Факультет физики

НИУ ВШЭ

Москва
2024

Квантовые вычисления: Начало

Докладчик: Малиницкий Дмитрий

Квантовая механика vs Классическая механика

Классическая механика

Описывает движение объектов на макроскопических масштабах (например, движение планет, машин и т.д.). Законы предсказуемы и детерминированы.

Квантовая механика

Оперирует поведением частиц на субатомных масштабах. Для таких систем применимы принципы суперпозиции, запутанности и неопределённости, что делает их поведение непредсказуемым с точки зрения классической механики.

Основные положения квантовой механики

Волновая функция (ψ)

Описывает состояние квантовой системы. Волновая функция содержит полную информацию о системе, но не говорит напрямую, где находится частица. Лишь после измерения волновая функция "схлопывается" в одно из возможных состояний.

Оператор

Математический объект, который описывает измеримые величины (например, энергию или импульс). Операторы применяются к волновой функции для получения возможных значений измерений.

Уравнение Шрёдингера

Фундаментальное уравнение, которое описывает, как изменяется волновая функция со временем. Это аналог второго закона Ньютона для квантовых систем:

$$\hat{H}\psi = i\hbar\frac{\partial\psi}{\partial t}$$

где $\hat{H}$ — оператор Гамильтона (энергия системы), $\hbar$ — редуцированная постоянная Планка.

Разделение энергетических уровней

Энергетические уровни

В квантовой механике атомы и другие системы могут находиться на различных энергетических уровнях. Эти уровни возникают из-за дискретной природы энергии на квантовом уровне, которая определяется решением уравнения Шрёдингера для данной системы.Частицы могут переходить с одного уровня на другой, поглощая или излучая энергию.

Двухуровневая система

В упрощённой модели квантовой системы мы рассматриваем только два возможных энергетических состояния: основное и возбужденное. Такая система позволяет описывать базовые квантовые процессы и является ключевой для квантовых вычислений.

Кубит

Кубит — наименьшая единица информации в квантовом компьютере, аналогичная биту в классическом компьютере.

Состояние кубита

Как и бит, кубит может находиться в двух состояниях: $|0\rangle$ и $|1\rangle$. Однако, в отличие от бита, он может находиться в их **суперпозиции**, которая описывается волновой функцией:

$\mathbf{A|0\rangle + B|1\rangle}$, где **A** и **B** — амплитуды вероятностей, являющиеся комплексными числами.

Эти числа удовлетворяют условию: $\mathbf{|A|^2 + |B|^2 = 1}$.

Сфера Блоха

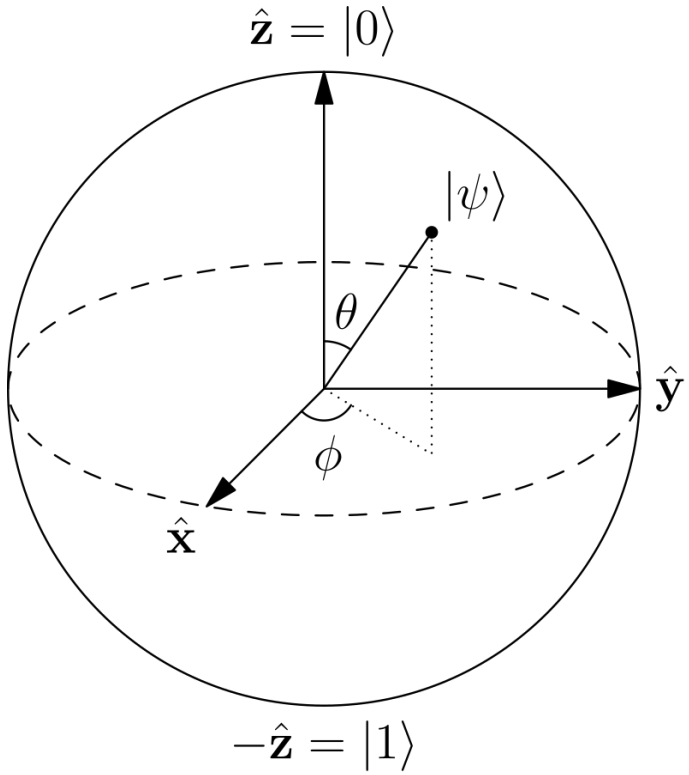
Сфера Блоха — это геометрическое представление состояния кубита. Каждое квантовое состояние кубита можно интерпретировать как точку на поверхности этой сферы. Полюса сферы представляют собой два собственных состояния кубита: |0⟩ (северный полюс) и |1⟩ (южный полюс).Состояние кубита описывается углами θ и φ:

