

1.25. ОСНОВЫ КВАНТОВЫХ ВЫЧИСЛЕНИЙ

Цель лекции: ознакомление с физическими основами построения квантовых вычислительных систем.

1.25.1. ОСНОВНЫЕ ПОНЯТИЯ В ОБЛАСТИ КВАНТОВЫХ ТЕХНОЛОГИЙ

В настоящее время перспективная общая архитектура процессоров, даже с применением углеродных нанотрубок, проявляющих квантовые свойства, не отличается от используемых в современной полупроводниковой вычислительной технике. Такой подход имеет предел развития из-за ограничения минимальных размеров элемента процессора. Увеличение числа транзисторов при этом предполагает линейный рост производительности процессора. Идея предельного распараллеливания массива информации в современной вычислительной технике в целях повышения производительности еще далека от эффективной реализации.

Принципиально новые — квантовые вычисления — были предложены в 1980-х годах Ю. Маниным и Р. Фейнманом. Высокая эффективность устройств достигается за счет использования квантовых эффектов. В квантовых вычислениях для выполнения логической операции используется кубит, который находится не в двух состояниях (0 и 1), как в случае традиционных битовых вычислений, а во всех состояниях одновременно, т. е. суперпозиции состояний. Подобное состояние не позволяет подобрать аналога в классической физике и является чистым квантово-механическим эффектом. Основное достоинство квантового компьютера состоит в так называемом квантовом параллелизме, т. е. вычисление происходит одновременно по 2^N (N — число кубитов) состояниям, тогда как в обычном компьютере требуется $2N$ последовательных операций (рис. 1.134). Такая особенность позволяет проводить вычисления параллельно, что обеспечивает экспоненциальное увеличение эффективности при решении задач по оптимизации и факторизации чисел.

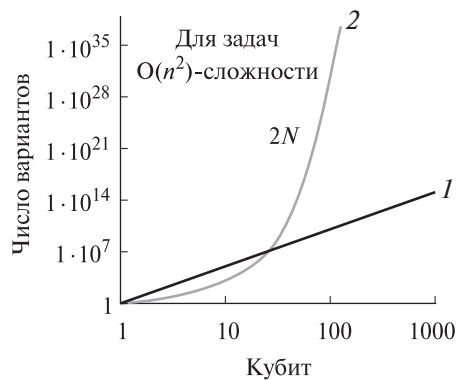


Рис. 1.134. Эффективность классических (1) и квантовых (2) вычислений

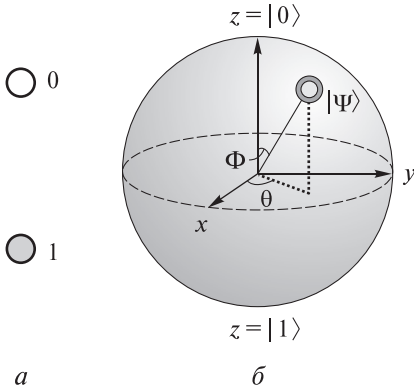


Рис. 1.135. Модель классического (а) и квантового (б) бита информации (<https://ai4wifi.com>)

Рассмотрим модель квантового бита информации. Представим шар, похожий на глобус, в котором направление по радиусу на север представлено нулем, а направление на юг — единицей. Это обычные биты. Любые другие положения соответствуют квантовым суперпозициям «0» и «1». Например, полужирной линией обозначен кубит, имеющий конкретные координаты, которые могут кодировать бесконечную последовательность цифр (рис. 1.135).

Следует отметить, что это не соответствует бесконечному количеству информации, которую содержит кубит. Квантовая механика требует, чтобы информация из кубита была извлечена путем измерения. Как и классический бит, кубит представляет единицу или ноль. Однако особенностью кубита, как и любого объекта квантовой механики, является огромный диапазон суперпозиций. В этом диапазоне содержатся в различных соотношениях оба исходных состояния. Другими словами, в кубите содержится топологическое пространство состояний между 0 и 1, поэтому кубит — базовый ресурс квантовой теории информации.

В одном кубите можно закодировать бесконечное количество классической битовой информации, однако извлечь ее обратно весьма проблематично. Если попытаться определить состояния кубита с помощью прямого измерения, то в результате прямого измерения получим ноль или единицу. Важнейшая особенность при этом — вероятность нуля или единицы зависит от широты исходного состояния (см. рис. 1.136). Таким образом, у кубита можно прочесть только один бит с определенной вероятностью. Кубит необходимо рассматривать как единицу квантовой информации, а не как бесконечное число квантовых битов.

Кубит обладает рядом уникальных особенностей. В квантовой системе состояние квантовой частицы (кубита) выражается через суперпозицию базисных состояний ($|0\rangle$ и $|1\rangle$), имеющих матрицы плотности. Сами квантовые состояния объединяются с помощью умножения тензоров, в результате которого образуется пространство состояний из n квантовых частиц с размерностью 2^n . Это означает, что если один кубит может быть в двух суперпозиционных состояниях: ($|0\rangle$ и $|1\rangle$), то два кубита — уже в четырех (00, 01, 10, 11). На k кубитах можно провести математические операции с 2^k числами одновременно. Таким образом, имея в распоряжении всего сотню кубитов, можно оперировать с числами, превосходящими число атомов во Вселенной. Отсюда следует принцип квантового параллелизма. Квантовый параллелизм представляет собой вычислительный процесс, при котором в квантовом компьютере определяются выходные значения всех входных состояний практически сразу, без необходимости последовательного перебора или расчета.

Такой результат говорит об очень высокой перспективности работ по созданию квантовых компьютеров.

Поразительные возможности квантового компьютера являются результатом развития идей квантовой физики и квантовой информатики. На квантовом уровне микромир может быть математически описан уравнением Шредингера:

$$\frac{i\hbar\partial|\Psi\rangle}{\partial t} = \tilde{H}|\Psi\rangle,$$

где линейный оператор \tilde{H} обладает свойством суперпозиции состояний

$$\tilde{H}(a|\Psi_1\rangle + b|\Psi_2\rangle) = a\tilde{H}|\Psi_1\rangle + b\tilde{H}|\Psi_2\rangle.$$

Другими словами, если система может существовать в состояниях $a|\Psi_1\rangle$ и $b|\Psi_2\rangle$, то она может существовать и в состоянии

$$|a|^2 + |b|^2 = 1,$$

где a, b — комплексные амплитуды.

Этот принцип является основой построения элементной базы квантовых компьютеров. Кубит представляет собой когерентную суперпозицию двух базисных состояний: $a|0\rangle$ и $b|1\rangle$. Для записи вектора состояния обычно используют дираковские обозначения. В самом элементарном случае двухуровневой системы (например, кубита) вектор состояния имеет вид

$$|\Psi_1\rangle = a|0\rangle + b|1\rangle.$$

Довольно часто в качестве синонима словосочетания «вектор состояния» используют термин «волновая функция».

Кубит — единица количества квантовой информации. Амплитуды a и b определяют вероятность нахождения системы в одном из базисных состояний, удовлетворяющих условию нормировки:

$$\int_V \Psi_1 \Psi_2 dV = 1.$$

Другими словами, суммарная вероятность обнаружения частицы во всем пространстве объема V равна единице. В общем случае интегрирование следует проводить по всем переменным, кроме времени, от которых волновая функция явно зависит в данном представлении.

