи с экспоненциально меньшим количеством шагов, чем лучший классический алгоритм для той же задачи, — потрясло основы информатики и открыло возможность совершенно новый способ быстрого решения вычислительных задач[10]. Практический потенциал квантовых компьютеров был продемонстрирован вскоре после этого, когда Питер Шор создал квантовые алгоритмы для факторизации больших чисел и вычисления дискретных логарифмов, которые были экспоненциально быстрее, чем любые разработанные для классического компьютера [46-47][11]. Эти квантовые алгоритмы вызвали серьёзную озабоченность в сообществе безопасности, поскольку классическая сложность этих двух проблем лежит в основе «криптосистем» с открытым ключом, которые защищают подавляющее большинство цифровых данных общества.

Действительно, алгоритмы разложения больших чисел на множители веками изучались математиками, а в последние несколько десятилетий очень интенсивно - программистами. Основной проблемой в этих и большинстве других вычислительных задач является комбинаторный взрыв: экспоненциальное количество потенциальных решений, между которыми должен выбирать алгоритм.

---

[10] Обратите внимание, что квантовые компьютеры не нарушают исходный тезис Чёрча-Тьюринга, который определяет пределы того, что вообще возможно вычислить (независимо от времени, необходимого для выполнения вычислений. Расширенный тезис Чёрча-Тьюринга иногда называют «осуществимостью тезис» или «теоретический тезис Чёрча-Тьюринга о вычислительной сложности».

[11] Алгоритм Шора для факторизации масштабируется асимптотически как $O(n^3)$, по сравнению с $O(e^{\sqrt[3]{n}})$ для наилучшего классического подхода, общего алгоритма решета числового поля.

В случае факторизации n-битного числа N возможные простые делители N включают все простые числа, меньшие N, и таких простых чисел экспоненциально много. Действительно, самый быстрый классический алгоритм для фактического нахождения простых делителей N занимает $O(e^{\sqrt[3]{n}})$ шагов, в то время как квантовый алгоритм Шора требовал только $O(n^3)$ шагов, позже улучшенный до $O(n^2 \log n)$.

Очень общая цель области алгоритмов состоит в том, чтобы решить вычислительную задачу с помощью алгоритма, число шагов которого (в просторечии называемое «время выполнения») полиномиально зависит от размера n входных данных, тем самым минуя комбинаторный взрыв. Вычислительные задачи, для которых существуют такие полиномиальные (классические) алгоритмы, относятся к классу сложности P. Соответствующий класс сложности, квантовое полиномиальное время с ограниченной ошибкой (bounded-error quantum polynomial time (BQP)), содержит все те вычислительные задачи, которые мог бы решить квантовый компьютер. решить за полиномиальное время. Напротив, алгоритмы, время выполнения которых экспоненциально увеличивается в зависимости от размера входных данных, очень быстро становятся непомерно дорогими по мере увеличения размера входных данных.

Важно понимать, что квантовые компьютеры не одинаково ускоряют все вычислительные задачи. Один из наиболее важных классов вычислительных задач, NP-полные задачи [48], описывается как поиск иголки в экспоненциально большом стоге сена. Примерно в то же время, что и заявление Шора, Bennett et al. [49] доказали, что квантовым алгоритмам требуется экспоненциальное время для решения NP-полных задач в модели «черного ящика» — то есть, если алгоритм игнорирует детальную структуру проблемы — и, следовательно, маловероятно, что они обеспечивают экспоненциальное ускорение для таких задач. Точнее, если N обозначает размер стога сена, Bennett et al. показал, что любой квантовый алгоритм для поиска иглы должен выполнять не менее $\sqrt{N}$ шагов.

Несколько лет спустя Гровер показал, что существует квантовый алгоритм, который может найти иглу за $O(\sqrt{N})$ шагов [50]. Класс NP характеризуется тем, что классический компьютер должен иметь возможность проверить правильность решения за полиномиальное время (неважно насколько сложно найти правильное решение). NP-полные задачи — самые сложные задачи в NP, в том числе знаменитая задача коммивояжёра, а также тысячи задач из всех областей науки.

Широко распространено мнение, что P ≠ NP (это одна из знаменитых семи проблем тысячелетия Клэя) и что любой классический алгоритм должен требовать экспоненциальное количество шагов для решения NP-полных задач [51].

Дизайн квантовых алгоритмов следует принципам, совершенно отличным от принципов классических алгоритмов. Начнём с того, что даже классические алгоритмы должны быть приведены в особую форму — как обратимые алгоритмы — прежде чем их можно будет запустить на квантовом компьютере. Алгоритмы, обеспечивающие квантовое ускорение, используют определенные квантовые алгоритмические парадигмы или строительные блоки, не имеющие классических аналогов.

Существует обширная литература по квантовым алгоритмам, которая была разработана за четверть века с момента появления первых алгоритмов, рассмотренных выше. Все эти алгоритмы основаны на нескольких квантовых строительных блоках, описанных в следующем разделе и предназначенных для работы на идеальном квантовом компьютере. Настоящие квантовые устройства подвержены шумам окружающей среды, поэтому была разработана сложная теория квантовых кодов, исправляющих ошибки, и отказоустойчивых квантовых вычислений, чтобы преобразовать шумные квантовые компьютеры в идеальные квантовые компьютеры. Однако это преобразование влечёт за собой накладные расходы как по количеству кубитов, так и по времени выполнения.

Сейчас мы вступаем в эру шумных квантовых устройств промежуточного масштаба (NISQ) [12] — гонку по созданию квантовых компьютеров, которые достаточно велики (от десятков до сотен или нескольких тысяч кубитов), чтобы их нельзя было эффективно смоделировать с помощью классической компьютера, но не являются отказоустойчивыми и поэтому не могут напрямую реализовать алгоритмы, разработанные для идеальных квантовых компьютеров. В то время как огромный интерес и финансирование для создания компьютеров NISQ, несомненно, продвинули разработку масштабируемых, отказоустойчивых квантовых компьютеров, всё ещё предстоит проделать значительную работу, прежде чем будет построен идеальный квантовый компьютер.

Самые большие предстоящие проблемы связаны с алгоритмами; в ближайшей перспективе это включает поиск вычислительных задач, которые такие компьютеры могут ускорить. Разработка алгоритмов, работающих на компьютерах NISQ, так же важна, как и создание физических устройств, поскольку без того и другого машина

бесполезна. В долгосрочной перспективе предстоит ещё много работы в области квантовых алгоритмов для идеальных (масштабируемых, отказоустойчивых) квантовых компьютеров. В следующем разделе описываются основные строительные блоки для квантовых алгоритмов, а также известные алгоритмы для идеальных квантовых компьютеров, которые обеспечивают ускорение по сравнению с лучшими классическими алгоритмами для тех же вычислительных задач. В следующем разделе описываются методы квантовой коррекции ошибок и отказоустойчивости для преобразования шумного квантового компьютера в идеальный квантовый компьютер. Глава завершается обсуждением основных алгоритмических проблем, связанных с компьютерами NISQ, и наиболее многообещающими направлениями поиска таких алгоритмов.

3.1. Квантовые алгоритмы для идеального квантового компьютера на вентилях.

Сила квантовых алгоритмов в конечном счёте проистекает из экспоненциальной сложности квантовых систем — состояние системы из n запутанных кубитов описывается (и, таким образом, может кодироваться) $N = 2^n$ комплексных коэффициентов, как обсуждалось в предыдущей главе. Более того, применение каждого элементарного вентиля, скажем, к двум кубитам обновляет 2^n комплексных чисел, описывающих состояние, таким образом, кажется, что выполняется 2^n вычислений за один шаг. С другой стороны, в конце вычислений, когда измеряются n кубитов, в результате получается только n классических битов. Задача разработки полезных и выгодных квантовых алгоритмов проистекает из противоречия между этими двумя явлениями — необходимо найти задачи, оперативные решения которых используют этот параллелизм и дают конечное квантовое состояние, которое с высокой вероятностью возвращает ценную информацию при измерении. Успешные подходы используют явление квантовой интерференции для получения полезных результатов. Далее описаны некоторые из основных строительных блоков квантовых алгоритмов, а также несколько основополагающих квантовых алгоритмов и то, как их можно использовать для решения различных видов абстрактных задач.

3.1.1 Квантовое преобразование Фурье и квантовая выборка Фурье

Одним из самых основных строительных блоков для квантовых алгоритмов является алгоритм квантового преобразования Фурье (КПФ). Преобразование Фурье, важный шаг во многих классических расчётах и вычислениях, представляет собой операцию, которая преобразует одно представление интересующего сигнала в другую

форму представления. Классическое преобразование Фурье превращает сигнал, представленный как функция времени, в соответствующий ему сигнал, представленный как функция частоты. Например, это может означать преобразование математического описания музыкального аккорда в терминах давления воздуха как функции времени в амплитуды набора музыкальных тонов (или нот), которые объединяются, чтобы сформировать аккорд. Это преобразование обратимо с помощью обратного преобразования Фурье, поэтому не происходит потери информации — ключевое требование для любой операции на квантовом компьютере. Конкретно, вход представляет собой N-мерный вектор с комплексными элементами $(a_1, a_2, \dots, a_N)$, а выход представляет собой N-мерный вектор с комплексными элементами $(b_1, b_2, \dots, b_N)$, который получается путем умножения входного вектора с матрицей преобразования Фурье $N \times N$.

Учитывая востребованность преобразования Фурье, было разработано множество умных алгоритмов для его реализации на классических компьютерах. Лучшее, быстрое преобразование Фурье (БПФ), занимает время $O(N \log N)$, что лишь немного больше, чем требуется для чтения входных данных $[O(N)]$. В то время как классическое БПФ довольно эффективно, КПФ работает экспоненциально быстрее, требуя только $O(\log^2 N) = O(n^2)$ времени (где $N = 2^n$) в своей первоначальной формулировке, позже улучшенной до $O(n \log n)$ [52].

Перед описанием КПФ важно понять, как вход и выход представлены в виде квантовых состояний. Вход $(a_1, a_2, \dots, a_N)$представлен как квантовое состояние $\sum_i a_i |i\rangle$, а выход $(b_1, b_2, \dots, b_N)$ представлен в виде квантового состояния $\sum_i b_i |i\rangle$. Таким образом, вход и выход представлены состояниями всего n кубитов, где $n = \log N$. Это показано на рис. 3.1. Экспоненциальное ускорение возможно только в том случае, если входные данные уже закодированы в компактное квантовое состояние или могут быть закодированы в это состояние за $O(\log N)$ шагов. Квантовая схема, которая выполняет это преобразование, имеет общее количество вентилей, которое масштабируется как $O(n \log n)$. Другое предостережение состоит в том, что, конечно, нельзя получить доступ к амплитудам bi посредством измерения. Действительно, если измеряется выход КПФ, он даёт индекс i с вероятностью $|b_i|^2$. Таким образом, измерение выходных данных этого алгоритма дает только индекс вероятного выходного сигнала, который называется квантовой выборкой Фурье (КВФ). Она является важным примитивом в квантовых алгоритмах и влечёт за

собой применение КПФ и измерение выходного состояния, что приводит к выборке индекса i из определенного распределения вероятностей.

Во-первых, поскольку для чтения входных данных требуется $O(N)$ времени, квантовый алгоритм может быть завершен только за $O(\log^2 N)$, то есть он может дать ускорение только по сравнению с его классическим аналогом, если входные данные предварительно закодированы в $\log N$ кубитов и не считываются напрямую из файла данных. Эти $\log N$ кубитов находятся в суперпозиции N квантовых состояний, и коэффициент для каждого состояния представляет последовательность данных, подлежащую преобразованию. Это показано на рис. 3.1. Применение алгоритма КПФ к этим данным изменяет состояние $\log N$ кубитов таким образом, что новые коэффициенты представляют собой преобразование Фурье входных коэффициентов. Конечно, поскольку вывод представляет собой квантовое состояние, напрямую прочитать эти значения невозможно. Когда измеряется выход, наблюдается только одно из N возможных классических выходных состояний. Вероятность того, что любое из N состояний будет наблюдаться, равна квадрату абсолютного значения коэффициента этого состояния, который также является квадратом значения его преобразования Фурье. Выполнение КПФ на наборе кубитов и последующее измерение их конечного состояния решает ту же задачу, что и то, что классически называют выборкой Фурье.

Оказывается, выборка результатов преобразования Фурье в некоторых случаях полезна для нахождения структуры в последовательности чисел, как показано на рис. 3.1. Обратите внимание, что коэффициенты входных данных являются периодическими, с четырьмя периодами в этой последовательности. Эта периодичность обусловливает большую амплитуду состояния $|100\rangle$, чем у всех остальных, поэтому с высокой вероятностью измерение конечного состояния системы вернёт 100 (двоичное значение для 4), показывая, что входная последовательность повторяется 4 раза или имеет расстояние повторения, равное 2. Этот пример иллюстрирует мощность и подводные камни квантовых вычислений. Если начальная входная суперпозиция уже существует, преобразование Фурье может быть выполнено для коэффициентов суперпозиции экспоненциально быстрее, чем это было бы возможно классически. Однако в конце этой операции производится выборка только одного из N состояний, а не получение всего набора выходных коэффициентов. Кроме того, в целом неясно, как создать входную суперпозицию, не затрачивая $O(N)$ времени, хотя это становится

меньшей проблемой, если КПФ выполняется с предварительно загруженным входным квантовым состоянием как один шаг в более длинном алгоритме.