Математическое описание

Кубит в суперпозиции можно представить как:

$$A = \cos\left(\frac{\theta}{2}\right), \quad B = e^{i\phi}\sin\left(\frac{\theta}{2}\right)$$

Здесь, **θ** — определяет, насколько состояние ближе к |0⟩ или |1⟩, а **φ** — фазовый сдвиг между этими состояниями.



Изменение квантового состояния

Квантовое состояние $|\Psi\rangle$ может изменяться во времени двумя принципиально различными путями:

Унитарная квантовая операция

Унитарные операции изменяют состояние кубита без потери информации. Эти операции реализуются с помощью квантовых вентилей и описываются унитарными матрицами, которые сохраняют норму волновой функции:

$$|\Psi'\rangle = U|\Psi\rangle$$

где **U** — унитарная матрица, а $|\Psi\rangle$ — исходное состояние кубита.
Важное свойство унитарных операций: $\mathbf{U^\dagger U = I}$, где $\mathbf{U^\dagger}$ — это эрмитово сопряжённая матрица.

Измерение (наблюдение)

При измерении квантового состояния происходит необратимый процесс. Суперпозиция разрушается, и система переходит в одно из собственных состояний с определённой вероятностью. Вероятность получить определённый результат измерения описывается квадратом модуля амплитуды вероятности.

Идея квантовых вычислений

Квантовая система из **L двухуровневых квантовых элементов (кубитов)** имеет 2^L линейно независимых состояний. Благодаря принципу суперпозиции, пространство состояний такого квантового регистра является 2^L мерным гильбертовым пространством. Операция в квантовых вычислениях соответствует **повороту вектора состояния регистра** в этом многомерном пространстве. Таким образом, квантовый компьютер имеющий **L кубитов** может одновременно обрабатывать 2^L классических состояний.

Физическая реализация кубитов

Кубиты могут быть реализованы с помощью различных физических систем, таких как:

- Поляризационные состояния фотонов
- Электронные состояния изолированных атомов или ионов
- Спиновые состояния ядер атомов
- И другие объекты с двумя квантовыми состояниями

Упрощённая схема вычисления

Процесс вычисления на квантовом компьютере выглядит так:

- Система кубитов инициализируется в начальном состоянии.
- Состояние системы изменяется с помощью унитарных преобразований.
- Выполняется измерение, которое даёт результат вычисления.

Кубиты играют роль проводов, а унитарные преобразования — роль логических блоков, как в классическом компьютере. Для выполнения вычислений достаточно двух базовых квантовых операций. Результат квантового алгоритма даётся с определённой вероятностью, но алгоритмы можно улучшить, чтобы эта вероятность приближалась к единице.