1.25.2. АРХИТЕКТУРА КВАНТОВОГО ПРОЦЕССОРА

Квантовые компьютеры представляют собой сопроцессоры или ускорители классических компьютеров, которые питают их и управляют ими. Квантовый компьютер всегда управляется классическим компьютером, как и графический процессор для видеоигр или для обучения нейронных сетей глубокому обучению. Эти обычные компьютеры используются для запуска

программ, управляющих квантовым процессором с физическими операциями, которые должны выполняться над кубитами, и интерпретируют результаты считывания кубитов.

Проведение кубитовых операций осуществляется под управлением обычного компьютера. Вычислительный процесс в квантовом компьютере носит интерференционный характер прежде всего потому, что амплитуды базисных состояний являются комплексными числами. Именно создание интерференции состояний позволяет приумножить вычислительную мощь квантового компьютера. Под континуальной средой, составляющей топологическое пространство состояний квантового компьютера, понимают физическую среду в любом агрегатном состоянии, в которой должно быть сосредоточено достаточное число кубитов, а также могут быть введены данные и на выходе измерено состояние кубитов.

Рассмотрим требования для физической реализации квантового компьютера.

1. Необходимо создать континуальную среду, содержащую определенное число кубитов, например из двухуровневых частиц.

2. Для осуществления заданного алгоритма вычислительного процесса должна быть реализована возможность физического воздействия на каждый кубит либо на любую их пару.

3. Необходимо технически реализовать возможность приготовления по командам управляющего компьютера требуемого числа кубитов входного регистра в исходном базисном состоянии $|01, 02, 03, \dots, 0L\rangle$.

4. В процессе квантовых вычислений следует исключить эффекты, связанные с разрушением квантовой когерентности и квантовых состояний при взаимодействии с внешней средой, а также исключить помехи.

5. Физические свойства континуальной среды, в которой используются выбранные кубиты, должны обеспечить нелинейные взаимодействия для выполнения одно- и двухкубитовых операций.

6. На выходе квантового компьютера должно быть обеспечено надежное и точное измерение состояний квантовой вычислительной системы.

Последний пункт является наиболее трудной задачей при создании квантового компьютера, поскольку, как известно, при попытке прямого измерения состояния микрочастицы наблюдается коллапс ее волновой функции.

Рассмотрим схему квантового компьютера (рис. 1.136). Квантовый компьютер состоит из трех основных блоков: квантового регистра состояний, блока контроллеров квантовых вентилях и блока измерения состояния кубитов.

Квантовые регистры хранят информацию, обрабатываемую в компьютере, и используют принцип суперпозиции и запутанности, позволяя выполнять одновременные операции с большим числом значений регистров. Если провести параллель с классическими вычислениями, это память. Но обработка проводится непосредственно в памяти.

Контроллеры квантовых вентилях — физические устройства, которые воздействуют на кубиты квантовых регистров как для их инициализации, так и для выполнения на них квантовых вентилях. Эти команды применяются итеративно, в соответствии с алгоритмами, которые должны быть выполнены.

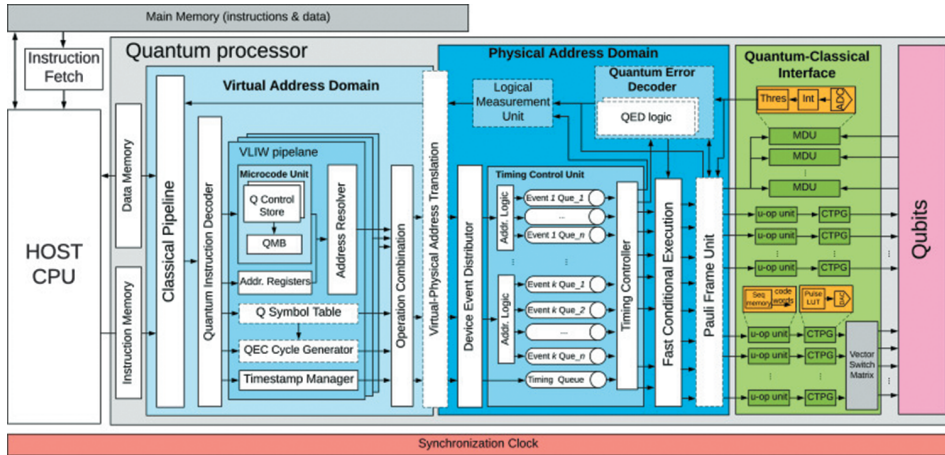


Рис. 1.136. Схема квантового компьютера (Fu X., Lao L., Bertels K., Almudever C.G. A control microarchitecture for fault-tolerant quantum computing. 2019. Vol. 70. Pp. 21–30)

Их также можно использовать для управления кодами исправления ошибок. Квантовые вентили передают регистры как данными, так и инструкциями. Это не отдельные операции, как в классических микропроцессорах.

Измерение состояния кубита используется для получения результата в конце последовательного выполнения квантовых вентилей алгоритма и для оценки синдромов ошибок во время квантовой коррекции ошибок. Этот цикл инициализации, расчета и измерения обычно применяется несколько раз для оценки результата алгоритма. Затем результат усредняется до значения от 0 до 1 для каждого кубита в регистрах квантового компьютера. Значения, считанные физическими считывающими устройствами, затем преобразуются в цифровые значения и передаются на обычный компьютер, который управляет всем и выполняет интерпретацию результатов. В обычных случаях, таких как D-Wave и IBM, вычисления повторяются не менее 1000 раз.

Квантовые микросхемы обычно включают в себя квантовые регистры, элементы управления квантовыми вентилями и измерительные устройства (в случае сверхпроводящих кубитов или кубитов с электронным спином управление осуществляется посредством подачи микроволнового сигнала). Другие типы кубитов, как, например, на ионных ловушках или холодных атомах, используют лазеры для инициализации и измерения кубитов. Существующие на данный момент чипы схем имеют размер полнокадрового или двухформатного фотосенсора. Каждый кубит относительно велик, их размер измеряется в микронах для сверхпроводящих кубитов или до 100 нм для кубитов с электронным спином, тогда как современные КМОП-транзисторы процессоров имеют размеры транзисторов около 5 нм.

Чип для сверхпроводящих и электронных спиновых кубитов имеет размеры несколько квадратных сантиметров. Обычно он интегрируется в мед-

ный корпус, оснащенный коаксиальными разъемами, необходимыми для управления вентилями кубитов. В новейших сверхпроводниковых процессорах от IBM и Google с 53 кубитами требуется более 160 таких разъемов. Чип интегрирован в два небольших концентрических корпуса из алюминия и Стурегт экраны (M μ Shield) с магнитной изоляцией.

Ключевые показатели. Самый известный набор ключевых показателей производительности квантовых компьютеров был создан Д. Ди Винченцо в 2000 г., когда он был исследователем IBM. Хотя отдельных кубитов практически не существовало, он определил основные технические характеристики универсального квантового компьютера на основе вентилях следующим образом.

1. Хорошо охарактеризованные кубиты.

Квантовые компьютеры используют кубиты, использующие квантовые объекты, которые могут иметь два различных и измеримых состояния. Их физические характеристики хорошо известны. Архитектура является масштабируемой в том смысле, что может использовать большое число физических кубитов, а затем и логических кубитов.