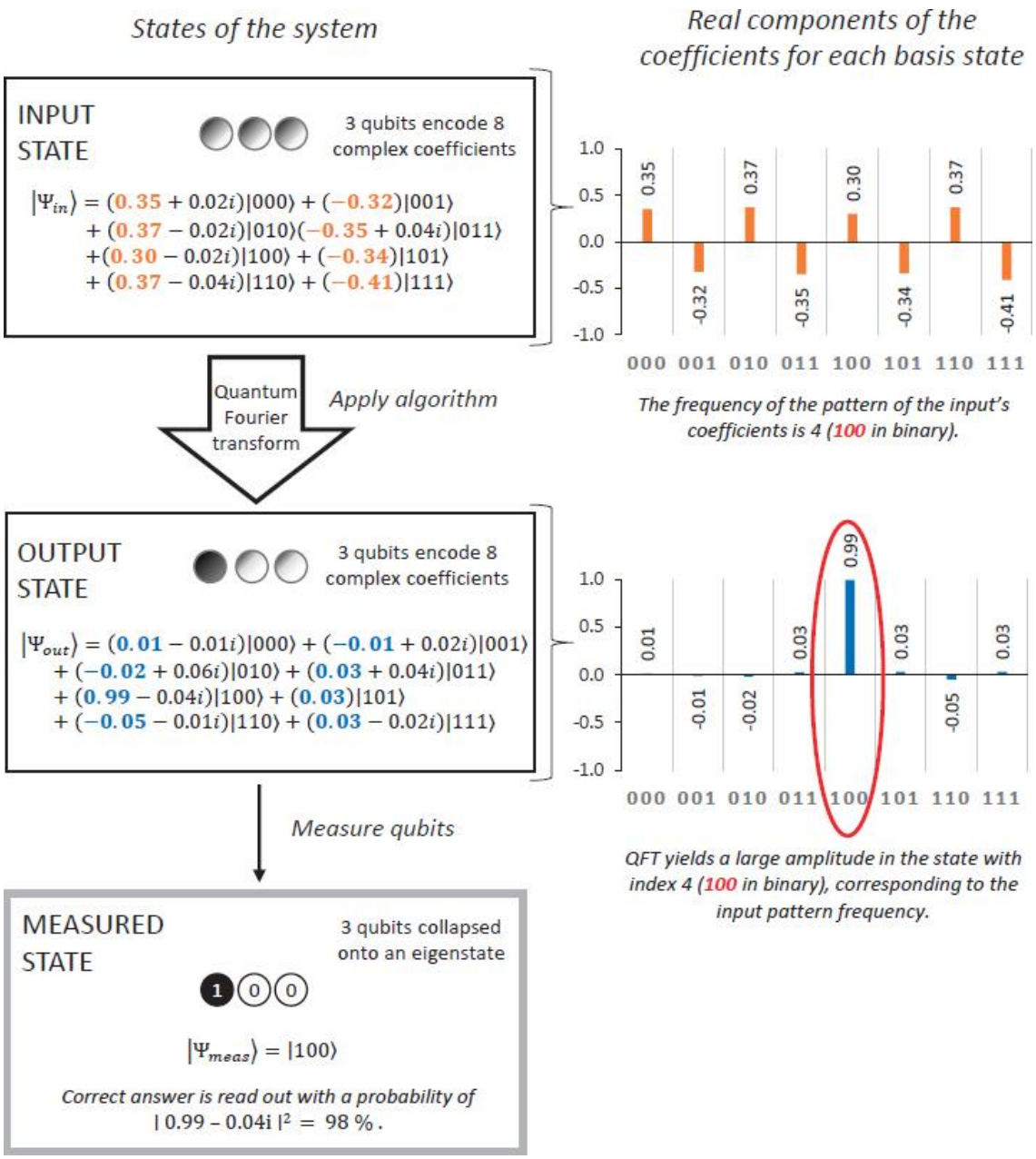


Рис. 3.1 Наглядный пример квантового преобразования Фурье (КПФ), применённого к системе с тремя кубитами [39]. [12]

[12] Три кубита должны быть изначально подготовлены таким образом, чтобы восемь ($2^3 = 8$) комплексных коэффициентов кодировали состояние системы, соответствующее последовательности значений, подлежащих преобразованию. Поскольку количество коэффициентов $N = 2^n$, где n — количество кубитов: 3 кубита могут представлять 8 значений. КПФ быстро находит закономерности во входной последовательности и определяет частоту их повторения. Все входные состояния здесь имеют одинаковую

КПФ, умело использует характеристики квантовых вычислений и полезна при построении множества квантовых алгоритмов. Примеры включают квантовый факторинг, поиск скрытой структуры и оценку квантовой фазы.

3.1.2 Квантовый факторинг и поиск скрытых структур

Открытие Шором полиномиальных алгоритмов разложения на множители и вычисления дискретных логарифмов [46] стало крупным прорывом в области квантовых алгоритмов как из-за очевидного ускорения по сравнению с классическими алгоритмами, так и из-за последствий этого ускорения для известных приложений. По сути, оба алгоритма можно рассматривать как оригинальный способ использования экспоненциального ускорения в КПФ, даже с учётом входных и выходных ограничений дискретизации Фурье.

Чтобы иметь возможность использовать возможности КПФ, Шор сначала преобразовал проблему нахождения множителей числа в задачу, включающую поиск повторяющегося паттерна — именно то, что обнаруживает КПФ. Шор смог показать, что проблема факторизации эквивалентна проблеме нахождения периода в последовательности чисел, хотя последовательность чисел экспоненциально длиннее, чем количество битов соответствующего числа, которое нужно разложить на множители. Таким образом, хотя эта эквивалентность не даёт никакой помощи в решении задачи на классическом компьютере (поскольку потребуется сгенерировать эту последовательность из 2^n чисел для факторизации n-битного числа, что заняло бы экспоненциальное количество времени), она идеальная задача для квантового компьютера. В квантовом компьютере экспоненциально длинная последовательность может быть закодирована всего в n кубитов и сгенерирована за время, полиномиальное от n. Как только эта последовательность сгенерирована, КПФ можно использовать для нахождения периода. Тот факт, что возвращаемый результат представляет собой только выборку выходных амплитуд ПФ, не является ограничивающим, поскольку желаемая информация, скорее всего, будет той, которая выберется при измерении.

Алгоритм Шора, если его развернуть на идеальном квантовом компьютере, позволит вычислить секретный ключ наиболее широко

вероятность, при этом действительные компоненты коэффициентов меняют знак четыре раза. Выходное состояние отражает это: a_i велик, если во входной последовательности i циклов. Таким образом, здесь все выходные сигналы малы, за исключением состояния 100, соответствующего частоте входного шаблона. Таким образом, измерение этого результата, вероятно, даст индекс этого сильного паттерна во входной последовательности.

используемой криптосистемы с открытым ключом, RSA. Кроме того, он сможет вычислить секретный ключ других широко используемых криптосистем с открытым ключом, таких как криптография Диффи-Хеллмана и криптография на эллиптических кривых.

Квантовый алгоритм Шора для факторинга и дискретного логарифмирования можно рассматривать как примеры обнаружения скрытой алгебраической структуры, связанной с известной математической проблемой, называемой «проблемой скрытых подгрупп» [53, 54]. В настоящее время существуют квантовые подходы для эффективного решения некоторых случаев этой проблемы, в частности, для так называемых абелевых и близких к ним групп (характеризующихся своими свойствами симметрии). С другой стороны, ожидается, что проблема будет сложной для так называемой группы диэдральной симметрии. Эта трудная проблема тесно связана с другой, называемой проблемой кратчайшего вектора, которая лежит в основе криптосистемы обучения с ошибками, одного из предложенных постквантовых (то есть квантово-устойчивых) шифров.

3.1.3 Алгоритм Гровера и квантовые случайные блуждания

Хотя КПФ лежит в основе многих квантовых алгоритмов, другой класс алгоритмов использует преимущества метода, называемого «квантовым случайным блужданием». Этот метод аналогичен классическим методам случайного блуждания, которые вероятностно имитируют продвижение по некоторой местности.

Алгоритм Гровера решает конкретную проблему поиска уникальных входных данных для заданной функции, которые дадут определенный результат[13] [50]. Классически это базовая задача NP-жёсткого поиска, то есть нет известных решений данной задачи за полиномиальное время. В отсутствие информации о характере функции самым быстрым известным классическим алгоритмом для этой задачи является полный поиск или исследование всех возможных входных данных для поиска ответа — процесс, который занимает $O(N) = O(2^n)$ шагов, где n — количество битов, необходимых для представления входных данных. Алгоритм Гровера решает эту задачу за $O\left(\sqrt{N}\right)$ шагов. Хотя это всего лишь полиномиальное ускорение по сравнению с лучшим классическим подходом, тем не менее, на практике оно может быть значительным. Как будет показано в следующей главе, этого может быть достаточно для компрометации некоторых криптографических операций. Более того, это оптимальный квантовый алгоритм для данной задачи, в свете результата Беннета и

[13] Проблему можно сформулировать следующим образом: найдите x, если $f(x) = 1$.

др. [49], показывая, что любой квантовый алгоритм должен предпринять по крайней мере $\sqrt{N}$ шагов для решения этой проблемы в модели черного ящика.

Проблема с классическим методом исчерпывающего поиска заключается в том, что систематическая проверка каждого возможного ответа представляет собой слепое угадывание и проверку: каждый запрос не предоставляет никакой информации об ответе до тех пор, пока он не будет найден. Чтобы обойти эту проблему, алгоритм Гровера использует набор из двух операций над кубитами. Первый – эффективно помечает состояние, соответствующее правильному ответу, изменяя знак его коэффициента. Второй, называемый оператором диффузии Гровера, может затем немного увеличить величину этого коэффициента. Вместе эти два шага составляют так называемую итерацию Гровера, каждое применение которой увеличивает вероятность того, что правильный ответ будет прочитан при измерении. Эта процедура увеличения амплитуды состояний, содержащих правильный ответ, является примером общего алгоритмического подхода, называемого усилением амплитуды [55], который полезен в ряде квантовых алгоритмов.

Последовательность операций усиления амплитуды можно рассматривать как своего рода квантовое случайное блуждание; однако алгоритм Гровера выполняет «проход» назад, от распределённого состояния (аналогично всем возможным конечным точкам случайного блуждания из заданной начальной точки) обратно в состояние, сфокусированное вокруг единственного верного компонента (аналогично начальной точке блуждания). Классический метод случайного блуждания может исследовать площадь, пропорциональную квадратному корню из числа шагов; квантовое случайное блуждание может исследовать область, пропорциональную количеству шагов. Следовательно, квантовый алгоритм обеспечивает квадратичное ускорение.

Этот метод универсален и привёл к созданию ряда квантовых алгоритмов, обеспечивающих полиномиальное ускорение для конкретных вычислительных задач. Например, существует основанный на квантовом блуждании алгоритм для решения основной проблемы определения того, имеет ли игрок, делающий первый ход, выигрышную стратегию в комбинаторной игре (например, в шахматах). Наивный классический алгоритм включает экспоненциальный поиск возможных ходов и исходов, называемый «игровым деревом», в то время как квантовый алгоритм обеспечивает квадратичное ускорение, описанное выше. В более общем смысле

квантовый алгоритм обеспечивает квадратичное ускорение вычисления любой формулы И-ИЛИ [56, 57].

Хотя алгоритм Гровера часто называют квантовым «поиском», это не совсем правильное применение данного метода. Чтобы выполнить настоящий квантовый поиск, набор искомых данных должен быть сначала представлен в виде суперпозиции квантовых состояний, а для того, чтобы квантовый алгоритм обеспечил какое-либо ускорение, это представление должно быть создано за время, намного меньшее, чем количество точек данных, N — где-то между $O(1)$ и $O(\log N)$. В классическом случае эти данные просто хранились бы в оперативной памяти (ОЗУ) и вызывались по мере необходимости. Однако, хотя ОЗУ является ключевым элементом классических вычислений, в настоящее время не существует надёжного практического эквивалента ОЗУ, который генерирует необходимое состояние квантовой суперпозиции для квантового компьютера.

Было высказано предположение, что квантовая версия оперативной памяти (КОЗУ) может генерировать эти данные за время $O(\log N)$ [58], хотя на практике это не было продемонстрировано. Для этого классический блок хранения данных должен быть дополнен квантовой логикой вокруг ячеек памяти. Существует классический аналог этой структуры, называемый памятью с адресацией по содержимому, или ПАС, которая решает эту задачу поиска за время $O(\log N)$. Однако с ПАС и КОЗУ получение данных в устройство в первую очередь по-прежнему занимает $O(N)$ времени, поэтому любой подход будет полезен только тогда, когда выполняется несколько запросов к одному и тому же набору данных, то есть полезность ПАС и КОЗУ, если они могут быть построены, растут прямо пропорционально количеству повторных использований входных данных.

3.1.4 Алгоритмы гамильтонового моделирования

Моделирование динамики квантовых систем является наиболее естественным и очевидным применением квантовых компьютеров и послужило мотивом для новаторского исследования квантовых вычислений Ричардом Фейнманом [5]. Квантовые алгоритмы могут экспоненциально превосходить классические при моделировании системы со многими квантовыми степенями свободы, с приложениями, включая проблемы в химии, материаловедении, конденсированных средах, ядерной физике и физике высоких энергий.

Общая цель моделирования квантовой системы состоит в том, чтобы определить её структуру или поведение, зная её компоненты и

среду, в которой она существует. Например, моделирование можно использовать для выяснения структуры вещества или поведения набора взаимодействующих частиц во времени. Эти проблемы могут иметь множество применений, от разработки новых промышленных материалов до решения важных физических задач. Как правило, для этих симуляций требуется знание гамильтониана (оператора энергии), описывающего все элементы и взаимодействия системы. Отсюда можно либо найти волновую функцию основного состояния для этой системы (в не зависящей от времени картине), либо, учитывая некоторое начальное состояние системы в момент времени t_0, вычислить близкое приближение к квантовому состоянию в точке будущего времени t. Учёные выполняли классические симуляции квантовых систем на протяжении десятилетий, либо ограничивая внимание небольшими системами, либо полагаясь на приближённые методы, которые могут пожертвовать точностью ради вычислительной эффективности. Точные модели настолько требовательны к вычислениям (учитывая присущую квантовым системам высокую размерность), что не подходят для большинства систем, кроме небольших.

Квантовое, а не классическое моделирование, естественно, лучше приспособлено для исследования пространства состояний, охватываемого квантовыми системами. В принципе, квантовое моделирование может осуществляться как минимум тремя общими подходами, каждый из которых обещает более эффективные методы решения в определенных задачах. Первый подход включает в себя реализацию алгоритмов эволюции во времени на квантовом компьютере на основе вентилей, обычно называемого «гамильтоновым моделированием». Второй — это вариационный подход к получению аппроксимаций квантовых состояний с помощью квантовых компьютеров, который будет обсуждаться далее в этой главе. Наконец, в области аналогового квантового моделирования специальные квантовые системы, хотя и не полноценные квантовые компьютеры, создаются для эмуляции определенных гамильтонианов. Хотя это аппаратное обеспечение, вероятно, будет намного проще, чем машина на основе вентилей, решающая ту же проблему, недостатком подхода аналогового моделирования является то, что аппаратное обеспечение имеет ограничения на гамильтонианы, которые оно может создать, поэтому результирующая система является специализированной, а приложение и симулятор должны разрабатываться совместно. Кроме того, в отличие от цифровых квантовых вычислений, которые можно защитить с помощью отказоустойчивых протоколов, возможность

выполнения аналогового квантового моделирования в реалистичных шумных средах менее изучена.

В алгоритмах моделирования гамильтониана с временной эволюцией в качестве входных данных должны быть представлены форма гамильтониана и, возможно, его собственная зависимость от времени, а также начальное состояние системы. Алгоритм начинается с установки кубитов в начальное состояние системы или приближения к нему. Затем система перемещается во времени или «распространяется» в соответствии с её гамильтонианом в дискретных интервалах Δt на количество итераций, необходимых для достижения интересующего момента времени t_f. На практике общий гамильтониан обычно представляется в виде суммы меньших, так называемых локальных гамильтонианов, каждый из которых действует только на компонент большей системы, что обеспечивает полезную декомпозицию (в более общем случае гамильтониан можно эффективно моделировать при условии, что он разреженный, и ненулевые элементы в любой заданной строке могут быть эффективно обнаружены и вычислены). Чтобы процесс протекал эффективно, для рассматриваемой системы необходимо тщательно выбирать метод кодирования начального состояния в кубитах и представления распространения во времени в виде последовательности вентилей. Первые конкретные квантовые алгоритмы для моделирования гамильтониана на основе вентилей были разработаны в середине 1990-х годов [59], за ними последовали дополнительные методы для различных типов квантовых систем, а также алгоритмические идеи, которые привели к значительному сокращению времени [60-66].