Сравнение с классическими компьютерами

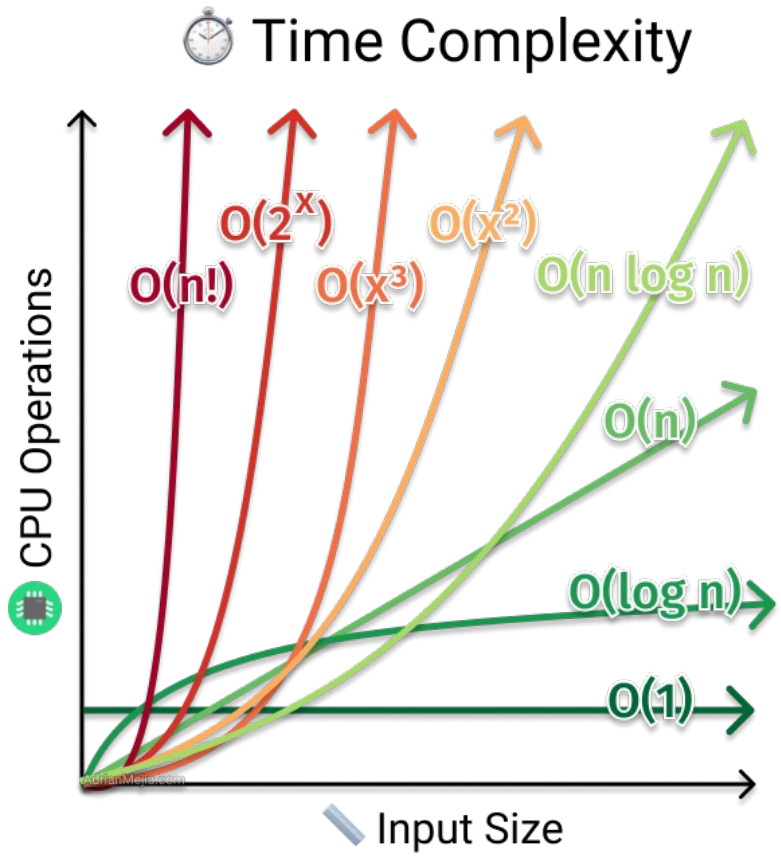
Квантовая система из **n кубитов** находится в суперпозиции всех 2^n базовых состояний, что позволяет обрабатывать их одновременно. Теоретически это даёт экспоненциальный прирост в скорости выполнения задач по сравнению с классическими алгоритмами. Например, **квантовый алгоритм Гровера** показывает квадратичное ускорение поиска в базе данных по сравнению с классическими методами.

Классическая сложность алгоритмов

Сложность алгоритма — это мера того, как изменяется время или количество шагов, необходимых для выполнения задачи, в зависимости от размера входных данных NN.

Асимптотическая сложность оценивается с помощью O-большое. Она показывает, как алгоритм ведёт себя при увеличении N. Примеры:

- **O(1)** — постоянное время, не зависит от размера входных данных.
- **O(N)** — линейная сложность, время выполнения пропорционально размеру данных.
- **O(N^2)**— квадратичная сложность, время растёт как квадрат размера данных.



Основные квантовые алгоритмы

Алгоритм Гровера

Предназначен для поиска решения уравнения f(x)=1, где 0≤x<N. Алгоритм находит решение за время O($\sqrt{N}$), что даёт квадратичное ускорение по сравнению с классическими методами.

Алгоритм Шора (Алгоритм Регева)

Позволяет разложить натуральное число n на простые множители за полиномиальное время O($log^3 n$) используя O(log n) кубитов. Это имеет значительное влияние на современные методы шифрования, которые основаны на сложности разложения больших чисел.

Не для всех классических алгоритмов возможно получить "квантовое ускорение". Более того, возможность достижения такого ускорения является редкостью для произвольных классических алгоритмов.

RSA (Rivest–Shamir–Adleman)

RSA — один из первых и наиболее широко используемых алгоритмов асимметричного шифрования. Он был разработан в 1977 году Рональдом Ривестом, Ади Шамиром и Леонардом Адлеманом.

Основные идеи RSA:

В основе RSA лежат два ключа: **открытый ключ** (для шифрования) и **закрытый ключ** (для расшифрования). Открытый ключ публикуется, а закрытый хранится в тайне. Чтобы зашифровать сообщение m, используют открытый ключ (n,e). Шифрованный текст вычисляется как:

$$c = m^e \mod n$$

где n — это произведение двух больших простых чисел, e — показатель открытого ключа, а c — зашифрованное сообщение.

Для расшифровки используют закрытый ключ (n,d), где d — это секретное число.

$$d \times e \equiv 1 \mod (p-1)(q-1)$$

$$m = c^d \mod n$$

Пример:

1.Пусть два простых числа p=3 и q=11. Вычисляем n=p×q=33

2.Выбираем открытый показатель e=3.