2. Инициализируемые кубиты.

В общем значении $|0\rangle$, часто называемому основным состоянием для ассоциированных квантовых объектов, соответствует, например, низший уровень энергии элементарной частицы или искусственного атома, как для сверхпроводящих кубитов.

3. Время когерентности.

Время, в течение которого кубиты находятся в когерентном состоянии, должно быть больше времени активации квантовых вентилях, чтобы можно было выполнить алгоритм, содержащий достаточно длинную последовательность квантовых вентилях. Преимущество кодов исправления ошибок, использующих большое число физических кубитов, заключается в увеличении полезного времени вычислений.

4. Набор универсальных квантовых вентилях.

Квантовое оборудование должно позволять создавать универсальный набор вентилях. Это зависит от технологии кубитов. Для этого требуется минимальный набор однокубитных вентилях, позволяющий создавать любое вращение в сфере Блоха, дополненное двухкубитным вентилем CNOT.

5. Измерение.

Возможность измерения состояния кубитов в конце вычислений. Это измерение не должно влиять на состояние других кубитов в системе. В идеале частота ошибок измерения должна быть значительно ниже 0,1 %.

Критерии Ди Винченцо довольно просты. С практической и эксплуатационной точки зрения квантовые компьютеры также можно охарактеризовать другим набором параметров.

6. Число кубитов.

Это обуславливает доступную вычислительную мощность, поскольку эта мощность теоретически увеличивается экспоненциально с числом кубитов, это ключевой параметр. По состоянию на середину 2021 г. коммерческий рекорд составлял 65 кубитов с самой большой системой IBMQ, доступной

в облаке. Число кубитов следует оценивать с точки зрения его масштабируемости. Некоторые технологии легче миниатюризировать и масштабировать, чем другие. В эту миниатюризацию необходимо интегрировать как чипы квантовых кубитов, так и элементы, которые ими управляют. Кроме того, необходимо следить за тем, чтобы декогеренция и шум не увеличивались по мере роста числа кубитов. Кубиты в ионных ловушках обладают превосходной точностью, но плохо масштабируются. Вероятно, сверхпроводящие кубиты лучше масштабируются, но их точность не стабильна по мере роста числа кубитов. Кубиты на холодных атомах масштабируются немного лучше, но с некоторыми практическими ограничениями по числу управляемых атомов. Теоретически кубиты с электронными спинами могут масштабироваться лучше всего.

7. Возможность подключения кубитов.

Это обуславливает скорость выполнения квантовых алгоритмов. Чем больше эта физическая связь, тем быстрее будет выполнение кода. При низкой связности компилятору квантового кода придется добавить гораздо больше операций для связывания кубитов вместе, особенно полагаясь на шлюзы SWAP. Эта связь сильно варьируется от одной технологии к другой. В 2D-технологиях, как и в случае со сверхпроводящими и кремниевыми кубитами, она ограничена соседними кубитами.

8. Параллельность вычислений.

То, как кубитовые вентили могут быть распараллелены в разных зонах кубитов без нарушения работы, также будет определять скорость выполнения квантовых алгоритмов.

9. Точность выполнения логических операций.

При выполнении квантовых вентилях и считывании их состояния точность кубитов обуславливает возможность выполнения длинных алгоритмов. Это напрямую влияет на глубину поддерживаемого алгоритма, а также на способность запускать коды квантовой коррекции ошибок и создавать логические кубиты с произвольным уровнем точности.

10. Длительность операций как для квантовых вентилях, так и для измерения состояния кубита.

Первое, очевидно, важно для того, чтобы алгоритмы работали как можно быстрее, но второе не менее важно, потому что кубит участвует в кодах исправления ошибок и, следовательно, обуславливает время выполнения всех алгоритмов.

11. Рабочая температура.

Для процессора и его оборудования многое зависит от типа кубитов. Действующие в настоящее время квантовые компьютеры на основе сверхпроводников работают при очень низкой, близкой к абсолютному нулю температуре, но предполагается, что некоторые типы кубитов все еще находятся на стадии исследований. Так, например, предназначены для работы при комнатной температуре, схемы на фотонах и NV-центрах. Однако это не обязательно относится к сопутствующему оборудованию, такому как фотонные генераторы и однофотонные детекторы. Работа при очень низкой температуре — это способ сохранить когерентность кубитов. Но чем ниже температура, тем меньше энергии могут излучать кубиты и их управляющая электроника.

12. Общее потребление энергии включает в себя потери на все компоненты квантового компьютера: сам процессор, всю его управляющую электронику, а также задействованные криогенные системы.

1.25.3. ФИЗИЧЕСКИЕ ПЛАТФОРМЫ ДЛЯ РЕАЛИЗАЦИИ КВАНТОВЫХ ВЫЧИСЛЕНИЙ

Рассмотрим варианты реализации квантового компьютера. Для создания реального квантового компьютера необходимо получить практические результаты по ряду направлений исследований, в частности, по созданию регистров кубитов. В качестве кубита может быть выбрана почти любая квантовая система, например, можно выбрать двухуровневые квантовые ячейки со спином, равным $1/2$. Это могут быть электронные или ядерные спины, можно также выбрать орбитальные состояния электрона в квантовых ямах или квантовых точках. Состояния «0» и «1» электрона в квантовых точках разделить потенциальным барьером; управление динамикой кубита осуществлять лазерными импульсами через возбужденные уровни энергии электрона. Одиночный фотон может также служить кубитом. Любые два состояния фотона с ортогональными поляризациями интерпретируются как состояния кубита $|0\rangle$ и $|1\rangle$. В качестве кубита можно использовать два фотонных состояния, различающихся фазой. Кроме двухуровневой реализации кубитов, возможна их реализация в трехуровневой системе. Биты в таких системах получили название «кутриты» (*q-trits*), в многоуровневых системах единицы информации называются кудитами (*q-dits*).

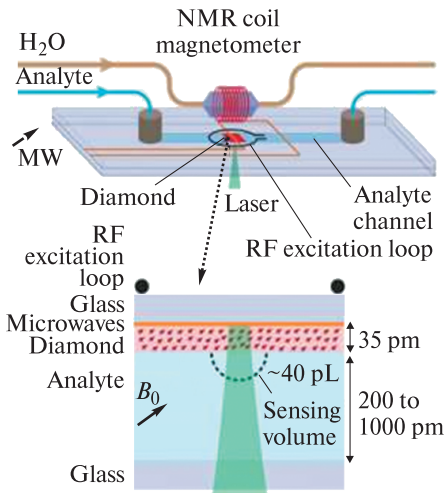


Рис. 1.137. Схема квантового компьютера на основе ЯМР-резонанса на МОП-структуре (*Hensen B et al. A silicon quantum-dot-coupled nuclear spin qubit // Nat. Nanotechnol., 2020. Vol. 15. No. 1. Pp. 13–17*)

Квантовые компьютеры на основе ядерного магнитного резонанса (ЯМР).

Такие устройства представляют собой непрерывную среду с ядерными спинами-кубитами. Считается, что реализовать ЯМР-компьютер возможно, если число кубитов в компьютере будет больше одной тысячи.