Эффективное моделирование гамильтониана на квантовом компьютере позволит значительно ускорить решение задач квантовой химии и моделирования материалов [67, 68]. В частности, проблема электронной корреляции была одной из самых сложных задач для решения классическими методами [69]. Чтобы понять и предсказать сложные механизмы реакций, участвующих, например, в химическом превращении, катализируемом переходными металлами, требуются чрезвычайно точные подходы к электронной структуре. Классически даже молекулы с менее чем сотней сильно коррелированных электронов выходят за пределы шкалы классических методов с требуемой химической точностью. Квантовые компьютеры обещают экспоненциальное ускорение моделирования проблемы электронной структуры, и было показано, что они позволят эффективно объяснять механизмы химических реакций [70]. Здесь квантовый компьютер может позволить исследователям вычислить или определить энергии

химических промежуточных соединений и переходных состояний и, в свою очередь, помочь найти точные энергии активации химических процессов, которые важны для понимания кинетики химических реакций [71]. Сильно коррелированные виды, участвующие в химических реакциях, где классические подходы в настоящее время не работают, включают такие проблемы, как фотохимические процессы, фиксация азота, разрыв связи C-H, фиксация и преобразование диоксида углерода, производство водорода и кислорода и другие проблемы катализа переходными металлами. Эти приложения распространяются на важные промышленные приложения, включая производство удобрений, катализация полимеризации и экологически чистые энергетические процессы [70]. Гамильтоновое моделирование также используется в квантовых алгоритмах для решения сложных коррелированных материальных задач [72], которые могут найти применение, например, при поиске высокотемпературного сверхпроводника. Квантовые компьютеры в дальнейшем обещают экспоненциальное ускорение по сравнению с классическими подходами. Таким образом, квантовые компьютеры могут оказать наибольшее влияние при решении задач квантовой химии, например, применительно к фармацевтике и материаловедению [73].

Однако существует много типов гамильтонианов, для которых потребуются новые методы, если они должны стать эффективно решаемыми на квантовом компьютере. Например, для моделирования электронной структуры для приложений в квантовой химии [74] гамильтониан n-орбитальной системы включает члены $O(n^4)$, что означает, что для его вычисления потребуется квантовый компьютер с малой ошибкой. Классические подходы к решению таких задач опирались на понимание физической структуры системы для создания специальных методов [73]. Исследователи недавно объединили эти методы с существующей структурой квантового моделирования гамильтониана, что привело к быстрому прогрессу в создании алгоритмов, решающих подобные задачи [68, 75-82].

Гамильтоновое моделирование также оказалось мощным инструментом разработки квантовых алгоритмов для задач, не имеющих непосредственной связи с квантовой механикой. Ярким примером является недавняя разработка нового класса квантовых алгоритмов, которые непосредственно строят линейную алгебру над квантовым состоянием.

3.1.5 Квантовые алгоритмы для линейной алгебры

Линейная алгебра, фундаментальная область математики, может быть полезна в различных контекстах, от науки о квантовой механике до дизайна компьютерной графики и методов машинного обучения. Общая задача линейной алгебры состоит в том, чтобы найти решение системы линейных уравнений, то есть одного или нескольких уравнений вида, где сумма набора независимых переменных, каждая из которых масштабируется некоторым коэффициентом, равна постоянной величине. Математически говоря, такую задачу можно записать в матричной форме как $Ax = b$, где A — матрица размера $N \times N$, элементами которой являются коэффициенты при переменных в уравнениях, x — вектор-столбец, элементами которого являются все переменные для решения, а b - вектор-столбец констант.

Квантовый алгоритм для таких приложений, названный ХХЛ в честь его разработчиков Харроу, Хассидима и Ллойда, использует методы гамильтонового моделирования [83]. Предполагается, что входной вектор b задан как квантовое состояние $\log N$ кубитов $|b\rangle = \sum_i |b_i\rangle$. Также предполагается, что матрица A разрежена и её элементы доступны через простую для вычисления функцию. Более того, он вычисляет выходной вектор x в виде квантового состояния $\log N$ кубитов $|x\rangle = \sum_i |x_i\rangle$. В основе алгоритма ХХЛ лежит один из основных строительных блоков квантового алгоритма: алгоритм квантовой оценки фазы Китаева. Это процедура экспоненциально быстрой оценки собственного значения (или фазы) собственного вектора унитарного оператора. Это относится к линейной алгебре, поскольку инвертировать матрицу A легко, если известны её собственные значения. Время работы алгоритма ХХЛ сравнимо с $O\left(\log^{\mathrm{k}} N\right)$ и числа обусловленности A. Конечно, доступ к решению x ограничен информацией, к которой можно легко получить доступ из квантового состояния $|\mathrm{x}\rangle$. Для данных A и b алгоритм выдаст квантовое состояние, для которого значения N коэффициентов пропорциональны N элементам решения x. Хотя решение присутствует в квантовом компьютере, правила квантовой механики не позволяют его прямое считывание. Однако, если кто-то заинтересован в нахождении только определенных средних значений решения, можно получить этот результат с числом вентилей, стоимость которого составляет $O\left(\log^{\mathrm{k}} N\right)$. [84].

Задачи линейной алгебры можно решить с помощью классического компьютера, использующего память и время работы, которые сравнимы с $\mathrm{O}(N^k)$, поэтому квантовый компьютер будет использовать экспоненциально меньше ресурсов и времени для

решения этой более ограниченной задачи. Недавняя связанная работа показала аналогичные результаты для решения линейных дифференциальных уравнений [85] и выполнения выпуклой оптимизации [86] в предположении, что входная матрица A очень разрежена, т. е. что большинство коэффициентов равны нулю, поскольку алгоритм работает полиномиально по количеству ненулевых элементов в строке.

Как и в случае с предыдущими алгоритмами, это экспоненциальное ускорение связано с рядом важных ограничений. Как упоминалось ранее, чтение вывода предоставляет только индекс i с вероятностью, пропорциональной $|x_i|^2$. Таким образом, одной из основных проблем при использовании этого алгоритма является поиск настроек, в которых эта ограниченная информация полезна. Одним из примеров такой настройки являются рекомендательные системы, в которых прошлые оценки нескольких продуктов группой пользователей (указаны матрицей) используются для предоставления персонализированных рекомендаций отдельным пользователям. Рекомендация — это продукт, который указывается индексом. Квантовый алгоритм для этой задачи был найден с экспоненциальным ускорением по сравнению с существующими классическими алгоритмами [87]. Недавно этот квантовый алгоритм вдохновил на создание нового классического алгоритма, который только полиномиально медленнее, чем квантовый алгоритм [88] (таким образом, прогресс в квантовых алгоритмах часто стимулирует новые достижения в классических алгоритмах).

Другая проблема заключается в том, что экспоненциальное ускорение присутствует только в том случае, если и вектор b, и матрица A уже закодированы в $\log N$ кубитов или если они могут быть закодированы в кубиты за $O(\log^k N)$ время. Это исключает чтение данных, поскольку простое чтение для создания данного состояния заняло бы как минимум $O(N)$ времени. Здесь экспоненциальное ускорение возможно только в том случае, если данные уже были приведены в квантовое состояние до запуска алгоритма или если найден какой-то метод для их эффективной подготовки.

Как упоминалось ранее, для экспоненциального ускорения недостаточная способность квантового процессора эффективно считывать большие объёмы данных является общей проблемой при разработке квантовых алгоритмов; вероятно, потребуется эффективное решение этой проблемы, чтобы многие алгоритмы могли быть полезны на практике. Конечно, даже если она не будет решена, квантовые алгоритмы все ещё могут обеспечить полиномиальное ускорение, тогда

как классические алгоритмы требуют $O(N^2)$ или более шагов для обработки ввода, поскольку квантовый компьютер может считывать данные за $O(N)$ шагов.

3.1.6 Требуемое качество машины

Алгоритмы, описанные в этом разделе, иллюстрируют типы задач, выполнение которых на квантовом компьютере привело бы к огромному вычислительному преимуществу. Для решения задач нужного размера им в основном требуются тысячи кубитов, что на несколько порядков больше, чем у современных машин. К сожалению, эти алгоритмы должны выполнять очень большое количество операций с кубитовыми вентилями, требуя порядка 10^{12} или даже 10^{18} операций. Для того чтобы эти результаты в конечном итоге были верными, частота ошибок логического элемента должна быть очень малой (порядка от 10^{-12} до 10^{-18}). Как объяснялось в главе 2, в отличие от современных классических компьютеров, чьи вентили могут достигать такой низкой частоты ошибок за счёт прямого подавления шума и создания выходных данных с меньшим уровнем шума, чем содержится на их входах, квантовые вентили имеют гораздо более высокую частоту ошибок. При этом современные квантовые компьютеры имеют частоту ошибок в диапазоне $10^{-2} - 10^{-3}$ и вряд ли достигнут требуемого уровня ошибки, необходимого для запуска этих квантовых алгоритмов в реальности. Квантовая коррекция ошибок — один из способов преодоления этого ограничения, и он описан далее.

3.2 Квантовая коррекция и снижение ошибок

Для уменьшения ошибок в квантовых системах были разработаны два общих подхода: исправление и смягчение. Из этих двух способов квантовая коррекция ошибок (QEC) — единственный способ значительно снизить эффективную частоту ошибок. Этот подход включает в себя кодирование квантового состояния с использованием множества избыточных кубитов и использование кода QEC (QECC), который использует эту избыточность информации для эмуляции стабильных кубитов с очень низким уровнем ошибок, часто называемых «отказоустойчивыми» или «логическими» кубитами. Состояние некоторых из этих дополнительных кубитов периодически измеряется, и классическое вычислительное устройство «декодирует» эту информацию, чтобы определить, какие кубиты имеют ошибки. Учитывая эту информацию, ошибки могут быть исправлены. Каждый логический кубит требует большого количества физических кубитов и множества операций квантовых вентилей (и классических вычислений) для достижения и поддержания своего состояния. Операции вентилей

над более надёжным логическим кубитом, который существует только как абстракция, должны быть преобразованы в операции над лежащими в их основе физическими кубитами. Таким образом, QEC несёт затраты, или «накладные расходы ресурсов», как на дополнительные кубиты для каждого логического кубита, так и на дополнительные квантовые вентили для каждой логической операции.

Квантовая коррекция ошибок — это активная область исследований квантовых алгоритмов, перед которой стоит цель значительно снизить накладные расходы в кубитах и времени для достижения полностью безошибочной работы. Большая часть этих исследований была сосредоточена на изучении поверхностных кодов и более широкого класса топологических кодов, частью которых они являются. Текущие коды для вентилей с коэффициентом ошибок 0,1 % по-прежнему требуют больших накладных расходов (до 15 000 раз) для создания логического кубита. До тех пор, пока не будет достигнут прорыв в сокращении частоты ошибок вентилей или уменьшении накладных расходах кода QEC, машины в ближайшем будущем не смогут создавать логические кубиты, что приведёт к созданию машин, которые должны справляться с шумом и ошибками (компьютеры NISQ). В краткосрочной перспективе исследователи обратились к подходам по уменьшению квантовых ошибок (QEM) и могут использовать QEC для снижения, но не устранения ошибок, поскольку количество ошибок падает.

3.2.1 Стратегии уменьшения квантовых ошибок

По сравнению с QEC, QEM имеет более скромную цель: уменьшить эффективную частоту ошибок квантовых вычислений для поддержки простых вычислений или для квантовых подходов, не основанных на вентилях, расширения когерентности несовершенных кубитов [89, 90] на достаточно продолжительное время, чтобы выполнять короткие алгоритмы. Поскольку более низкая частота ошибок снижает накладные расходы при использовании QEC, многие из этих стратегий снижения риска также могут использоваться с исправлением ошибок.

Сегодня широко используются два полезных подхода к уменьшению ошибок, в том числе применение составных импульсов и методов динамической развязки. Хотя такие методы не подавляют все типы ошибок, они могут быть разработаны для уменьшения известных систематических ошибок (составные импульсы) или когерентных ошибок расфазировки (последовательности динамической развязки).

Как для аналоговых, так и для цифровых квантовых компьютеров разрабатываются методы подавления ошибок, основанные на «энергетических штрафах» для подавления определенных типов ошибок. Эти подходы работают путём стратегического кодирования кубитов способами, для которых эти ошибки менее энергетически выгодны и, следовательно, менее вероятны. Кроме того, оба типа компьютеров могут использовать преимущества «подпространств без декогеренции», где многокубитные архитектуры спроектированы таким образом, что система кубитов нечувствительна к определенным источникам шума. Поскольку эти методы подавляют только определенные типы ошибок, улучшение коэффициента ошибок будет зависеть от системы и может быть скромным.

Ожидается, что QEM будет особенно важен для аналоговых квантовых компьютеров, поскольку в настоящее время не считается, что полное QEC достижимо практически в таких системах. В то время как QEC является корректирующим, т. е. измеряет ошибки, а затем исправляет их, методы QEM являются превентивными и пытаются уменьшить неблагоприятное воздействие шума и вероятность ошибок.

3.2.2 Коды квантовой коррекции ошибок

Первые коды квантовой коррекции ошибок были разработаны в середине 1990-х годов [90, 91]. Дальнейшая работа предоставила практическое понимание порога ошибки, то есть максимально допустимой частоты ошибок каждого физического элемента в реальном устройстве, для которого QEC исправляет больше ошибок, чем вносит [91, 92]. Однако достижение как количества, так и точности кубитов, необходимых для успешной реализации QEC и обеспечения отказоустойчивых вычислений, оказалось сложной задачей.

В классических вычислениях один из простейших типов кодов исправления ошибок, называемый «повторяющимся кодом», копирует каждый бит информации в несколько битов, чтобы сохранить информацию за счёт избыточности. Все операции шлюза также реплицируются для поддержания этой избыточности. Все эти биты имеют одинаковое значение, если только не произойдёт ошибка, которая приведёт к тому, что одному из битов будет присвоено неправильное значение. Поскольку вероятность возникновения какой-либо ошибки невелика, правильное значение может быть определено как значение, которое содержится в большинстве копий. «Расстояние» кода исправления ошибок — это минимальное количество ошибок, которое необходимо для преобразования одного допустимого представления данных в другое допустимое представление данных.