3.Находим d (закрытый показатель), который удовлетворяет условию

$$d \times e \equiv 1 \mod (p-1)(q-1)$$

В данном примере d=7.

Теперь для шифрования сообщения m=4, шифруем с помощью открытого ключа (33,3):

$$c = 4^3 \mod 33 = 64 \mod 33 = 31$$

Для расшифровки с использованием закрытого ключа (33,7):

$$m = 31^7 \mod 33 = 4$$

Квантовая криптография

Квантовая криптография — это область криптографии, которая использует принципы квантовой механики для создания систем безопасной передачи данных. В отличие от классических криптографических методов, безопасность квантовой криптографии основана на фундаментальных законах физики, таких как **принцип неопределённости Гейзенберга** и **коллапс волновой функции при измерении**. В квантовой криптографии использование квантовых состояний для передачи информации гарантирует, что любое вмешательство в передаваемый сигнал (например, попытка перехвата) изменит эти состояния. Это делает попытки перехвата заметными и позволяет обнаружить атаку.

Протоколы квантовой криптографии:

В квантовой криптографии используются квантовые протоколы для генерации и распределения ключей шифрования. Один из самых известных протоколов — **BB84**, предложенный в 1984 году Чарльзом Беннетом и Жилем Брассаром.

Преимущества квантовой криптографии:

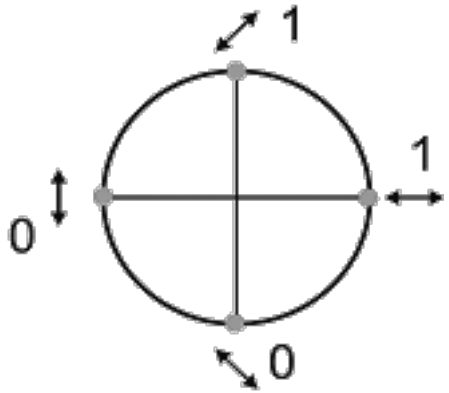
Обнаружение попыток перехвата.

Устойчивость к атакам, основанным на вычислительной мощности, включая атаки с использованием квантовых компьютеров.

Протокол BB84

Основная цель: безопасная передача ключей шифрования между двумя сторонами (Алиса и Боб), с гарантией обнаружения перехвата злоумышленником (Ева).
Основа протокола: передача информации с помощью кубитов (например, фотонов), которые могут быть поляризованы в одном из двух базисов:

- **Прямой базис**: горизонтальная ($|0\rangle$) или вертикальная ($|1\rangle$) поляризация.
- **Диагональный базис**: поляризация под углами 45° ($|+\rangle$) и 135° ($|-\rangle$).



Алгоритм распределения ключей

Участники:

- **Алиса** (отправитель) — должна передать ключ Бобу.
- **Боб** (получатель) — принимает ключ от Алисы.
- **Ева** (злоумышленник) — пытается перехватить ключ.

Этапы формирования ключа:

1.Выбор состояния и отправка:

Алиса случайным образом выбирает базис (прямоугольный или диагональный) и поляризацию фотона (0 или 1).

Фотоны передаются по квантовому каналу.

2.Измерение Бобом:

Боб случайно выбирает базис для каждого фотона (прямоугольный или диагональный) и измеряет его.

3.Открытый обмен базисами:

Боб сообщает, в каком базисе он провёл измерение, но не раскрывает результаты.

Алиса сообщает, где базис совпал с её выбором, и только эти данные сохраняются для ключа.

Просеивание и оценка безопасности

Формирование ключа:

- Только те измерения, где базисы Алисы и Боба совпали, используются для формирования ключа. Эти данные превращаются в биты (0 или 1).
- Примерно 50% данных отбрасывается. Оставшаяся часть данных — это «просеянный ключ».

Оценка безопасности:

- Если в канале связи нет шума или перехвата, Алиса и Боб получают полностью коррелированный ключ.
- В случае перехвата Евой, ошибки измерений у Боба могут выявить наличие вмешательства.