Материал подложки выполняют из бесспинового изотопа кремния ^{28}Si . В подложку в приповерхностный слой внедрены донорные атомы фосфора ^{31}P , замещающие атомы кремния в узлах кристаллической решетки (рис. 1.137). Такие доноры обладают ядерными спинами $I = 1/2$. Спины не взаимодействуют с окружающими атомами кремния, но могут взаимодействовать между собой за счет частичного перекрытия электронных волновых функций. Регулярно расположенные в полупроводниковой структуре донорные атомы с

ядерными спинами могут быть использованы в качестве кубитов. Глубина залегания доноров ~ 20 нм.

Кубиты располагают на расстоянии l (~ 20 нм) один от другого, а над ними формируют решетку из управляющих затворов с периодом l . Решетка из A -затворов служит для управления резонансной частотой ядерно-спинового кубита. Подобная решетка из J -затворов служит для управления взаимодействием электронов соседних ядерных спинов.

Квантовые компьютеры на квантовых точках. Квантовые точки удерживают один или несколько электронов или дырок основного материала, которые достаточно малы, чтобы квантовые эффекты были значительными, и достаточно велики, чтобы их можно было контролировать. В качестве основного материала обычно используют полупроводники. Изначально использовался GaAs, так как на его основе возможно сделать высококачественные квантовые ямы для улавливания электронов. Однако и Ga, и As имеют общий ядерный спин, который взаимодействует с электронным спином и вызывает быстрое разрушение когерентного состояния. В настоящее время предпочтительными полупроводниковыми материалами являются Si, Ge, SiGe и изотоп ^{28}Si . Преимуществом такого подхода является возможность использования передовых полупроводниковых технологий.

Цепочка квантовых точек формируется в подзатворном диэлектрике кремниевое МОП-транзистора (рис. 1.138). Для индивидуального управления кубитами наряду с общим затвором внутри диэлектрика создают систему индивидуальных управляющих затворов G_i , действующих непосредственно на каждый кубит.

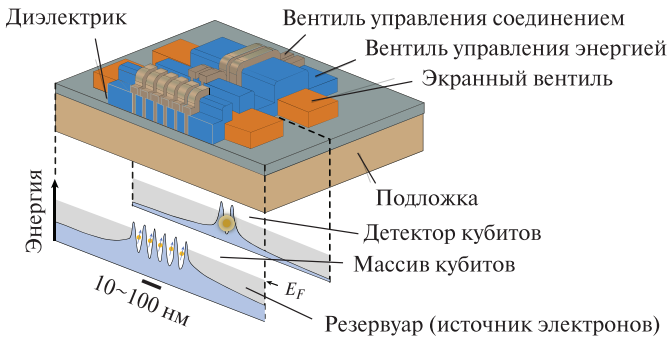


Рис. 1.138. Схема квантового компьютера на квантовых точках

При приложении к общему верхнему затвору большого напряжения происходит заполнение состояний квантовых точек и унифицируются состояния кубитов. Входные и выходные сигналы поступают через индивидуальные затворы каждого кубита. Систему кубитов в МОП-транзисторе можно рассматривать как последовательный ряд МОП-структур, которые соответствуют связанным квантовым точкам.

При приложении напряжения между истоком и стоком начнет формироваться обедненная область, ширина которой будет увеличиваться в сторону стока. Из условия уравнивания непрерывности следует, что токи на разных участках должны быть равны. Если напряжение на первом кубите равно V_1 , а на втором — V_2 , то, вычисляя ток, можно определить перераспределение зарядов и сдвиг порогового напряжения.

Рабочие температуры кубитов на квантовых точках могут достигать 1 К, что позволяет интегрировать управляющую электронику на одном чипе. Архитектуры квантовых компьютеров на основе квантовых точек в настоящее время являются активной областью исследований.

Квантовые компьютеры на ионных ловушках. Кубиты на ионных ловушках кодируют квантовую информацию на электронных энергетических уровнях ионов, таких как Ca^+ или Yb^+ . Благодаря тому что ион обладает электрическим зарядом, возможно получить два практических явления. Во-первых, ионы можно «подвесить» во внешнем электромагнитном поле в так называемой ионной ловушке. Во-вторых, ионы отталкиваются друг от друга вследствие действия кулоновских сил и выстраиваются в цепочку на расстоянии 5...10 мк друг от друга. Благодаря этому же кулоновскому взаимодействию реализуется запутанное состояние между ними (рис. 1.139). Для контроля и считывания состояния кубитов обычно используют лазеры и детекторы фотонов.

Работа системы при криогенных температурах помогает достичь необходимых условий вакуума и снижает электронные шумы. Так, работа при температуре 50...100 К дает значительные преимущества.

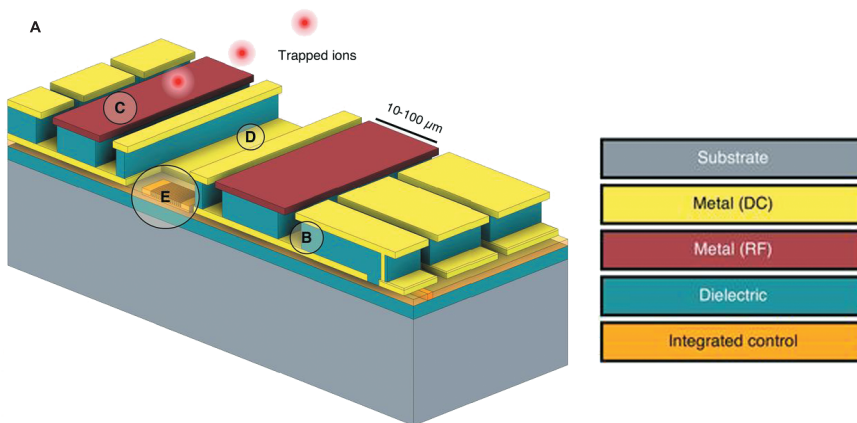


Рис. 1.139. Схема квантового компьютера на ионных ловушках (*Fu X., Lao L., Bertels K., Almudever C.G. A control microarchitecture for fault-tolerant quantum computing. 2019. Vol. 70. Pp. 21–30*)

Линейные ионные ловушки хорошо зарекомендовали себя и позволяют получить запутанные состояния для 10...20 кубитов. Текущие усилия сосредоточены на масштабировании до 50...100 кубитов. При большем числе кубитов необходим поиск нового метода физического перемещения ионов между линейными ловушками или передачи квантовой информации между модулями. Возникают проблемы с масштабируемостью систем с несколькими линейными ловушками.

Квантовые компьютеры на фотонах. Кубиты на основе фотонов имеют ряд преимуществ. Во-первых, в отличие от остальных систем, квантовые состояния света слабо подвержены декогеренции, или она может быть эффективно подавлена, во-вторых, оптические фотоны являются универсальными носителями информации, пригодными как для обработки (реализации алгоритмов вычислений), так и для передачи (в том числе и по квантовым каналам связи) информации. Однако практическое применение такого рода систем ограничено вероятностным характером двухкубитных оптических гейтов, обусловленным слабым взаимодействием одиночных фотонов друг с другом.

Ключевыми компонентами (модулями) линейно-оптического квантового компьютера являются источники одиночных неразличимых фотонов, фотонные интегральные схемы с предельно малыми потерями и высокоэффективные однофотонные детекторы.