Тройной код (каждый бит либо 000, либо 111) является кодом расстояния 3, поскольку нужно изменить все три бита, чтобы перейти от одного действительного представления, 111, к другому действительному представлению, 000. В общем, расстояние D код может исправить $(D-1)/2$ ошибки, поэтому тройной код может исправить одну ошибку. Это имеет смысл, так как даже если произошла только одна ошибка, большинство битов по-прежнему будут представлять верные значение.

Подходы к QEC аналогичны этому классическому подходу. Однако точная реализация QEC требует совершенно иных методов, чем классический повторный код, потому что квантовая информация не может быть скопирована напрямую, как описано в теореме о запрете клонирования [23], а также из-за дополнительных типов ошибок, которые могут возникать в квантовых вентилях. Тем не менее, были разработаны протоколы QEC, которые позволяют кодировать логический кубит в распределённую структуру физических кубитов. Поскольку эти кубиты содержат квантовое состояние, ни один из них нельзя измерить напрямую: любое измерение приведёт к коллапсу квантового состояния и разрушению вычислений. Вместо этого два кубита, которые должны иметь одинаковое значение, сравниваются друг с другом, и все, что нужно прочитать, — это согласованность этих двух кубитов. Такое измерение не раскрывает значение кубита, поэтому не приводит к коллапсу квантового состояния. Измеряемые кубиты иногда называют «синдромными» или «вспомогательными» кубитами (Вставка 3.1). Из всех этих сравнительных измерений и знаний об используемых QECC классический компьютер может вычислить, какие кубиты имеют ошибки и какой тип ошибки имеет кубит. Таким образом, он может обеспечить квантовую операцию, которую необходимо применить для устранения ошибок в квантовом состоянии. Хотя эти операции могут быть непосредственно применены к физическим кубитам, для ПО часто более эффективно «виртуально» применять эти исправления, изменяя будущие операции для учёта подобных ошибок, а не добавляя отдельный шаг только для их исправления.

Классический алгоритм, также называемый «алгоритмом декодирования» или «декодером», который принимает измерения синдрома в качестве входных данных и вычисляет, какие кубиты имеют ошибки, становится сложнее по мере увеличения расстояния, чтобы справиться с более высоким уровнем ошибок. Если частота ошибок близка к порогу ошибки, не только сильно возрастают накладные расходы, но и алгоритм декодирования также усложняется.

Если частота ошибок невысока или для работы алгоритма требуется очень мало логических кубитов, то в качестве декодера можно использовать небольшую таблицу поиска.

Вставка 3.1

Использование вспомогательных кубитов для квантовой коррекции ошибок.

Для исправления ошибок необходимо воспроизвести состояние кубита на несколько других кубитов. Хотя теорема об отсутствии клонирования не позволяет копировать состояние одного кубита непосредственно в другой, можно создать избыточное запутанное состояние многих кубитов.

Суть в том, что запутываемые кубиты должны начинаться с известного состояния. Кубиты с известным состоянием (например, это будет состояние $|0\rangle$), называемые «вспомогательными кубитами», могут быть добавлены к вычислениям для этой цели. Поскольку состояние вспомогательных кубитов известно, можно создать простую схему, которая сделает выходное состояние всех этих вспомогательных кубитов соответствующим защищенному кубиту: пропустите каждый вспомогательный элемент через вентиль «CNOT», где управление осуществляется кубитом, который нужно повторить. Предположим, что имеется кубит с состоянием ψ, который мы хотим защитить, где $|\psi\rangle$ представляет произвольное состояние суперпозиции $|\psi\rangle = a_0|0\rangle + a_1|1\rangle$. В вентиле CNOT состояние $|0\rangle$ вспомогательного кубита состояние останется как $|0\rangle$ состояние компоненты $|\psi\rangle$, но он будет преобразован в $|1\rangle$ по $|1\rangle$ состоянию компоненты $|\psi\rangle$. Результатом этой операции является вновь запутанное двухкубитное состояние $a_0|00\rangle + a_1|11\rangle$, создавая систему, в которой вспомогательный кубит теперь полностью запутан с первым кубитом. Добавление дополнительных вспомогательных кубитов увеличивает расстояние повторяющегося кода.

Вычислительная сложность декодера ошибок может быть проблемой, поскольку выполнение QEC тесно связывает кубиты квантового компьютера и классического управляющего процессора, который декодирует ошибки и выбирает следующие операции квантовых вентилей для выполнения. На высоком уровне необходимы следующие операции.

1. Управляющий процессор отправляет кубитам квантовую операцию, и для выполнения операций требуется некоторое время.

2. Вспомогательный кубит должен быть измерен и отправлен обратно в управляющий процессор.
3. Управляющий процессор должен использовать измерения для декодирования присутствующих ошибок.
4. Нужно обновлять свои будущие операции для учёта этих ошибок.

Для квантового компьютера проще всего, если классический компьютер может декодировать состояние ошибки, не замедляя следующую квантовую операцию. Для сверхпроводящего квантового компьютера это означает, что у классического компьютера есть всего несколько сотен наносекунд (порядка тысячи инструкций в современном процессоре) для декодирования ошибок. Если это невозможно, то для решения проблемы можно использовать специальное оборудование для ускорения вычислений или изменение алгоритма QEC, позволяющее выполнять дополнительные квантовые операции до декодирования информации об ошибке. Если эти методы не будут реализованы, добавленное время снизит эффективную скорость квантового компьютера, а задержки между логическими элементами приведут к дополнительной декогеренции и более высокому уровню ошибок.

3.2.3 Накладные расходы на квантовую коррекцию ошибок

Количество физических кубитов, необходимых для кодирования отказоустойчивого логического кубита, зависит от частоты ошибок физического квантового устройства и требуемого расстояния или способности защиты выбранного квантового кода с исправлением ошибок. В качестве простого примера рассмотрим так называемый код Стина с квантовой коррекцией ошибок. Этот подход кодирует один логический кубит в семь физических кубитов и имеет расстояние, равное трём[14], что означает, что он может исправить одну ошибку. Чтобы получить протокол с более высоким расстоянием (тот, который может исправлять дополнительные ошибки) с использованием кода Стина, можно использовать рекурсивный подход, называемый «конкатенацией». По сути, это влечёт за собой применение кода Стина к набору физических кубитов, а затем его повторное применение к исправленным кубитам, используя выходные данные первого уровня исправлений в качестве лучших кубитов, которые будут использоваться на последующем уровне. Несколько уровней могут быть объединены друг с другом до тех пор, пока не будет достигнута

[14] Для кода расстояния 3 требуется более 3 кубитов, поскольку измерения синдрома не могут раскрыть никакой информации о фактическом квантовом состоянии.

желаемая степень защиты от ошибок. В общем, объединение QECC, которое кодирует k кубитов в n физических кубитов и имеет расстояние d, записанное как $[[n, k, d]]$, масштабируется до кода $[[nr, k, d^*]]$ для r уровней объединения, где $d^* \geq d^r$. Т. е. требуется n^r физических кубитов на логический кубит. Например, три уровня конкатенации кода Стина потребуют 343 физических кубита для кодирования одного логического кубита и достижения расстояния не менее 27. Здесь затраты на кубит будут меньше, чем во многих других подходах QEC. Однако для кода Стина требуется частота ошибок ниже 10^{-5}, что намного ниже, чем у современных машин. Другие коды конкатенации имеют более высокие накладные расходы кубитов, но могут выдерживать более высокий уровень ошибок. Поиск лучших кодов является активной областью исследований.

Другой подход к QECC, так называемый поверхностный код, менее чувствителен к частоте ошибок физического кубита и может защитить от ошибок даже при частоте ошибок квантового устройства до 10^{-2} (1 %), что означает, что он исправляет больше ошибок, чем добавляет, если все вентили и измерения дают сбой в среднем не более 1 на 100 раз. Порог ошибки поверхностного кода в один процент применяется к архитектуре устройства, в которой каждый физический кубит взаимодействует только со своими четырьмя ближайшими соседними кубитами, что распространено в некоторых современных конструкциях квантовых компьютеров.

Однако высокий порог ошибки достигается за счёт больших накладных расходов. Поверхностный код на расстоянии d требует решётки из $(2d - 1) \times (2d - 1)$ физических кубитов для кодирования одного логического кубита. Как видно из формулы, поверхностный код с расстоянием в три — наименьший возможный код — требует 25 физических кубитов для кодирования логического кубита[15]. Хотя код с расстоянием три не будет полностью исправлять все ошибки, поскольку две ошибки генерируют неверный вывод, этот код снижает эффективную частоту ошибок. По мере увеличения размера квантового компьютера и снижения частоты ошибок эти меньшие коды можно использовать для повышения эффективной частоты ошибок машины, но со значительным уменьшением количества эффективных кубитов.

Конечно, чтобы полностью удалить ошибки, большинство квантовых алгоритмов достаточно громоздки, чтобы требовать расстояния больше трех. Например, для отказоустойчивого выполнения алгоритма Шора или гамильтоновой симуляции в

[15] Существуют некоторые улучшения стоимости поверхностного кодирования, однако минимально можно использовать код с расстоянием в 3 на 13 или 17 кубитах.

квантовой химии требуемое расстояние около 35, а это означает, что для кодирования логического кубита требуется примерно 15 000 физических кубитов, при начальной частоте ошибок в 10^{-3} [70, 93]. Помимо кодов Стина и поверхностного, были разработаны другие, более ресурсо-эффективные QECC; однако на данный момент в таких кодах либо отсутствуют эффективные алгоритмы декодирования, либо требуется слишком низкая частота ошибок для эпохи NISQ. Работа в этой области необходима для достижения цели создания квантового компьютера с полной исправлением ошибок.

В дополнение к накладным расходам физических кубитов QEC, чтобы работать с отказоустойчивыми логическими кубитами, во время компиляции должно быть доступно программное обеспечение для преобразования желаемых вентилей логических кубитов в вентили реальных физических кубитов, которые их кодируют. Этот перевод будет происходить непосредственно при компиляции квантового алгоритма, при этом каждый логический кубит и каждая логическая операция заменяются в соответствии с QECC и правилом отказоустойчивой замены, зависящим от расстояния. Правило замены учитывает реализацию как логического вентиля, так и алгоритма исправления ошибок, включая измерения синдрома и соответствующий классический алгоритм декодирования. Количество вентилей и временных шагов, необходимых для реализации каждого логического вентиля, зависит от логического вентиля и алгоритма QEC; подробности таких вычислений можно найти в [92-95].

Таким образом алгоритмы квантовой коррекции ошибок (QEC) позволят эмулировать идеальный квантовый компьютер с использованием шумных физических кубитов для развёртывания практических алгоритмов. Однако QEC несёт значительные накладные расходы с точки зрения как количества физических кубитов, необходимых для эмуляции логического кубита, так и количества операций с примитивными кубитами, необходимых для эмуляции логической квантовой операции.

Возможно, самой сложной и дорогостоящей задачей квантовой коррекции ошибок является создание отказоустойчивого «универсального» набора операций. Существующие схемы QEC разработали очень экономичные правила замены и другие методы для достижения отказоустойчивых операций логических вентилей в так называемой группе Клиффорда (состоящей из операций Паули, управляемого НЕ [CNOT], Адамара [H], фазового вентиля S и их производных), а также измерение в расчётной основе. Однако универсальное решение также требует отказоустойчивой реализации

вентилей, отличных от группы Клиффорда (таких как вентиль Тоффоли или вентиль $\pi/8$, также известный как T). Для этого можно использовать различные техники. Например, дистилляция магического состояния позволяет улучшить частоту ошибок логического вентиля, отличного от группы Клиффорда, такой как логический T-образный вентиль. Другой недавно разработанный метод, «переключение кода», переключается между кодом, который эффективен для вентилей Клиффорда, и кодом, оптимизированным для вентилей не-Клиффорда для достижения универсальности. Оба подхода сопряжены с накладными расходами в виде дополнительных физических кубитов, квантовых вентилей и классической сложности декодирования. Существенные накладные расходы, связанные с переходом от отказоустойчивых вентилей Клиффорда к универсальному набору отказоустойчивых вентилей, стали основной движущей силой исследований кодов квантовой коррекции ошибок и схем отказоустойчивости.

В случае дистилляции в магическом состоянии было разработано несколько методов для снижения накладных расходов [96-99]. В своей простейшей форме, хотя и не оптимальной с точки зрения накладных расходов на ресурсы, дистилляция магического состояния для T-вентиля может преобразовать физический T-вентиль в логический T-вентиль с частотой ошибок примерно $35p^3$. Если эта частота все ещё слишком велика для реализации интересующего алгоритма, то процедуру можно повторить, достигнув $35(35p^3)^3$, и так далее для r раундов, в результате чего получится $35^r p^{3r}$. В свою очередь, каждый раунд требует 15 кубитов для выполнения одного улучшенного T-вентиля; таким образом, для r раундов требуется 15^r кубитов (могут использоваться физические или логические кубиты, в зависимости от желаемой частоты ошибок вывода на T-вентиле). Таким образом, в то время как протокол QEC является дорогостоящим для операций Клиффорда и кодирования логических кубитов, наиболее дорогостоящей процедурой на сегодняшний день является отказоустойчивая реализация не-Клиффордского вентиля, необходимая для достижения универсальности [70]. Чтобы передать смысл требований к вентилям Клиффорда и не-Клиффорда, в Таблице 3.1 приведены оценки требований для проведения квантового моделирования молекулярной системы FeMoco с коррекцией ошибок. Эти данные справедливы на 2017 год. Прогресс в области квантовой химии и алгоритмах моделирования продолжается, и эти цифры, вероятно, будут улучшаться.

Таблица 3.1 Оценка потребности в ресурсах для моделирования химической структуры на основе последовательного алгоритмического подхода гамильтонового моделирования и поверхностного QEC.

Частота ошибок физического кубита	10^{-3}	10^{-6}	10^{-9}
Физических кубитов на 1 логический	15313	1103	313
Всего физических кубитов в КК	$1{,}7 \times 10^{6}$	$1{,}1 \times 10^{5}$	$3{,}5 \times 10^{4}$
Количество фабрик Т-состояния	202	68	38
Число физических кубитов на фабрику	$8{,}7 \times 10^{5}$	$1{,}7 \times 10^{4}$	$5{,}0 \times 10^{3}$
Общее количество физических кубитов, включая фабрики Т-состояния	$1{,}8 \times 10^{8}$	$1{,}3 \times 10^{6}$	$2{,}3 \times 10^{5}$

Примечание. В таблице 3.1. показаны компромиссы между количеством и качеством физических кубитов, необходимых для обеспечения отказоустойчивой реализации алгоритма, для трех конкретных коэффициентов ошибок физических кубитов. Оценки основаны на требовании 111 логических кубитов для экземпляра алгоритма и частоте физических вентилей 100 МГц. Обратите внимание, что требования для дистилляции (Т-фабрики) намного выше, чем для остальных кубитов исправлений ошибок. Стоимость создания безошибочного вентиля не из группы Клиффорда на порядки выше, чем кодирование кубитов операциями Клиффорда с помощью этого конкретного QECC (поверхностный код и дистилляция магического состояния) [70].