Обнаружение перехвата:

- Ева не может точно измерить фотоны без искажений, так как не знает базисов. Если она выберет неправильный базис, это приведёт к искажениям в измерениях Боба.

Пример распределения ключей

Последовательность фотонов Алисы	↕	↗	↗	↔	↖	↕	↕	↔	↔
Последовательность анализаторов Боба	+	x	+	+	x	x	x	+	x
Результаты измерений Боба	0	0	1	1	1	0	1	1	0
Анализаторы выбраны верно	да	да	нет	да	да	нет	нет	да	нет
Ключ	0	0		1	1			1	

Алиса передала последовательность фотонов.
Боб использовал случайные анализаторы для измерений.
После обмена базисами Алиса и Боб оставляют только те измерения, где их базисы совпали, и из этих данных формируют ключ.

Текущее состояние квантовых вычислений (2024)

Прогресс квантовых компьютеров:

В 2024 году квантовые вычисления достигли значительного прогресса благодаря крупным технологическим компаниям и научным институтам (Google, IBM, D-Wave, Rigetti и др.).

Увеличение числа кубитов: Современные квантовые процессоры уже могут оперировать сотнями кубитов. Google и IBM разрабатывают квантовые системы с более чем 1000 кубитов, что позволяет проводить сложные вычисления.

Квантовая устойчивость: Разрабатываются методы коррекции квантовых ошибок, что делает системы более надёжными и устойчивыми к шумам.

Области применения:

Квантовые алгоритмы, такие как **Гровера** и **Шора**, продолжают привлекать внимание благодаря их потенциалу для ускорения вычислений в области криптографии, химии, оптимизации и моделирования сложных систем.

Квантовое превосходство:

Эксперимент Google по квантовому превосходству в 2019 году продемонстрировал вычислительные задачи, которые классическим компьютерам было бы сложно решить. В 2024 году продолжаются разработки в этом направлении, расширяя область квантовых вычислений.

Современное состояние квантовой криптографии (2024)

Применение квантовой криптографии:

Квантовая криптография, особенно **протокол BB84**, активно применяется для **распределения ключей**(QKD) в защищённых каналах связи. Страны и компании внедряют квантовые сети для безопасной передачи данных.

Примеры внедрения квантовой криптографии в реальных проектах — квантовые сети в Китае и Европе, которые обеспечивают безопасность в критически важных системах (например, для банков и правительственных учреждений).

Защита от квантовых атак:

Квантовая криптография позволяет защититься от атак квантовых компьютеров, которые могут взломать классические криптографические алгоритмы (например, RSA) с помощью **алгоритма Шора**.

Разрабатываются гибридные системы шифрования, которые сочетают квантовую и классическую криптографию для повышения безопасности в долгосрочной перспективе.

Проблемы и вызовы:

Хотя квантовая криптография обещает высокую безопасность, её масштабное внедрение требует значительных инвестиций в инфраструктуру, и многие проекты находятся на стадии экспериментов.

Важной проблемой остаётся обеспечение долгосрочной надёжности квантовых каналов в условиях шума и помех.

Перспективы

Опасности для современной криптографии:

В ближайшие годы (десятилетия) **квантовые компьютеры** смогут взломать классические криптографические системы, такие как RSA, используя алгоритм Шора, что ставит под угрозу современную интернет-безопасность.

Необходима разработка **постквантовых криптографических алгоритмов**, которые смогут выдержать атаки квантовых компьютеров.

Постквантовая криптография:

Ведутся активные исследования и стандартизация новых криптографических систем, которые защищены от квантовых атак (NIST проводит конкурс на выбор постквантовых алгоритмов).

Постквантовые алгоритмы будут постепенно внедряться в правительственные и коммерческие системы для обеспечения долгосрочной безопасности.

Будущее квантовых вычислений:

Успех квантовых технологий будет зависеть от способности научного сообщества решить технические проблемы, такие как коррекция ошибок и улучшение кубитных процессоров.