В настоящее время реализована многофотонная запутанность в кремниевых устройствах и квантовая телепортация, которые могут обеспечить масштабируемую платформу для квантовых вычислений или более общей квантовой обработки информации.

Квантовые компьютеры на базе сверхпроводников. Наиболее перспективной платформой создания квантового компьютера являются сверхпроводниковые кубиты. Первая реализация такого типа кубита была представлена Компанией NEC в 1999 г. Сверхпроводниковый кубит по сути является нелинейным устройством. Конструктивно кубит представляет собой *LC*-контур, где в качестве индуктивности используется джозефсоновский переход — нелинейный бездиссипативный элемент. В качестве емкости может быть использован встречно-штыревой либо плоскопараллельный конденсатор. Для связи между кубитами, а также для считывания состояния кубита используются линейные резонансные структуры (резонаторы). Как правило, резонаторы выполнены в виде компланарной линии.

Благодаря особенности джозефсоновского перехода, заключающейся в нелинейной индуктивности данного элемента, дополнительно шунтируя переход конденсатором, возможно создать особый колебательный контур. Энергетические уровни данного контура эквидистантны, что дает возможность разделять и четко определять состояния системы. Типовая схема сверхпроводникового кубита представлена на рис. 1.140. Для возбуждения состояния кубита используется *XU*-управление, для настройки частоты кубита — *Z*-управление.

Преимуществом рассматриваемой платформы является совместимость с технологиями микроэлектронной промышленности. За счет планарной ре-

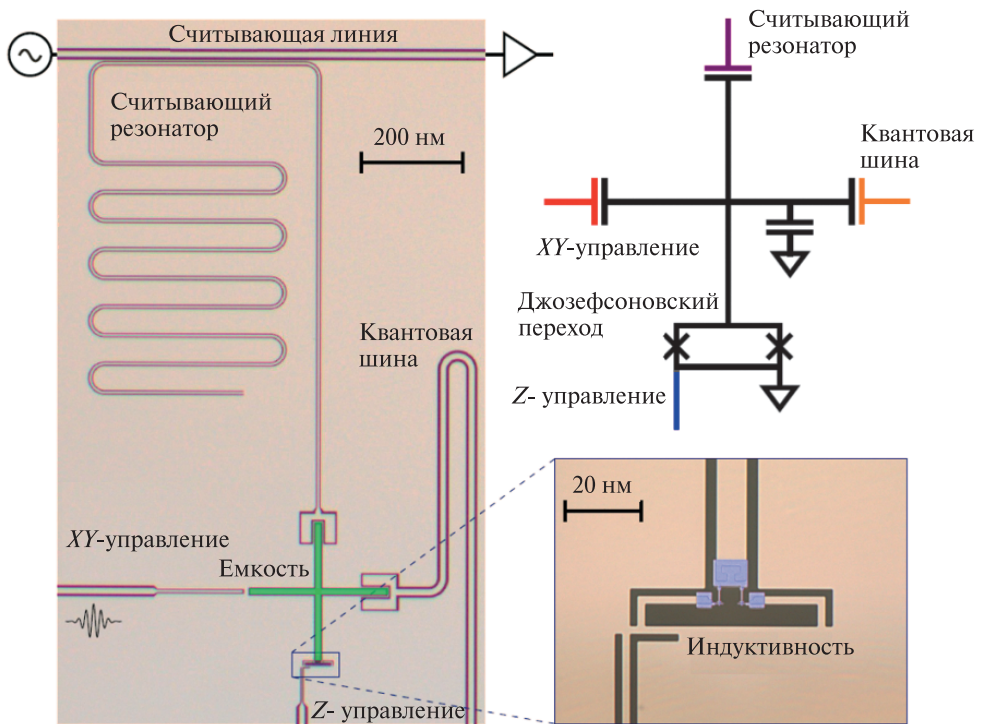


Рис. 1.140. Схема квантового компьютера на сверхпроводящих кубитах (*Pino J.M. et al. Demonstration of the trapped-ion quantum CCD computer architecture // Nature, 2021. Vol. 592. No. 7853. Pp. 209–213*)

лизации кубитов также возможна масштабируемость. Работа со сверхпроводниковыми структурами подразумевает работу при сверхнизких температурах, для этого используют криостат растворения.

Традиционный подход к управлению сверхпроводящими кубитами и реализации квантовых вентилях предполагает использование резонансных микроволновых импульсов с тщательно контролируемой амплитудой и фазой. Генерация микроволновых сигналов для сверхпроводниковых кубитов требует значительных аппаратных затрат на оборудование, работающее при комнатной температуре за пределами криостата, включая микроволновые источники, генераторы сигналов произвольной формы и усилители сигнала.

В 2019 г. специалистами Google был опубликован доклад о достижении квантового превосходства. В научном эксперименте исследовали квантовый компьютер Google на базе процессора, содержащего 53 кубита, получивший название Sycamore. Данный результат наглядно продемонстрировал перспективность реализации квантового компьютера на базе сверхпроводников.

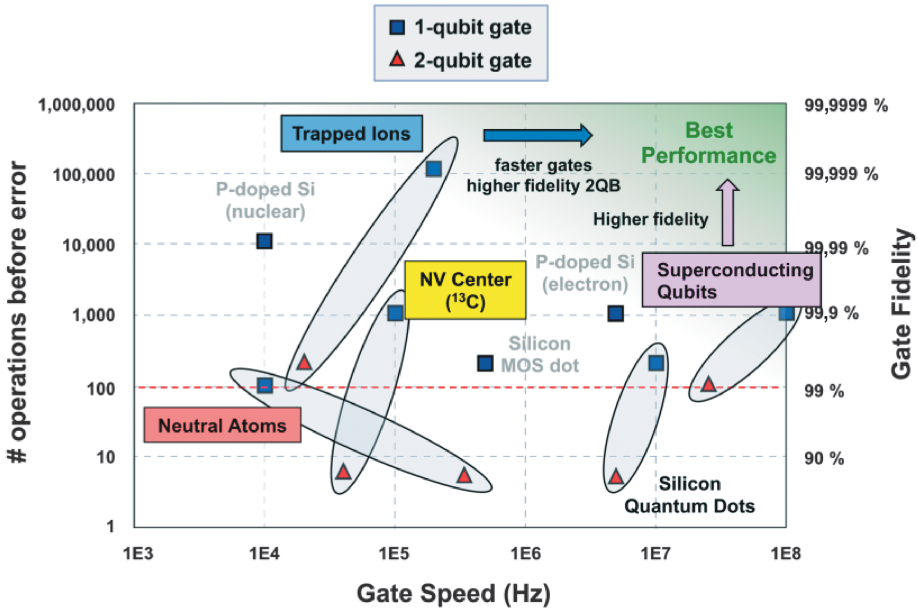


Рис. 1.141. Тенденции развития различных типов кубитов

На рис. 1.141 представлено сравнение кубитов по трем параметрам: тактовой частоте квантовых вентилей (число вентилей, которые могут выполняться в секунду), по числу операций до возникновения ошибок и точности квантовых вентилей. В последнее время наблюдается стремительное развитие кубитов различных типов.