Таким образом можно утверждать, что производительность квантового алгоритма с исправлением ошибок будет ограничена количеством операций, которые являются наиболее затратными для исправления ошибок, необходимых для его реализации — например, в случае поверхностного кода QECC, «группы, не принадлежащей Клиффорду». операции требуют многих операций с примитивными вентилями для исправления ошибок и доминируют над общим временем (количеством операций), которое требуется алгоритму.

При этом продолжается разработка новых QEC и новых схем квантовой отказоустойчивости с целью значительного снижения накладных расходов, необходимых для достижения отказоустойчивых квантовых вычислений. Большая часть этой работы была сосредоточена на изучении поверхностных кодов и их вариантов, класса кодов, называемых топологическими кодами[16] [100]. Из-за

[16] Топологические коды относительно хорошо справляются с точки зрения помехоустойчивости и кубитных накладных расходов, и их преимущество заключается в том, что они являются естественно геометрически локальными в двух измерениях, что

многочисленных нерешённых вопросов о поверхностных кодах исследователи продолжают искать лучшие способы использования этих кодов [101-105] и лучшие способы оценки и декодирования этих кодов [106-107]. Когда экспериментальные системы достигают размера, при котором можно проводить интересные эксперименты по отказоустойчивости, и эти машины могут чередовать квантовые операции и измерения, схемы QEC могут быть протестированы для проверки теории и анализа. Настоящая польза от этих экспериментов будет заключаться в том, что исследователи, работающие над QEC, увидят эффекты и источники «реальных» системных ошибок, а не будут использовать теоретические модели шума. Информация о фактических ошибках может позволить разработать более эффективные коды QEC, адаптированные к статистике ошибок реальной машины. Опять же, минимизация накладных расходов имеет решающее значение для развёртывания схем отказоустойчивости, особенно на ранних квантовых устройствах, которые будут иметь ограниченное количество высококачественных кубитов.

Ранняя демонстрация ограниченной работы QEC на устройствах датируется 2005 годом, и основные функции таких протоколов были реализованы как на устройствах со сверхпроводящими кубитами, так и на кубитах с захваченными ионами. Такие эксперименты ещё не привели к созданию отказоустойчивых логических кубитов, учитывая, как правило, низкую точность логических операций физических операций с кубитами [108-110]. Недавно квантовые коды обнаружения ошибок — ранние предшественники QEC — были реализованы в доступных квантовых процессорах с некоторым успехом [111, 112].

3.3 Алгоритмы квантового приближения

Учитывая, что высокая стоимость исправления ошибок не позволяет использовать его в первых квантовых компьютерах, исследователи искали другие подходы для реализации преимуществ первых квантовых компьютеров. Многообещающий метод состоит в том, чтобы отказаться от стремления получить точное решение вычислительной задачи и вместо этого использовать приближенный или эвристический подход к решению задачи. Этот подход породил ряд квантовых и гибридных квантово-классических алгоритмов для задач, которые варьируются от моделирования систем многих тел, таких как молекулы и материалы [113-121], до приложений оптимизации [122-124] и машинного обучения [125-127]. Цель этих методов —

делает их многообещающим классом кодов для физической реализации, хотя некоторые из важных вариантов естественным образом существуют в трех или более измерениях.

предоставить приблизительные, но полезные решения рассматриваемой задачи с меньшими требованиями к ресурсам, чем другие подходы.

3.3.1 Вариационные квантовые алгоритмы

Многие интересующие нас проблемы, в частности вопросы квантовой химии, могут быть сформулированы как так называемые проблемы собственных значений. Согласно вариационному принципу квантовой механики, вычисленная энергия основного (наименее энергетического) состояния квантово-химической системы уменьшается по мере улучшения приближений к решению, асимптотически приближаясь к истинному значению сверху. Этот принцип породил итерационные классические алгоритмы для решения подобных задач, в которых грубая догадка о решении является входом, а несколько улучшенная аппроксимация является выходом. Этот вывод затем используется в качестве предположения для следующей итерации, и с каждым циклом вывод становится все ближе и ближе к истинному решению, но никогда не выходит за пределы.

Этот подход может быть разделён между классическим и квантовым алгоритмом, при этом шаг оптимизации выполняется квантовым процессором, а затем считывается, а классический блок управления решает, выполнять ли ещё одну итерацию. Возможность разделить квантовую обработку на множество небольших независимых шагов — с когерентностью, требуемой только в ходе одного шага — делает эти подходы разумным способом снизить требования к точности кубитов и получить требуемый результат. По этой причине квантовые вариационные алгоритмы были предложены в качестве приложений для цифровых компьютеров NISQ. Стоит отметить, что, конечно, эти алгоритмы легко выполняются и с использованием квантовых компьютеров с полной исправлением ошибок.

Одним из конкретных примеров является вариационный квантовый собственный решатель (VQE) [113-121], в нём задача разбивается на сумму набора более мелких задач, каждая из которых может быть аппроксимирована независимо, при этом сумма всех выходных данных соответствует интересующему приближенному решению. Процесс повторяется до тех пор, пока не будет достигнут эвристический критерий остановки, обычно соответствующий достижению энергетического порога. Вычислительная мощность VQE зависит от используемой формы предполагаемого квантового состояния или анзаца[17]. Некоторые анзацы определяются

[17] Некое предположение о форме искомого ответа.

исключительно удобными формами схем, которые могут быть легко доступны аппаратному обеспечению, в то время как другие предназначены для захвата конкретных типов квантовых корреляций. Считается, что алгоритм VQE может конкурировать с классическим компьютером в аналогичной задаче аппроксимации волновой функции и свойств системы многих тел, когда количество кубитов в квантовом регистре и глубина используемой квантовой схемы генерируют состояния, которые невозможно подготовить на классическом компьютере. Конкретное количество вентилей и кубитов, где это происходит, сильно зависит от типа алгоритма, но очень грубая оценка для приложений квантового моделирования может состоять из сотен кубитов и десятков тысяч квантовых вентилей [128].

Родственным подходом является алгоритм квантовой приближенной оптимизации [122], алгоритм для подготовки вариационного приближения волновой функции, которая удовлетворяет задаче оптимизации, такой как проблема выполнимости. Алгоритм следует той же процедуре, что и алгоритм VQE, а именно, серии экспериментов по подготовке и измерению с последующей оптимизацией с помощью классического компьютера. Результирующее квантовое состояние при выборке обеспечивает приближенное или точное решение вычислительной задачи.

3.3.2 Аналоговые квантовые алгоритмы

В дополнение к алгоритмам, для которых требуется квантовый компьютер на основе вентилей, существует набор подходов, которые работают путём прямого представления задачи в терминах гамильтониана, который может меняться или не меняться со временем. Желаемый результат кодируется в состоянии системы в конце запуска моделирования. «Прямое квантовое моделирование», в котором созданный гамильтониан аналогичен гамильтониану исследуемой квантовой системы, является одним из примеров такого подхода и типа аналоговых квантовых вычислений. Примеры прямого квантового моделирования включают реализацию спиновых гамильтонианов [129] или изучение квантовых фазовых переходов [130-132].

Квантовый отжиг и, в частности, адиабатическая квантовая оптимизация также используют этот «аналоговый» подход и предоставляют схему общего назначения для разработки квантовых алгоритмов, не требуя уровня абстракции логических операций или вентилей. Эти два подхода тесно связаны: адиабатическая квантовая оптимизация — это просто квантовый отжиг при нулевой температуре. Адиабатические квантовые вычисления интересны тем, что в принципе

можно преобразовать любые квантовые вычисления на основе вентилей в эквивалентные адиабатические квантовые вычисления (хотя это может быть неэффективный метод решения) [133]. Эти методы требуют преобразования интересующей задачи оптимизации в гамильтониан H_f таким образом, чтобы нахождение наименьшей энергии или основного состояния системы, определяемой этим гамильтонианом, было эквивалентно решению проблемы.

Алгоритм квантовой адиабатической оптимизации реализуется следующим образом: набор кубитов начинается с гамильтониана H_i, для которого известно основное состояние, а затем H_i медленно преобразуется в H_f. Поскольку квантовая система останется в своём основном состоянии, если гамильтониан изменяется достаточно медленно (адиабатически), эта процедура перетаскивает систему из основного состояния H_i в основное состояние H_f. Измерение конечного состояния даёт искомый ответ с высокой вероятностью [134, 135].

Перспективы таких алгоритмов вызвали большой интерес после работы Farhi et al. [136], что свидетельствует о том, что эти алгоритмы могут быть быстрыми на случайных экземплярах 3SAT, проблемы логической выполнимости, которая эквивалентна многим другим сложным задачам. Теоретический анализ этого алгоритма был довольно сложным, поскольку время его работы определялось спектральной щелью (разницей в энергии состояний вблизи основного состояния) гамильтониана, развивающегося во времени. В серии статей анализировался этот разрыв в ряде случаев, устанавливая, что существуют классы формул 3SAT и других NP-полных задач, для которых спектральный разрыв для адиабатического алгоритма экспоненциально мал, что означает, что для этих задач данный подход потребует экспоненциального времени в зависимости от размерности задачи [137, 138]. В результате формальная мощность такого типа вычислений до сих пор неизвестна. Таким образом, подход к установлению ускорения алгоритмов квантового отжига в значительной степени является эмпирическим; исследователи буквально сравнивают время, необходимое для выполнения данной задачи на квантовом отжиге, с лучшим временем оптимальных классических компьютерных систем для получения того же результата.

Все реальные квантовые компьютеры работают при конечной температуре. Когда эта температура соответствует энергии, превышающей спектральную щель, аналоговый квантовый компьютер может реализовать только квантовый отжиг, а не квантовые адиабатические вычисления. Квантовый отжиг особенно привлекателен с точки зрения экспериментальной реализации, с той

оговоркой, что теоретический анализ этих алгоритмов сложен, и для этой модели нет чёткой теории отказоустойчивости. Устройства адиабатической оптимизации, в частности машины компании D-Wave, преодолели серьёзные инженерные трудности и быстро масштабировались до тысяч кубитов, хотя и с некоторыми компромиссами в точности кубитов. Хотя изначально казалось, что эти устройства продемонстрировали многообещающее ускорение для некоторых приложений, дальнейшая работа над новыми классическими алгоритмами для этих конкретных задач стёрла эти ускорения [139-149]. Недавняя работа предполагает, что это отражает относительно высокую температуру, при которой работают процессоры D-Wave [150], и наличие определенных аналоговых ошибок в этих устройствах [151], хотя это не исключает возможности наличия других принципиальных ограничений. квантовых отжигов.

3.4 Применение квантового компьютера

Как видно из предыдущих обсуждений, было разработано множество квантовых алгоритмов как для квантовых компьютеров на основе вентилей, так и для квантовых отжигов. Полный онлайн-каталог квантовых алгоритмов поддерживается Национальным институтом стандартов и технологий США (NIST) [152]. Хотя эта коллекция включает в себя множество алгоритмов, которые теоретически предлагают квантовое ускорение, это ускорение часто является результатом нескольких основных методов по своей сути, в частности, квантового преобразования Фурье, квантовых случайных блужданий и гамильтонового моделирования. Кроме того, для большинства алгоритмов требуется большое количество высококачественных кубитов, скорее всего, требующих квантовой коррекции ошибок. Это далеко за пределами доступности квантовых ресурсов, в известных прототипах устройств. Кроме того, текущая неспособность эффективно загружать большие объёмы входных данных предполагает, что многие из них будет сложно реализовать на практике.

Более того, алгоритмы, как правило, сами по себе не являются приложениями; скорее, они являются строительными блоками, которые необходимо комбинировать для выполнения полезной задачи. Поскольку экспериментальные усилия по реализации квантовых компьютеров набирают обороты, ближайшая задача состоит в том, чтобы идентифицировать или создать квантовые приложения и требуемые для них алгоритмы — предпочтительно практические, которые будут обеспечивать значительное ускорение по сравнению с

классическими подходами, и которые можно развернуть на устройствах без исправления ошибок.

3.4.1 Ближайшие приложения квантового компьютера

Потенциальная краткосрочная полезность квантового компьютера в настоящее время является активной областью исследований. Ожидается, что такие приложения, вероятно, будут теми, которые требуют небольшого количества кубитов, могут быть реализованы с помощью относительно неглубокого кода (то есть требуют относительно коротких последовательностей вентилей) и могут работать на компьютерах NISQ. Приближенные алгоритмы, рассмотренные в разделе 3.3, рассматриваются как наиболее перспективные для реализации на ближайших аналоговых или цифровых машинах NISQ. Несмотря на то, что существует много потенциальных коммерческих[18] приложений для этого класса машин, на данный момент (2022 г.), ни один из них не даёт никаких преимуществ по сравнению с классическими подходами при работе на компьютере NISQ. Все исследователи, в том числе представители стартапов, согласились, что это критически важная область для исследований.

Сделаем вывод: пока не существует общеизвестного приложения, представляющего коммерческий интерес, основанного на квантовых алгоритмах, которое можно было бы запустить на ближайшем аналоговом или цифровом компьютере NISQ, что дало бы преимущество перед классическими подходами.

3.4.2 Квантовое превосходство

Необходимой вехой на пути к полезным квантовым компьютерам является квантовое превосходство — демонстрация любых квантовых вычислений, которые непомерно сложны для классических компьютеров, независимо от того, полезны они или нет. По сути, квантовое превосходство — это экспериментальная демонстрация того, что квантовые компьютеры нарушают расширенный тезис Чёрча-Тьюринга. Квантовое превосходство также устранит скептицизм в отношении жизнеспособности квантовых компьютеров, а также обеспечит проверку квантовой теории в области высокой сложности. Чтобы достичь этого, нужно было бы создать квантовый компьютер, достаточно большой, чтобы продемонстрировать превосходство, и найти простую задачу, которую он может решить, но которую трудно

[18] Коммерческим приложением называется приложение, за которое кто-то готов платить деньги за ответ, который оно может дать. Это приложение, которое принесёт доход квантовым вычислениям.

решить классической машине. Распространённым типом таких задач являются те, в которых над кубитами выполняются операции для создания запутанного квантового состояния, а затем выборки этого состояния для оценки его вероятностного распределения [153].

Первое предложение хорошей тестовой задачи принадлежит Аароносну и Архипову в 2010 г. в их предложении выборки бозонов [154], основанном на более ранней работе по классической сложности задач выборки[19] [155, 156]. Им удалось доказать, что вычисление выходных вероятностей случайной системы невзаимодействующих бозонов относится к классу сложности (P-трудных), соответствующему вычислениям, которые считались сложными для выполнения на классических компьютерах. Более того, при правдоподобном предположении, что эти задачи остаются P-трудными для аппроксимации, следует, что классические компьютеры не могут даже отбирать случайные выходные данные типичной линейно-оптической сети. Для квантового компьютера предоставление такой выборки (называемой «выборкой кубитов») может означать демонстрацию квантового превосходства. Хотя выборка бозонов пользуется популярностью среди экспериментаторов, а в ряде лабораторий уже достигнуты мелкомасштабные реализации, включая эксперимент с 6 фотонами [157], по-прежнему сложно довести эти эксперименты примерно до 50 фотонов, необходимых для установления частичного квантового превосходства [158].