1.25.4. ОБЛАСТИ ПРИМЕНЕНИЯ КВАНТОВЫХ КОМПЬЮТЕРОВ

Ключевым отличием квантовых вычислений от классических является их значительная вычислительная мощность. Квантовые компьютеры могут быть использованы для решения NP-полных задач в области информационной безопасности, машинного обучения, квантовой химии, моделирования новых материалов и лекарств.

Теоретическое обоснование концепции использования квантовой механики для повышения производительности вычислений было дано при публикации алгоритма Шора⁶, обеспечивающего экспоненциальное ускорение

⁶ Shor P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer // SIAM J. Comput., 1997. Vol. 26. No. 5. Pp. 1484–1509.

для факторизации числа. Спустя семь лет с помощью этого алгоритма компанией IBM было экспериментально показано разложение числа 15 с использованием кубитов на основе явления ядерного магнитного резонанса. Другим подтверждением эффективности является алгоритм Гровера, обеспечивающий полиномиальное ускорение для неструктурированного поиска. В настоящее время доступно множество алгоритмов, в том числе алгоритмы машинного обучения, оптимизации на основе алгоритма квантовой приближенной оптимизации (QAOA) и, в частности, применения в теоретической химии и материаловедении.

Несмотря на то что для создания универсального квантового компьютера необходимо решить огромное количество фундаментальных и научно-прикладных задач, квантовые вычисления уже находят применение в жизни. Такие компании, как Google и Microsoft, начали работу над квантово-безопасными алгоритмами шифрования. Хотя в настоящее время они находятся на стадии тестирования, ожидается, что квантово-безопасные алгоритмы помогут защитить банковские транзакции, военную связь, медицинские записи и т. д. В сотрудничестве с Recruit Communication компания D-Wave Systems стала первой в применении квантовых вычислений для оптимизации маркетинга, рекламы и коммуникации. Концерн Volkswagen продемонстрировал использование квантовых вычислений для оптимизации трафика. Компания The Weather Company в сотрудничестве с Национальным центром атмосферных исследований и Университетской корпорацией атмосферных исследований в США IBM создает модель квантовых вычислений, которая может оценивать грозы на региональном уровне.

В развитии квантовых вычислений выделяют несколько этапов.

1. Квантовое превосходство — академическое определение способности построить квантовый компьютер, который превосходит возможности классического компьютера при решении какой-либо задачи. В настоящее время квантовое превосходство принадлежит компаниям Google на сверхпроводниковой платформе и Научно-техническому университету Китая (USTC) на фотонных интегральных схемах.

2. Квантовые симуляторы — системы, позволяющие моделировать другие квантовые системы, что может быть использовано при исследовании материалов, комбинаторной оптимизации и обработке больших данных. Узконаправленные вычислители моделируют системы, чтобы предоставить информацию об их поведении. Например, система из одиночных холодных атомов в оптической решетке, создаваемой лазерными лучами, может моделировать процессы, происходящие в сложных твердотельных системах, таких как высокотемпературные сверхпроводники. Кроме того, с помощью квантовых симуляторов уже в настоящее время можно рассчитать свойства простых материалов, исследовать свойства атомного ядра или разработать более эффективные алгоритмы для компенсации ошибок, отработать настройки квантовой системы и т. д.



Рис. 1.142. Прогноз Компании McKinsey & Company

3. Универсальный квантовый компьютер, на его создание могут потребоваться десятки лет. Ключевым отличием квантовых вычислений от классических является их огромная вычислительная мощность. Квантовые компьютеры могут быть использованы для решения NP-полных задач в области информационной безопасности, машинного обучения, квантовой химии, моделирования новых материалов и лекарств.

Инфографика распределения квантовых вычислений в различных областях (прогноз от Компании McKinsey & Company) представлена на рис. 1.142.

Оптимизация. Самый известный пример проблемы, допускающей полиномиальное квантовое ускорение, это неструктурированный поиск, нахождение отмеченного элемента из списка в базе данных, что необходимо для оптимизации цепочек поставок и производства. Оптимизация включает в себя выбор наилучшего из многих и важна для решения множества практических задач в таких областях, как инженерное проектирование, логистика, производство и финансы. Сложность решения оптимизационных задач возрастает с количеством элементов, возможных взаимодействий и ограничений. Ожидается, что квантовые компьютеры обеспечат наибольшую пользу именно при решении сложных задач оптимизации. Например, квантовые вычисления могут быть использованы для снижения затрат на производ-

ственные процессы и сокращения времени цикла сложных процессов. Еще одно применение — квантовая оптимизация кредитных портфелей, чтобы кредиторы могли высвободить капитал, снизить процентные ставки и улучшить свои предложения. Оптимизация является основной подзадачей в приложениях машинного обучения и требует множества примеров оптимальных и почти оптимальных решений. Процессоры квантового отжига от коммерческой Компании D-Wave Systems позволяют получить доступ в режиме онлайн в модели облачных вычислений. Решение задач оптимизации трафика и поездов включено в пилотные программы компаний D-Wave и Volkswagen для оптимизации транспортных потоков в Пекине, Барселоне и Лиссабоне. В последнем случае парк автобусов двигался по разным маршрутам, адаптированным к условиям движения в реальном времени с помощью квантового алгоритма, который Концерн Volkswagen продолжает настраивать после каждого пробного запуска.

Криптография. Предполагается, что квантовые компьютеры достаточного размера могут использоваться для взлома существующих криптографических протоколов (в частности, шифрования RSA). Целочисленная факторизация, которая лежит в основе безопасности криптографических систем с открытым ключом, считается вычислительно невыполнимой с обычным компьютером для больших целых чисел, если они являются произведением нескольких простых чисел (например, произведения двух 300-значных простых чисел). Для сравнения: квантовый компьютер мог бы эффективно решить эту проблему, используя алгоритм Шора, чтобы найти ее факторы. Эта способность позволит квантовому компьютеру взломать многие криптографические системы, используемые в настоящее время. В частности, большинство популярных шифров с открытым ключом основаны на сложности факторизации целых чисел или проблеме дискретного логарифмирования, которые могут быть решены с помощью алгоритма Шора.

Квантовая сеть. Коммуникационная сеть будет защищать передаваемые данные с использованием фундаментальных законов квантовой механики. Квантовая сеть является практической реализацией так называемой квантовой криптографии. Квантовые сети формируют важный элемент квантовых вычислений и квантовых систем криптографии. Они допускают транспортировку квантовой информации между физически разделенными квантовыми системами. В распределенных квантовых вычислениях сетевые узлы в сети могут обрабатывать информацию, выполняя функцию квантовых вентилялей. Безопасная передача данных может быть реализована с помощью алгоритмов квантового распределения ключей.

Машинное обучение, поддерживаемое или улучшенное квантовыми вычислениями, является относительно новой областью применения, находящейся на стадии оценки и разработки. Квантовый отжиг может быть использован при дискретной оптимизации и выборке, в частности, при выборке Больцмана, которая является основным методом машинного обучения. Из-

вестные приложения включают в себя распознавание изображений и вывод образов для транспортных средств и здравоохранения, нейронные сети и системы рекомендаций. Достижения в алгоритмах квантового машинного обучения также привели к усовершенствованию классических алгоритмов, что уменьшило потенциальные выгоды.

В 2020 г. Компания Google в сотрудничестве с Концерном Volkswagen и Университетом Ватерлоо запустила программу TensorFlow Quantum для ускорения разработки квантовых вычислений, которая представляет собой библиотеку с открытым исходным кодом, используемую для прототипирования моделей квантового машинного обучения.

Разработка лекарств входит в список особенно важных применений квантовых вычислений. Фармацевтическим компаниям может потребоваться более 10 лет и затраты миллиардов долларов, чтобы открыть или разработать новое лекарство, для которого ученые проводят сотни миллионов сравнений на обычных компьютерах. Однако возможности обработки традиционных компьютеров ограничены, поскольку они могут анализировать молекулы только до определенного размера. Эту проблему можно решить с помощью квантовых вычислений. По мере того как алгоритмы и аппаратное обеспечение квантовых вычислений становятся все более распространенными, они сделают возможным сравнение гораздо более крупных молекул. Это может резко сократить время и затраты, связанные с разработкой лекарств, что позволит ученым находить лекарства от различных болезней быстрее, чем ожидалось.

Реклама и маркетинг. Применение квантовых вычислений в рекламе и маркетинге является революционным. Квантовые алгоритмы могут помочь создавать и доставлять более качественную рекламу, интерпретируя ассоциации, влияющие на модели покупок. Вместо того чтобы просто использовать историю браузера для показа рекламы, квантовые алгоритмы фокусируются на том, как пользователи себя чувствуют после просмотра рекламы и какие типы рекламы могут помочь установить долгосрочные отношения с клиентами.

В сотрудничестве с Компанией Recruit Communication компания D-Wave Systems стала первой в применении квантовых вычислений для оптимизации маркетинга, рекламы и коммуникации. Они стремятся использовать квантовые вычисления в рекламе для анализа сложных данных за меньшее время и повышения эффективности доставки рекламы своим целевым клиентам.

Интеллектуальная деятельность. Гигантская вычислительная мощность квантовых компьютеров позволит использовать их для осуществления интеллектуальной деятельности различного характера, например, создать на их основе экспертную систему. В памяти такой экспертной системы может храниться огромное количество научных и технических сведений — стандартов, патентов, образцов промышленного оборудования и др.; экспертная система под контролем специалистов будет выдавать готовые чертежи экспериментальных разработок.

1.25.5. КВАНТОВЫЕ КОМПЬЮТЕРЫ В РОССИИ

Российские ученые внесли огромный вклад в развитие квантовых вычислений: от зарождения идеи вычислений Ю. Манина в 1980 г. до реализации первого кубитного процессора. Так, группа ученых из Гарвардского университета и Массачусетского технологического института под руководством М. Лукина, профессора физики из Гарварда и сооснователя Российского квантового центра, создала программируемый квантовый вычислитель на базе 51 кубита, став, таким образом, лидером среди участников «квантовой гонки». Принцип его работы заключался в формировании кубитов на основе «холодных атомов», которые удерживались оптическими «пинцетами» — специальным образом организованными лазерными лучами (рис. 1.143). С помощью этого квантового вычислителя была решена задача моделирования поведения квантовых систем из множества частиц, практически нерешаемая с помощью классических компьютеров.

В 2021 г. специалисты Национальной квантовой лаборатории совместно с Российским квантовым центром (РКЦ) и ФИАН сообщили о создании прототипа квантового компьютера на платформе из 20 ионов, захваченных электромагнитной ловушкой. Российские ученые также работают и над специализированным облачным софтом. Собственные универсальные облачные платформы квантовых вычислений представили Центр квантовых тех-

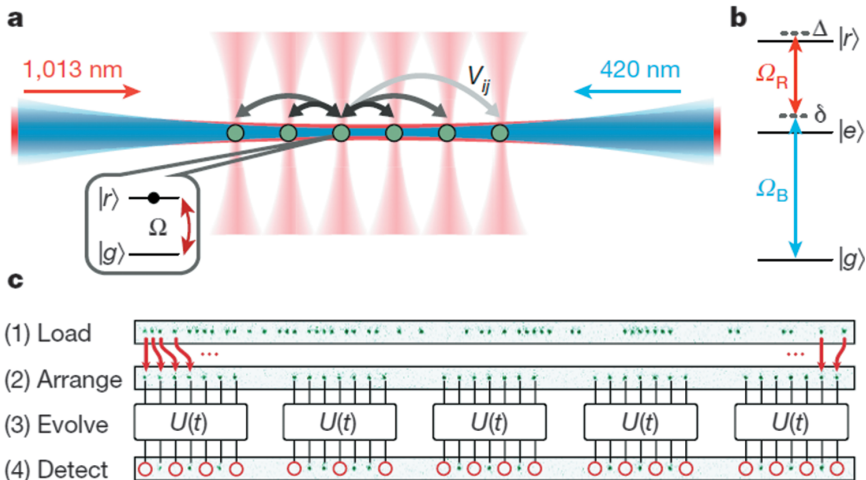


Рис. 1.143. Схема квантового вычислителя на основе «холодных атомов» (Perdomo-Ortiz A., Benedetti M., Realpe-Gómez J., Biswas R. Opportunities and challenges for quantum-assisted machine learning in near-term quantum computers // Quantum Sci. Technol., 2018. Vol. 3. No. 3)

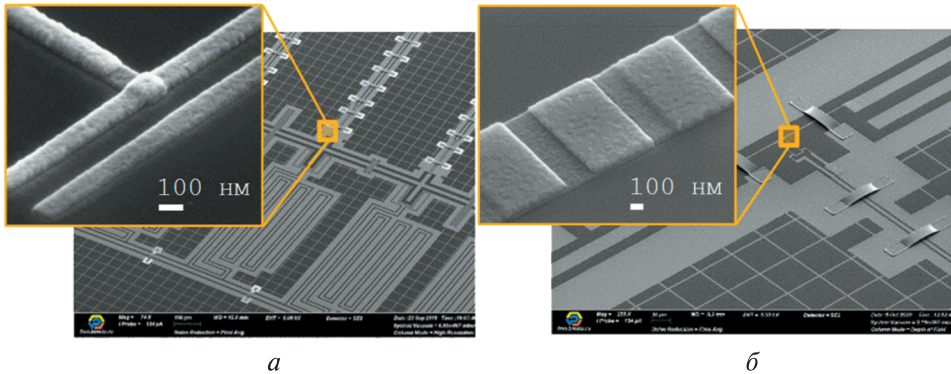


Рис. 1.144. Изображения схем зарядовых (а) и потоковых (б) кубитов, изготовленных в НОЦ «ФМНС» МГТУ им. Н.Э. Баумана, полученные на СЭМ

нологий МГУ им. М.В. Ломоносова и РКЦ. В 2022 г. была запатентована новая архитектура квантового процессора на основе кудитов, которые в отличие от кубитов имеют более двух энергетических уровней.

Развитие элементной и измерительной баз для наиболее перспективной — сверхпроводниковой платформы, требующей огромных материальных ресурсов, передового технологического оборудования и высокой квалификации кадров, началось только в 2016 г. при поддержке Фонда перспективных исследований. Исполнителями проекта выступили научный консорциум ведущих российских вузов (МФТИ, МИСиС, НГТУ, МГТУ им. Н.Э. Баумана), ИФТГ РАН, РКЦ и ФГУП «ВНИИА им. Н.Л. Духова», являющийся головной организацией консорциума.