Другой подход для демонстрации квантового превосходства в сверхпроводящих кубитах был предложен теоретической группой Google в 2016 году [159]. Он был вдохновлён экспериментально, и квантовое превосходство сыграло роль этапа на пути к созданию сверхпроводящих компьютеров NISQ. Конкретное предложение — Random Circuit Sampling (RCS) — призывало к реализации случайной квантовой схемы и измерению выходных данных схемы. Они предположили, что выборка из выходного распределения таких случайных схем представляет собой сложную задачу для классических вычислений. Недавно Bouland et al. предоставил убедительные теоретико-сложные доказательства классической жёсткости RCS наравне с выборкой бозонов. [160].

Предложение о квантовом превосходстве состоит из двух основных частей: во-первых, это определение вычислительной задачи, которая может быть экспериментально реализована в ближайшем будущем, но которая непомерно сложна для любого алгоритма,

[19] Термин «квантовое превосходство» ввёл Джон Прескилл в 2012 году, хотя работы в этой области начались ещё раньше.

работающего на классическом компьютере. Второй — эффективный метод проверки того, что квантовое устройство действительно выполнило вычислительную задачу. Это особенно сложно, поскольку предлагаемые алгоритмы вычисляют выборки из определенного распределения вероятностей (а именно, выходного распределения выбранной квантовой схемы). Первое упрощение, позволяющее обойти эту проверку, состоит в том, чтобы выбрать n, число кубитов, достаточно малым ($n \approx 50$), чтобы классический суперкомпьютер действительно мог вычислить выходное распределение выбранной квантовой схемы. Это по-прежнему оставляет проблему проверки того, что выходы квантового устройства действительно взяты из этого (или ближайшего) распределения. Это тоже может быть трудно доказать.

Для достижения данной цели модель превосходства RCS [159] предлагает вычисление оценки в виде кросс-энтропии между распределением, выбранным из устройства, и истинным выходным распределением выбранной квантовой схемы. Оказывается, показатель перекрёстной энтропии подтверждает, что два распределения близки, при условии, что выполняется простое условие, а именно, что энтропия распределения, взятого из устройства, по крайней мере так же велика, как энтропия истинного выходного распределения выбранная квантовая схема. [160]. К сожалению, невозможно проверить это условие энтропии, используя любое разумное количество выборок, хотя оно справедливо для многих моделей с шумом, таких как локальный деполяризующий шум. В другом предложении для проверки используется концепция генерации тяжёлых выходных данных (или HOG) [161], и можно доказать, что она проверяет превосходство при (нестандартном) предположении сложности. Наконец, третье предложение по проверке – генерация бинарных выходных данных (BOG), одновременно проверяет HOG и кросс-энтропию и является теоретически оптимальной информацией в некоторой формальной модели [160].

Проверка концепции этого алгоритма квантового превосходства была проведена в 2017 году на 9-кубитном устройстве [161]. Было показано, что частота ошибок пропорциональна количеству операций, умноженному на количество кубитов, при этом средняя ошибка на 2-кубитный вентиль составляет около 0,3 %. Простая экстраполяция на кубитное устройство с примерно 50 кубитами показывает, что результат квантового превосходства должен быть возможен с этой архитектурой, и команда аппаратного обеспечения Google (и другие) усердно работают для достижения этой цели.

Рассмотренные подходы оставляют без ответа два вопроса. Во-первых, как выполнить проверку без предположения об энтропии (или предположения о нестандартной сложности). Во-вторых – возможность установления квантового превосходства за пределами вычислительной мощности классических суперкомпьютеров, как это понимается в настоящее время[20], чтобы соответствовать порядка примерно 50 кубитам. Недавнее предложение показывает, как доказуемо реализовать квантовое превосходство на основе постквантовой криптографии. В частности, исходя из сложности проблемы обучения с ошибками, предлагается способ доказуемой проверки квантового превосходства для квантовых компьютеров с произвольно большим числом кубитов [162, 163].

Стоит заметить, что хотя несколько команд работали над демонстрацией квантового превосходства, этот этап ещё не завершён и квантовое превосходство пока не достигнуто. Такое достижение будет трудно установить окончательно, кроме того, эта цель будет отдаляться по мере улучшения классических подходов к решению выбранной контрольной задачи.

Таким образом, стремление к квантовому превосходству уже достигло интересной цели: разработка теоретических инструментов, полезных для строгого анализа вычислительной сложности определенных квантовых задач, которые вскоре могут быть реализованы экспериментально. Однако из-за неопределённого характера результатов трудности (т. е. из-за зависимости от нестандартных предположений трудности) и из-за ограничительного характера моделей шума, учитываемых этими результатами, предстоит ещё много работы.

3.4.3 Приложения для идеального квантового компьютера

В случае разработки надёжного крупномасштабного квантового компьютера с исправлением ошибок существующие алгоритмы с известным ускорением, вероятно, будут полезны для решения любого количества практических задач или частей задач. Возможно, наиболее понятным применением квантовых алгоритмов является область

[20] Хотя точное число зависит от спецификаций и приближений конкретной симуляции, это число будет увеличиваться по мере совершенствования классических методов. Ожидается, что данный порядок будет оставаться на текущем уровне в течение долгового времени. Недавно исследователи использовали новый классический подход для выполнения единственного экземпляра задачи квантового превосходства, которая была бы достижима с помощью квантового устройства на 70 кубитов. не соответствует полному эксперименту квантового превосходства со 100 000 экземпляров, предложенному для устройства с 50 кубитами, который ещё не доказал свою достижимость на классическом компьютере.

криптографии (в частности, её преодоление), приложение, основанное непосредственно на математике; эти приложения будут обсуждаться в следующей главе. Квантовое моделирование, как для фундаментальной, так и для прикладной науки, также часто упоминается как потенциальное «приложение-убийца», особенно в области квантовой химии [164].

Проблема электронной структуры привлекла большое внимание из-за того, что она занимает центральное место в областях химии и материаловедения. Эта проблема требует решения для энергий основного состояния и волновых функций электронов, взаимодействующих в присутствии некоторого внешнего поля, обычно возникающего от атомных ядер. Электронная структура определяет химические свойства, скорость и продукты химических реакций. Хотя классические вычислительные подходы к этой проблеме (такие как теория функционала плотности) весьма эффективны во многих контекстах (например, для предсказания молекулярной геометрии), они часто не достигают уровня точности, необходимого для предсказания скоростей химических реакций или различения конкурирующих фаз коррелированных взаимодействий исследуемых веществ. Это особенно верно, когда в систему входят элементы переходных металлов (которые присутствуют в большинстве катализаторов). Квантовые компьютеры могли бы обеспечить эффективное решение этой проблемы в классически неразрешимом режиме. Фактически, один ранний квантовый алгоритм предлагает экспоненциальное ускорение по сравнению с классическими подходами к вычислению констант скорости химических реакций [165]. Этот и другие алгоритмы могут открыть двери для важных открытий о химических реакциях и фазах материи, которые долгое время ускользали от описания систематической и предсказательной теорией. Такие результаты также могут иметь коммерческое применение в таких областях, как хранение энергии, разработка дисплеев для устройств, создание новых промышленных катализаторов и фармацевтических препаратов.

ЗАКЛЮЧЕНИЕ

В то время как квантовая химия, оптимизация (включая машинное обучение) и преодоление криптографии являются наиболее изученными потенциальными приложениями идеального квантового компьютера, эта область все ещё находится на ранней стадии — с точки зрения как алгоритмов, как обсуждалось в этой главе, так и устройств. Существующие алгоритмы могут быть изменены или реализованы способами, которые ещё не предполагались; новые алгоритмы, скорее всего, появятся по мере продолжения исследований. В результате, за исключением криптографии, невозможно предсказать влияние квантовых компьютеров на различные коммерческие сектора — эта область настолько молода, что эти изменения даже не предвидятся. Что касается криптографии, то потенциал будущего квантового компьютера, работающего на алгоритме Шора, достаточен, чтобы повлиять на действия сегодня. Проблемы такого рода на данный момент активно исследуются. Однако даже большой квантовый компьютер с исправлением ошибок в целом не превосходит классический компьютер. На самом деле квантовые компьютеры не ускоряют многие классы задач, а зрелость классической вычислительной экосистемы (включая аппаратное обеспечение, программное обеспечение и алгоритмы) означает, что для этих классов задач классические вычисления останутся доминирующей вычислительной платформой. Даже приложения, ускоренные квантовым компьютером или ускоренные части данных приложений, вероятно, будут составлять лишь небольшой объём рассматриваемой более широкой задачи. Таким образом, в обозримом будущем квантовый процессор, вероятно, будет полезен для выполнения только определенных частей определенных задач, а остальные операции будут более эффективно выполняться на классическом компьютере. Таким образом, ожидается, что квантовый компьютер будет служить сопроцессором, а не заменой классическому компьютеру. Кроме того, физическая реализация любых квантовых вычислений потребует выполнения множества сложных операций управления кубитами, поддерживаемыми в контролируемой среде, что потребует использования классических компьютеров.

Следовательно квантовые компьютеры вряд ли будут полезны в качестве прямой замены обычных компьютеров или для всех приложений; скорее, в настоящее время ожидается, что они будут устройствами специального назначения, работающими в дополнение к обычным процессорам, аналогично сопроцессору или ускорителю.

СПИСОК ЛИТЕРАТУРЫ

[1] *Dongarra J.* The U. S. Once Again Has the World's Fastest Supercomputer. Keep Up the Hustle [Электронный ресурс] // The Washington Post, 25.06.2018, URL: https://www.washingtonpost.com/opinions/united-states-wins-top-honors-in-supercomputer-race/2018/06/25/82798c2c-78b1-11e8-aeee-4d04c8ac6158_story.html.

[2] *Nicas J.* How Google's Quantum Computer Could Change the World [Электронный ресурс] // Wall Street Journal, 16.10.2017, URL: https://www.wsj.com/articles/how-googles-quantum-computer-could-change-the-world-1508158847.

[3] *Asmundsson J.* Quantum Computing Might Be Here Sooner than You Think [Электронный ресурс] // Bloomberg, 14.06.2017, URL: https:// www.bloomberg.com/news/features/2017-06-14/the-machine-of-tomorrow- today-quantum-computing-on-the-verge.

[4] *Castevecchi D.* Quantum computers ready to leap out of the lab in 2017 // Nature. 2017. V. 541(7635). pp. 9–10.

[5] *Feynman R.P.* Simulating physics with computers // International Journal of Theoretical Physics. 1982. V. 21. pp. 467–488.

[6] *Lloyd S.* Universal quantum simulators // Science, 1996. V. 273. Iss. 5278. pp. 1073–1078.

[7] *Bernstein E., Vazirani U.* Quantum Complexity Theory // 20 in Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing (STOC '93), Association of Computing Machinery, New York, .1993. pp. 11. URL: https://dl.acm.org/citation.cfm?id=167097.

[8] *Kaye P., Laflamme R., Mosca M.* An Introduction to Quantum Computing. Oxford: Oxford University Press, 2007.

[9] *Nielsen M.A., Chuang I.* Quantum Computation and Quantum Information. Cambridge: Cambridge University Press, 2002.

[10] *Simon D.* On the power of quantum computation // SIAM Journal on Computing. 1997. V. 26. №5. pp. 1474–1483.

[11] Industry Statistics [Электронный ресурс] // Semiconductor Industry Association, 6 February 2018.
URL: http://www.semiconductors.org/index.php?src=directory&view= IndustryStatistics&srctype=billing_reports&submenu=Statistics.

[12] *Preskill J.* Quantum Computing in the NISQ Era and Beyond // Quantum. 2018. V. 2. №79.

[13] *Young K.C., Sarovar M., Blume-Kohout R.* Error suppression and error correction in adiabatic quantum computation: Techniques and challenges, // Physical Review X. 2013. V. 3. №041013.

[14] *Mizel A.* Fault-Tolerant, Universal Adiabatic Quantum Computation. [Электронный ресурс]. 2014. Препринт: arXiv:1403.7694.

[15] *Jordan S.P., Farhi E., Shor P.W.* Error-correcting codes for adiabatic quantum computation // Physical Review A. 2006. V. 74. №052322.

[16] *Pudenz K.L., Albash T., Lidar D.A.* Error-corrected quantum annealing with hundreds of qubits // Nature Communications. 2014. V. 5. №324.

[17] *Vinci W., Albash T., Lidar D.A.* Nested quantum annealing correction // Quantum Information. 2016. V. 2. №16017.

[18] *Bookatz A.D., Farhi E., Zhou L.* Error suppression in Hamiltonian-based quantum computation using energy penalties // Physical Review A. 2015. V. 92. №022317.

[19] *Marvian M., Lidar D.A.* Error suppression for Hamiltonian-based quantum computation using subsystem codes // Physical Review Letters. 2017. V. 118. №030504.

[20] *Landauer R.* Irreversibility and heat generation in the computing process // IBM Journal of Research and Development. 1961. V. 5. № 3. pp. 183–191.

[21] *Nielsen M., Chuang I.* Quantum Computation and Quantum Information // Cambridge: Cambridge University Press, 2016, 189 p.

[22] *Roetteler M., Svore K.M.* Quantum computing: Codebreaking and beyond // IEEE Security and Privacy. 2018. V. 16. № 5. pp. 22–36.

[23] *Wootters W.K., Zurek W.H.* A single quantum cannot be cloned // Nature. 1982. V. 299. Issue 5886. pp.802–803.

[24] *Dieks D.* Communication by EPR devices // Physics Letters A. 1982. V. 92. №6. pp. 271–272.

[25] *Harty T.P., Allcock D.T.C., Ballance C.J., Guidoni L., Janacek H.A., Linke N.M., Stacey D.N., Lucas D.M.* High-fidelity preparation, gates, memory, and readout of a trapped-ion quantum bit // Physical Review Letters. 2014. V. 113. № 220501.

[26] *Blume-Kohout R., Gamble J.K., Nielsen E., Rudinger K., Mizrahi J., Fortier K., Maunz P.* Demonstration of qubit operations below a rigorous fault tolerance threshold with gate set tomography // Nature Communications. 2017. V. 8. №4485.

[27] *Mount E., Kabytayev C., Crain S., Harper R., Baek S.-Y., Vrijsen G., Flammia S.T., Brown K.R., Maunz P., Kim J.* Error compensation of single-qubit gates in a surface-electrode ion trap using composite pulses // Physical Review A. 2015. V.92. №060301.

[28] *Gustavsson S., Zwier O., Bylander J., Yan F., Yoshihara F., Nakamura Y., Orlando T.P., Oliver W.D.* Improving quantum gate fidelities

by using a qubit to measure microwave pulse distortions // Physical Review Letters. 2013. V. 110. №0405012.

[29] *Gaebler J.P., Tan T.R., Lin Y., Wan Y., Bowler R., Keith A.C., Glancy S., Coakley K., Knill E., Leibfried D., Wineland D.J.* High-fidelity universal gate set for 9Be+ ion qubits // Physical Review Letters. 2016. V. 117. №060505.

[30] *Ballance C.J., Harty T.P., Linke N.M., Sepiol M.A., Lucas D.M.* High-fidelity quantum logic gates using trapped-ion hyperfine qubits // Physical Review Letters. 2016. V. 117. №060504.

[31] *Barends R., Kelly J., Megrant A., Veitia A., Sank D., Jeffrey E., White T.C., et al.* Logic gates at the surface code threshold: Supercomputing qubits poised for fault-tolerant quantum computing // Nature. 2014. V. 508. pp. 500–503.

[32] *Sheldon S., Magesan E., Chow J., Gambetta J.M.* Procedures for systematically turning up cross-talk in the cross-resonance gate // Physical Review A. 2016. V. 93. №060302.

[33] *Kitaev A.Y., Shen A.H., Vyalyi M.N.*, Classical and Quantum Computation // American Mathematical Monthly. 2011. v. 47. pp. 257–278.

[34] *DiVincenzo D.P.* The physical implementation of quantum computation // Fortschritte der Physik. 2000. V. 48. pp. 771–783.

[35] *Amin M.H.S., Averin D.V., Nesteroff J.A.* Decoherence in adiabatic quantum computation // Physical Review A. 2009. V. 79. Iss. 2. №022107.

[36] *Childs A.M., Farhi E., Preskill J.* Robustness of adiabatic quantum computation // Physical Review A. 2001. V. 65. Iss. 1. №012322.

[37] *Amin M.H.S., Love P.J., Truncik C.J.S.* Thermally assisted adiabatic quantum computation // Physical Review Letters. 2008. V. 100. Iss. 6. №060503.

[38] *Dickson N.G., Johnson M.W., Amin M.H.S., Harris R., Altomare F., Berkley A.J., Bunyk P., et al.* Thermally assisted quantum annealing of a 16-qubit problem // Nature Communications. 2013. V. 4. №1903.

[39] Quantum Computing: Progress and Prospects. [Электронный ресурс]. – The National Academies Press, Washington, DC. DOI: https:// doi.org/10.17226/25196.

[40] *Горшков В.В., Ниязова Б.Н., Мокряков А.В., Лежинский М.В.* Квантовый компьютер. Патент на полезную модель 208668 U1, 29.12.2021. Заявка № 2021120477 от 12.07.2021.

[41] *Моисеев С.А., Герасимов К.И., Миннегалиев М.М., Урманчеев Р.В., Желтиков А.М., Федотов А.Б.* Способ подавления квантовых шумов в оптической квантовой памяти на основе протокола восстановления подавленного фотонного эха в резонаторе (варианты).

Патент на изобретение 2766051 C1, 07.02.2022. Заявка № 2020143728 от 29.12.2020.

[42] *Фастовец Д.В.* QRVE - модульное программное обеспечение для характеризации квантовых вычислительных устройств. Свидетельство о регистрации программы для ЭВМ 2022611779, 01.02.2022. Заявка № 2022610940 от 26.01.2022.

[43] *Лежинский М.В., Мокряков А.В.* Алгоритмы шифрования, устойчивые ко взлому в условии квантового превосходства // Сборник научных трудов кафедры прикладной математики и программирования по итогам работы постоянно действующего семинара "Теория систем". М.: РГУ. 2021. С. 141–147.

[44] *Кирилюк М.А., Бочаров Н.А.* Разработка программной модели квантовых вычислений и моделирование работы квантовых алгоритмов на платформе "Эльбрус" // Вестник Концерна ВКО "Алмаз – Антей", 2022. № 1. С. 93–101.

[45] *Bernstein E., Vazirani U.* Quantum complexity theory // SIAM Journal on Computing. 1997. V. 26. №5. pp. 1411–1473.

[46] *Shor P.* Algorithms for Quantum Computation: Discrete Logarithms and Factoring // Proceedings 35th Annual Symposium on Foundations of Computer Science. 1994. pp. 124–134.

[47] *Anderson R.J., Wolf H.* Algorithms for the certified write-all problem // SIAM Journal on Computing. 1997. V. 26. №5. pp. 1277–1283.

[48] *Karp R.M.* On the computational complexity of combinatorial problems // Networks. 1975. V. 5. №1. pp. 45–68.

[49] *Bennett C.H., Bernstein E., Brassard G., Vazirani U.* Strengths and weaknesses of quantum computing // SIAM Journal on Computing. 1997. V. 26. №5. pp. 1510–1523.

[50] *Grover L.K.* A Fast Quantum Mechanical Algorithm for Database Search // Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing. 1996. pp. 212–219.

[51] *Cook S.* The P versus NP problem // The Millennium Prize Problems, Clay Mathematics Institute. American Mathematical Society, Providence, R.I. 2006. pp. 87–104.

[52] *Hales L., Hallgren S.* An Improved Quantum Fourier Transform Algorithm and Applications // Proceedings of 41st Annual Symposium on Foundations of Computer Science. 2000. pp. 515–525.

[53] *Jozsa R.* Quantum factoring, discrete logarithms, and the hidden subgroup problem // Computing in Science and Engineering. 2001. V. 3. №2. pp. 34–43.

[54] *Kitaev A.Y.* Quantum Measurements and the Abelian Stabilizer Problem // Electronic Colloquium on Computational Complexity. 1996. V. 13. №38.

[55] *Brassard G., Hoyer P., Mosca M., Tapp A.* Quantum amplitude amplification and estimation // Contemporary Mathematics. 2002. V. 305. pp. 53–74.

[56] *Farhi E., Goldstone J., Gutmann S.* A Quantum Algorithm for the Hamiltonian NAND Tree // Theory of Computing. 2007. V. 4. pp. 169–190.

[57] *Ambainis A., Childs A.M., Reichardt B.W., Špalek R., Zhang S.* Any AND-OR formula of size N can be evaluated in time N1/2+O(1) on a quantum computer // SIAM Journal on Computing. 2010. V. 39. №6. pp. 2513–2530.

[58] *Giovannetti V., Lloyd S., Maccone L.* Quantum random access memory // Physical Review Letters. 2008. V. 100. Iss. 16. №160501.

[59] *Abrams D.S., Lloyd S.* Simulation of many-body Fermi systems on a universal quantum computer // Physical Review Letters. 1997. V. 79. Iss. 13. №2586.

[60] *Aharonov D., Ta-Shma A.* Adiabatic Quantum State Generation and Statistical Zero Knowledge // Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing. 2003. pp. 20–29.

[61] *Berry D.W., Childs A.M., Cleve R., Kothari R., Somma R.D.* Simulating Hamiltonian dynamics with a truncated Taylor series // Physical Review Letters. 2015. V. 114. Iss. 9. pp. 090502.

[62] *Babbush R., Berry D.W., Kivlichan I.D., Scherer A., Wei A.Y., Love P.J., Aspuru-Guzik A.* Exponentially more precise quantum simulation of fermions in the configuration interaction representation // Quantum Science and Technology. 2017. V. 3. №015006.

[63] *Low G.H., Chuang I.L.* Hamiltonian Simulation by Qubitization // Quantum. 2019. V. 3. pp. 163–185.

[64] *Low G.H., Chuang I.L.* Optimal Hamiltonian simulation by quantum signal processing // Physical Review Letters. 2017. V. 118. Iss. 1. №010501.

[65] *Babbush R., Berry D.W., Kivlichan I.D., Wei A.Y., Love P.J., Aspuru-Guzik A.* Exponentially more precise quantum simulation of fermions I: Quantum chemistry in second quantization // New Journal of Physics. 2016. V. 18. №033032.

[66] *Berry D.W., Childs A.M., Kothari R.* Hamiltonian Simulation with Nearly Optimal Dependence on All Parameters // Proceedings of the 56th IEEE Symposium on Foundations of Computer Science. 2015. pp. 792-809.

[67] *McArdle S., Endo S., Aspuru-Guzik A., Benjamin S., Yuan X.* Quantum Computational Chemistry // Reviews of Modern Physics. 2020. V. 92. № 015003.

[68] *Wecker D., Hastings M.B., Wiebe N., Clark B.K., Nayak C., Troyer M.* Solving strongly correlated electron models on a quantum computer // Physical Review A. 2015. V. 92. Iss. 6. №062318.

[69] *Dykstra C., Frenking G., Kim K.S., Scuseria G.E.* Theory and Applications of Computational Chemistry: The First Forty Years. – Amsterdam: Elsevier, 2005.

[70] *Reiher M., Wiebe N., Svore K.M., Wecker D., Troyer M.* Elucidating reaction mechanisms on quantum computers // Proceedings of the National Academy of the Sciences of the U.S.A. 2017. V. 114. pp. 7555–7560.

[71] *Wendin G.* Quantum information processing with superconducting circuits: A review // Reports on Progress in Physics. 2017. V. 80. Iss. 10. №106001.

[72] *Bauer B., Wecker D., Millis A.J., Hastings M.B., Troyer M.* Hybrid quantum-classical approach to correlated materials // Physical Review X. 2016. V. 6. №031045.

[73] *Olson J., Cao Y., Romero J., Johnson P., Dallaire-Demers P.-L., Sawaya N., Narang P., Kivlichan I., Wasielewski M., Aspuru-Guzik A.* Quantum Information and Computation for Chemistry [Электронный ресурс]. 2017. Препринт: arXiv:1706.05413.

[74] *Babbush R., Berry D.W., Kivlichan I.D., Wei A.Y., Love P.J., Aspuru-Guzik A.* Exponentially more precise quantum simulation of fermions in the configuration interaction representation // Quantum Science and Technology V. 3. №015006.

[75] *Kivlichan I.D., J. McClean, N. Wiebe, C. Gidney, A. Aspuru-Guzik, Kin-Lic G. Chan, Babbush R.* Quantum simulation of electronic structure with linear depth and connectivity// Physical Review Letters. 2018. V. 120. №11501.

[76] *Babbush R., Gidney C., Berry D.W., Wiebe N., McClean J., Paler A., Fowler A., Neven H.* Encoding Electronic Spectra in Quantum Circuits with Linear T Complexity // Physical Review X. 2018. V. 8. № 041015.

[77] *Low G.H., Wiebe N.* Hamiltonian Simulation in the Interaction [Электронный ресурс]. 2018. Препринт: arXiv:1805.00675.

[78] *Berry D.W., Kieferová M., Scherer A., Sanders Y.R., Low G.H., Wiebe N., Gidney C., Babbush R.* Improved techniques for preparing eigenstates of fermionic Hamiltonians // Quantum Information. 2018. V. 4. Iss. 1. №22.

[79] *Poulin D., Hastings M.B., Wecker D., Wiebe N., Doherty A.C., Troyer M.* The Trotter step size required for accurate quantum simulation of quantum chemistry // Quantum Information & Computation. 2015 V. 15. Iss. 5-6. pp. 361–384.

[80] *Hastings M.B., Wecker D., Bauer B., Troyer M.* Improving Quantum Algorithms for Quantum Chemistry // Quantum Information & Computation 2015. V. 15. Iss. 1-2. pp. 1–21.

[81] *Poulin D., Kitaev A., Steiger D.S., Hastings M.B., Troyer M.* Quantum algorithm for spectral measurement with a lower gate count // Physical Review Letters. 2018. V. 121. Iss. 1. №010501.

[82] *Wecker D., Bauer B., Clark B.K., Hastings M.B., Troyer M.* Gate-count estimates for performing quantum chemistry on small quantum computers // Physical Review A. 2014. V. 90. Iss.2. №022305.

[83] *Harrow A.W., Hassidim A., Lloyd S.* Quantum algorithm for linear systems of equations // Physical Review Letters. 2009. V. 103. Iss. 15. №150502.

[84] *Childs A.M., Dam W.V.* Quantum algorithms for algebraic problems // Reviews of Modern Physics V. 82. Iss. 1. №1.

[85] *Berry D.W., Childs A.M., Ostrander A., Wang G.* Quantum algorithm for linear differential equations with exponentially improved dependence on precision // Communications in Mathematical Physics. V. 2017. V. 356. Iss. 3. pp. 1057–1081.

[86] *Brandao F.G.S.L., Svore K.* Quantum Speed-Ups for Semidefinite Programming // Proceedings of 58th Annual IEEE Symposium on Foundations of Computer Science. 2017. pp. 415–426.

[87] *Kerenidis I., Prakash A.* Quantum Recommendation Systems // Proceedings of 8th Innovations in Theoretical Computer Science Conference. 2017. pp. 49:1–49:21.

[88] *Tang E.* A Quantum-Inspired Classical Algorithm for Recommendation Systems // Electronic Colloquium on Computational Complexity. 2018. № 128.

[89] *Johnson P.D., Romero J., Olson J., Cao Y., Aspuru-Guzik A.* QVECTOR: An Algorithm for Device-Tailored Quantum Error Correction [Электронный ресурс]. 2017. Препринт: arXiv:1711.02249.

[90] *Kandala A., Temme K., Corcoles A.D., Mezzacapo A., Chow J.M., Gambetta J.M.* Extending the Computational Reach of a Noisy Superconducting Quantum Processor [Электронный ресурс]. 2018. Препринт: arXiv: 1805.04492.

[91] *Calderbank A.R., Shor P.W.* Good quantum error-correcting codes exist // Physical Review A. 1997. V. 54. pp. 1098–1106.

[92] *Aliferis P., Gottesman D., Preskill J.* Quantum accuracy threshold for concatenated distance-3 codes // Quantum Information and Computation. 2006. V. 6. pp. 97–165.

[93] *Fowler A.G., Mariantoni M., Martinis J.M., Cleland A.N.* Surface codes: Towards practical large-scale quantum computation // Physical Review A V. 86. №032324.

[94] *Tomita Y., Svore K.M.* Low-distance Surface Codes under Realistic Quantum Noise // Physical Review A. 2014. V. 90. №062320.

[95] *Svore K.M., DiVincenzo D.P., Terhal B.M.* Noise Threshold for a Fault-Tolerant Two-Dimensional Lattice Architecture // Quantum Information & Computation. 2007. V. 7. Iss. 4. pp. 297–318.

[96] *Hastings M.B., Haah J.* Distillation with Sublogarithmic Overhead // Physical Review Letters. 2006. V. 120, Iss. 5. №050504.

[97] *Haah J., Hastings M.B.* Codes and Protocols for Distilling T, controlled S, and Toffoli Gates // Quantum. 2017. V. 2. №71.

[98] *Haah J., Hastings M.B., Poulin D., Wecker D.* Magic State Distillation at Intermdediate Size [Электронный ресурс]. 2017. Препринт: arXiv: 1709.02789.