В результате выполнения проекта был сформирован перспективный научный и технологический задел по созданию квантовых компьютеров на основе сверхпроводящих кубитов. Были разработаны уникальные технологии создания элементной базы для сверхпроводящих кубитов с толщинами пленок 20...300 нм, параметром шероховатости не более 1,5 нм, контролируемой толщиной туннельного слоя менее 2 нм и высокой воспроизводимостью линейных размеров в широком диапазоне размеров от 0,08 до 2 мкм (среднеквадратическая ошибка не ниже 5 нм). Изображения изготовленных схем кубитов-трансмонов и флаксониумов, полученные с разрешением до 1 нм на сканирующем электронном микроскопе (СЭМ), представлены на рис. 1.144.

Одной из ключевых характеристик кубитов, необходимой для выполнения логических операций, является «время жизни» кубита. Разработанная в рамках проекта технология создания сверхпроводниковых кубитов-трансмонов позволила обеспечить характерное время когерентности более 50 мкс и высокую точность выполнения операций, что приближает российские разработки в этой области к лучшим мировым аналогам.

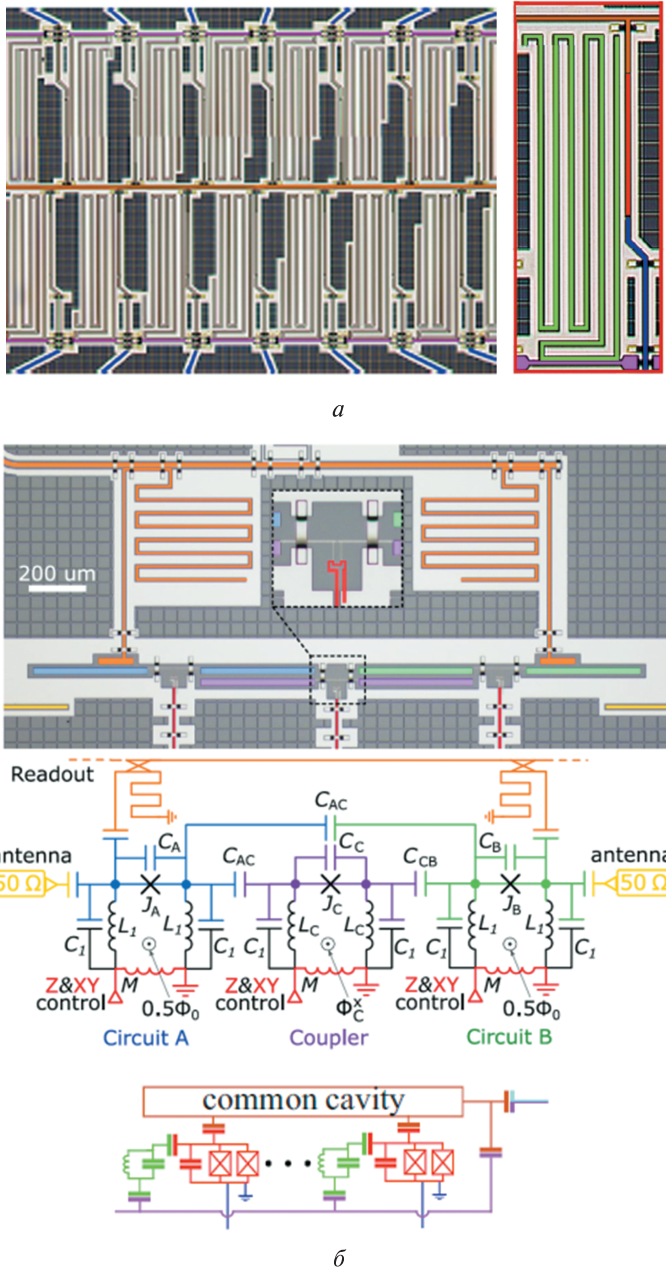


Рис. 1.145. Оптические изображения (а) и электрическая схема чипов с 25 перестраиваемыми кубитами-трансмонами (б) (*Mazhorin G.S. et al. Cavity-QED of a quantum metamaterial with tunable disorder // Phys. Rev. A 105. 033519. 2022. Pp. 1–12*) и кубитов-флаксоиумов с высокой точностью выполнения логических операций (*Moskalenko I.N., Simakov I.A., Abramov N.N. et al. High fidelity two-qubit gates on fluxoniums using a tunable coupler // Quantum Inf 8, 130. 2022. <https://doi.org/10.1038/s41534-022-00644-x>*), изготовленных в НОЦ «ФМНС» МГТУ им. Н.Э. Баумана

В результате проведенной работы в 2019 г. был реализован алгоритм Гровера на двух кубитах, продемонстрировавший возможность реализации всех необходимых логических операций для универсального квантового процессора: инициализации, одно- и двухкубитных операций и считывания с удовлетворительным для небольших алгоритмов уровнем ошибок. В 2021 г. был продемонстрирован сверхпроводящий чип с 25 перестраиваемыми кубитами-трансмонами, а также получены высокоточные одно- и двухкубитные вентили с точностью соответственно 99,55 и 99,23 % на кубитах-флаксонаумах. Оптические изображения (*a*) и эквивалентная электрическая схема устройства (*б*) приведена на рис. 1.145, где различным цветам соответствуют разные элементы схемы (емкостные и индуктивные элементы).

В 2021 г. были созданы квантовые симуляторы на основе сверхпроводящих кубитов для решения квантово-механических задач. Так, квантовая симуляция распространения фотонов в рамках модели Бозе — Хаббарда была выполнена за 2 ч, в то время как на классическом 138-ядерном вычислительном кластере на это ушло почти семь дней машинного времени, а также был создан квантовый симулятор на основе массива из 25 сверхпроводящих кубитов для демонстрации затухания мезоскопической флуктуации, имитирующей приближение к термодинамическому пределу⁷.

Тесты к лекции 1.25

1. Что такое кубит?

- а) единичный носитель информации в квантовом компьютере;
- б) бит информации в кубе;
- в) название квантовой пленки.

2. В чем заключается основное достоинство квантового компьютера?

- а) в так называемом квантовом параллелизме;
- б) в его очень небольшом размере;
- в) в очень небольшом энергопотреблении.

3. Что является особенностью кубита?

- а) диапазон суперпозиций. В этом диапазоне содержатся в различных соотношениях оба исходных состояния;
- б) возможность создания квантового компьютера с очень небольшим энергопотреблением;
- в) возможность организации последовательных вычислений.

4. С каким количеством чисел можно одновременно произвести математические операции, если число кубитов равно k ?

⁷ Fedorov G.P. et al. Photon transport in a Bose-Hubbard chain of super-conducting artificial atoms // Physical Review Letters. 2021. Vol. 126. No. 18. Pp. 180503.

- а) можно провести математические операции с 2^k числами одновременно;
- б) можно провести математические операции с $2k$ числами одновременно;
- в) можно провести математические операции с k^2 числами одновременно.

5. Что представляет собой квантовый параллелизм?

- а) вычислительный процесс, при котором в квантовом компьютере определяются выходные значения всех входных состояний;
- б) параллельное выделение квантовых частиц в микромире;
- в) процесс образования двух пар частиц, связанных между собой.