[99] *Haah J., Hastings M.B., Poulin D., Wecker D.* Magic State Distillation with Low Space Overhead and Optimal Asymptotic Input Count // Quantum. 2017. V. 1. №31.

[100] *Bombin H., Martin-Delgado M.A.* Topological quantum distillation // Physical Review Letters. 2006. V. 97. №180501.

[101] *Moussa J.E.* Transversal Clifford gates on folded surface codes // Physical Review A. 2016. V. 94. №042316.

[102] *Horsman C., Fowler A. G., Devitt S., Van Meter R.* Surface code quantum computing by lattice surgery // New Journal of Physics. 2012. V. 14. №123011.

[103] *Bravyi S.,* Cross A. Doubled Color Codes [Электронный ресурс]. 2015. Препринт: arXiv:1509.03239.

[104] *Bombin H.* Gauge color codes: Optimal transversal gates and gauge fixing in topological stabilizer codes // New Journal of Physics. 2015. V. 17. №083002.

[105] *Yoder T.J., Kim I.H.* The surface code with a twist // Quantum. 2017. V. 1. №2.

[106] *Bravyi S., Suchara M., Vargo A.* Efficient algorithms for maximum likelihood decoding in the surface code // Physical Review A. 2014. V. 90. №032326.

[107] *Duclos-Cianci G., Poulin D.* Fault-tolerant renormalization group decoder for abelian topological codes // Quantum Information and Computation. 2014. V. 14. pp. 721–740.

[108] *Chiaverini J., Leibfried Di., Schaetz T., Barrett M.D., Blakestad R.B., Britton J., Itano W.M., et al.* Realization of quantum error correction // Nature. 2004. V. 432 Iss. 7017. №602.

[109] *Nigg D., Mueller M., Martinez E.A., Schindler P., Hennrich M., Monz T., Martin-Delgado M.A., Blatt R.* Quantum computations on a topologically encoded qubit // Science. 2014. №1253742.

[110] *Rosenblum S., Reinhold P., Mirrahimi M., Jiang Liang, Frunzio L., Schoelkopf R.J.* Fault-Tolerant Measurement of a Quantum Error // Science. 2018. V. 361, Iss. 6399. pp. 266–270.

[111] *Linke N.M., Gutierrez M., Landsman K.A., Figgatt C., Debnath S., Brown K.R., Monroe C.* Fault-tolerant quantum error detection // Science Advances. 2017. V. 3. Iss. 10. №e1701074.

[112] *Harper R., Flammia S.* Fault Tolerance in the IBM Q Experience [Электронный ресурс]. 2018. Препринт: arXiv:1806.02359.

[113] *Peruzzo A., McClean J.R., Shadbolt P., Yung M.-H., Zhou X.-Q., Love P.J., Aspuru-Guzik A., O'Brien J.L.* A Variational Eigenvalue Solver on a Photonic Quantum Processor // Nature Communications. 2014. V. 5. №4213.

[114] *Wecker D., Hastings M.B., Troyer M.* Progress towards practical quantum variational algorithms// Physical Review A. 2015. V. 92. №042303.

[115] *McClean J.R., Romero J., Babbush R., Aspuru-Guzik A.* The theory of variational hybrid quantum-classical algorithms // New Journal of Physics V. 18. №023023.

[116] *O'Malley P.J.J., Babbush R., Kivlichan I.D., Romero J., McClean J.R., Barends R., Kelly J., et al.* Scalable quantum simulation of molecular energies // Physical Review X. 2016. V. 6. №031007.

[117] *Santagati R., Wang J., Gentile A.A., Paesani S., Wiebe N., McClean J.R., Short S.R., et al.* Quantum Simulation of Hamiltonian Spectra on a Silicon Chip [Электронный ресурс]. 2016. Препринт: arXiv:1611.03511.

[118] *Guerreschi G.G., Smelyanskiy M.* Practical Optimization for Hybrid Quantum-Classical Algorithms [Электронный ресурс]. 2017. Препринт arXiv: 1701.01450.

[119] *McClean J.R., Kimchi-Schwartz M.E., Carter J., de Jong W.A.* Hybrid quantum-classical hierarchy for mitigation of decoherence and determination of excited states // Physical Review A. 2017. V. 95. №042308.

[120] *Romero J.R., Babbush R., McClean J.R., Hempel C., Love P., Aspuru-Guzik A.* Strategies for Quantum Computing Molecular Energies Using the Unitary Coupled Cluster Ansatz [Электронный ресурс]. 2017. Препринт: arXiv:1701.02691.

[121] *Shen Y., Zhang X., Zhang S., Zhang J.-N., Yung M.-H., Kim K.* Quantum implementation of the unitary coupled cluster for simulating molecular electronic structure // Physical Review A. 2017. V. 95. №020501.

[122] *Farhi E., Goldstone J., Gutmann S.* A Quantum Approximate Optimization Algorithm [Электронный ресурс]. 2014. Препринт: arXiv: 1411.4028.

[123] *Farhi E., Goldstone J., Gutmann S.* A Quantum Approximate Optimization Algorithm Applied to a Bounded Occurrence Constraint Problem [Электронный ресурс]. 2014. Препринт: arXiv:1412.6062.

[124] *Farhi E., Harrow A.W.* Quantum Supremacy through the Quantum Approximate Optimization Algorithm [Электронный ресурс]. 2016. Препринт: arXiv:1602.07674.

[125] *Romero J., Olson J., Aspuru-Guzik A.* Quantum autoencoders for efficient compression of quantum data // Quantum Science and Technology. 2017. V. 2. №045001.

[126] *Benedetti M., Garcia-Pintos D., Nam Y., Perdomo-Ortiz A.* A Generative Modeling Approach for Benchmarking and Training Shallow Quantum Circuits [Электронный ресурс]. 2018. Препринт: arXiv:1801.07686.

[127] *Verdon G., Broughton M., Biamonte J.* A Quantum Algorithm to Train Neural Networks Using Low-Depth Circuits [Электронный ресурс]. 2017. Препринт: arXiv:1712.05304.

[128] *Dallaire-Demers P.-L., Romero J., Veis L., Sim S., Aspuru-Guzik A.* Low-Depth Circuit Ansatz for Preparing Correlated Fermionic States on a Quantum Computer // Quantum Science and Technology. 2019. V. 4. №045005.

[129] *Smith J., Lee A., Richerme P., Neyenhuis B., Hess P.W., Hauke P., Heyl M., Huse D.A., Monroe C.* Many-Body Localization in a Quantum Simulator with Programmable Random Disorder // Nature Physics. 2016. V. 12. pp. 907–911.

[130] *Mazurenko A., Chiu C.S., Ji G., Parsons M.F., Kanász-Nagy M., Schmidt R., Grusdt F., Demler E., Greif D., Greiner M.* A cold-atom Fermi-Hubbard antiferromagnet // Nature. 2017. V. 545. pp. 462–466.

[131] *Harris R., Sato Y., Berkley A.J., Reis M., Altomare F., Amin M.H., Boothby K., et al.* Phase transitions in a programmable quantum spin glass simulator // Science. 2018. V. 361. Iss. 6398. pp. 162–165.

[132] *King A.D., Carrasquilla J., Raymond J., Ozfidan I., Andriyash E., Berkley A., Reis M., et al.* Observation of topological phenomena in a programmable lattice of 1,800 qubits // Nature. 2018. V. 560. Iss. 7719. №456.

[133] *Aharonov D., van Dam W., Kempe J., Landau Z., Lloyd S., Regev O.* Adiabatic Quantum Computation is Equivalent to Standard Quantum Computation // SIAM Review. 2008. V. 50. №4. pp. 755–787.

[134] *Kadowaki T., Nishimori H.* Quantum annealing in the transverse Ising model // Physical Review E. 1998. V. 58. Iss. 5. №5355.

[135] *Albash T., Lidar D.A.* Adiabatic Quantum Computing // Reviews of Modern Physics. 2018. V. 90. № 015002.

[136] *Farhi E., Goldstone J., Gutmann S., Lapan J., Lundgren A., Preda D.* A quantum adiabatic evolution algorithm applied to random instances of an NP-complete problem // Science. 2001. V. 292. Iss. 5516. pp. 472–475.

[137] *Van Dam W., Mosca M., Vazirani U.* How Powerful Is Adiabatic Quantum Computation? // Proceedings of 42nd IEEE Symposium on Foundations of Computer Science. 2001. pp. 279–287.

[138] *Young A.P., Knysh S., Smelyanskiy V.N.* Size dependence of the minimum excitation gap in the quantum adiabatic algorithm // Physical Review Letters. 2008. V. 101. Iss. 17. №170503.

[139] *Selby A.* D-Wave: comment on comparison with classical computers [Электронный ресурс]. URL: http://www.archduke.org/stuff/d-wave-comment-on-comparison-with-classical-computers/.

[140] *Boixo S., Rønnow T.F., Isakov S.V., Wang Z., Wecker D., Lidar D.A., Martinis J.M., Troyer M.* Evidence for quantum annealing with more than one hundred qubits // Nature Physics. 2014. V. 10. pp. 218–224.

[141] *Rønnow T.F., Wang Z., Job J., Boixo S., Isakov S.V., Wecker D., Martinis J.M., Lidar D.A., Troyer M.* Defining and detecting quantum speedup // Science. 2014. V. 345. №420.

[142] *King J., Yarkoni S., Nevisi M.M., Hilton J.P., McGeoch C.C.* Benchmarking a Quantum Annealing Processor with the Time-to-Target Metric [Электронный ресурс]. 2015. Препринт: arXiv:1508.05087.

[143] *Hen I., Job J., Albash T., Rønnow T.F., Troyer M., Lidar D.A.* Probing for quantum speedup in spin-glass problems with planted solutions // Physical Review A. 2015. V. 92. №042325.

[144] *Mandrà S., Zhu Z., Wang W., Perdomo-Ortiz A., Katzgraber H.G.* Strengths and weaknesses of weak-strong cluster problems: A detailed overview of state-of-the-art classical heuristics versus quantum approaches // Physical Review A. 2016. V. 94. №022337.

[145] *Denchev V.S., Boixo S., Isakov S.V., Ding N., Babbush R., Smelyanskiy V., Martinis J., Neven H.* What is the Computational Value of Finite-Range Tunneling? // Physical Review X. 2016. V. 6. №031015.

[146] *Mandrà S., Katzgraber H.G., Thomas C.* The pitfalls of planar spin-glass benchmarks: Raising the bar for quantum annealers (again) // Quantum Science and Technology. 2017. V. 2. №3;

[147] *King J., Yarkoni S., Raymond J., Ozfidan I., King A.D., Nevisi M.M., Hilton J.P., McGeoch C.C.* Quantum Annealing amid Local Ruggedness and Global Frustration [Электронный ресурс]. 2017. Препринт: arXiv:1701.04579.

[148] *Mandrà S., Katzgraber H.G.* A deceptive step towards quantum speedup detection // Quantum Science and Technology. 2018. V. 3 №04LT01.

[149] *Albash T., Lidar D.A.* Demonstration of a scaling advantage for a quantum annealer over simulated annealing // Physical Review X. 2018. V. 8. №031016.

[150] *Albash T., Martin-Mayor V., Hen I.* Temperature scaling law for quantum annealing optimizers // Physical Review Letters. 2017. V. 119. Iss. 11. №110502.

[151] *Albash T., Martin-Mayor V., Hen I.* Analog Errors in Ising Machines // Quantum Science and Technology. 2019. V. 4 №02LT03.

[152] *Jordan S.* Algebraic and Number Theoretic Algorithms [Электронный ресурс] / National Institute of Standards and Technology. 2018. URL: http://math.nist.gov/quantum/zoo/.

[153] *Harrow A.W., Montanaro A.* Quantum computational supremacy // Nature. 2017. V. 549. Iss. 7671. №203.

[154] *Aaronson S., Arkhipov A.* The Computational Complexity of Linear Optics // Proceedings of the Forty-Third Annual ACM Symposium on Theory of Computing. 2011. pp. 333–342.

[155] *Bremner M.J., Jozsa R., Shepherd D.J.* Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy // Proceedings of the Royal Society of London A. 2010. V. 467. Iss. 2126. №20100301.

[156] *Terhal B.M., DiVincenzo D.P.* Classical Simulation of Noninteracting Fermion Quantum Circuits // Physical Review A. 2002. V. 65. №032325.

[157] *Carolan J., Harrold C., Sparrow C., Martín-López E., Russell N.J., Silverstone J.W., Shadbolt P.J., et al.* Universal linear optics // Science. 2015. V. 349. Iss. 6249. pp. 711–716.

[158] *Clifford P., Clifford R.* The Classical Complexity of Boson Sampling // Proceedings of the Twenty-Ninth Annual ACM-SIAM Symposium on Discrete Algorithms. 2018. pp. 146–155.

[159] *Boixo S., Isakov S.V., Smelyanskiy V.N., Babbush R., Ding N., Jiang Z., Bremner M.J., Martinis J.M., Neven H.* Characterizing Quantum

Supremacy in Near-Term Devices // Nature Physics. 2018. V. 14. Iss. 6. pp. 595–600.

[160] *Bouland A., Fefferman B., Nirkhe C., Vazirani U.* Quantum Supremacy and the Complexity of Random Circuit Sampling // Proceedings of 10th Innovations in Theoretical Computer Science Conference (ITCS 2019). 2018. V. 124. pp. 15:1–15:2.

[161] *Aaronson S., Chen L.* Complexity-Theoretic Foundations of Quantum Supremacy Experiments // 32nd Computational Complexity Conference, CCC 2017, Volume 79 of LIPIcs, Schloss Dagstuhl—Leibniz-Zentrum für Informatik. 2017. pp. 22:1–22:67.

[162] *Brakerski Z., Christiano P., Mahadev U., Vazirani U., Vidick T.* Certifiable Randomness from a Single Quantum Device [Электронный ресурс]. 2018. Препринт: arXiv:1804.00640.

[163] *Mahadev U., Vazirani U., Vidick T.* Efficient Certifiable Randomness from a Single Quantum Device. 2022 [Электронный ресурс]. Препринт: arXiv: 2204.11353.

[164] *Bourzac K.* Chemistry is quantum computing's killer app // Chemical and Engineering News. 2017. V. 95. Iss. 43. pp. 27–31.

[165] *Lidar D.A., Wang H.* Calculating the thermal rate constant with exponential speedup on a quantum computer // Physical Review E. 1999. V. 59. Iss. 2. №2429.

Мокряков Алексей Викторович
Горшков Владимир Владимирович

Основы квантовых вычислений

Учебное пособие

Объем 1,2 МБ Тираж 10

Редакционно-издательский отдел ФГБОУ ВО
«РГУ им. А.Н. Косыгина»

115035, Москва, ул. Садовническая, 33, стр. 1
тел. 8-495-811-01-01 доб. 1099
e-mail: riomgudt@mail.ru