Квантовые вычисления рассматривают вычислительные мощности и другие свойства компьютеров, спроектированные на основе принципов квантовой механики

Квантовое состояние представляет собой суперпозицию классических состояний, которые можно измерить или применить унитарную операцию. Представим, что некая физическая система, которая может быть в N различных классических состояний. Назовем эти состояния |1>, |2>, …,|N>. Грубо говоря, под классическим понимается состояние, в котором система может быть измерена. Квантовое состояние |φ> это суперпозиция классических состояний: |φ> = α1|1> + α2|2> +…+ αN|N>, где αi – комплексное число. Таким образом, можно сказать, что система в квантовом состоянии находится во всех классических состояниях одновременно. Говоря математическим языком, состояние |1>, ..., |N> формирует ортонормальный базис N-размерного Гильбертова пространства, в котором квантовое состояние |φ> является вектором. С квантовым состоянием можно проводить 2 операции: измерить и изменить унитарно, без измерения.

Задача обработки квантовой информации состоит в решении определенного класса проблем, которых не могут решить классические компьютеры за приемлемое время.

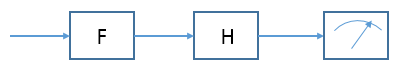
Перечислим 3 основных мотиваций изучения квантовых компьютеров:

Процесс миниатюризации, который сделал современные компьютеры мощными и дешевыми, практически достиг микро-уровней, на которых проявляются квантовые эффекты. Производители чипов склонны перейти к большим размерам, чтобы подавить эти эффекты, но стоит попробовать сработаться с ними, открывая путь к дальнейшей миниатюризации.

Использование квантовых эффектов позволяет значительно ускорить некоторые вычисления и даже реализовать некоторые вещи, недоступные классическим компьютерам. Основная цель данной работы – демонстрация этих идей.

Одна из задач теории компьютерной науки звучит как «выявить возможности и ограничения самого допустимо-сильного вычислительного устройства, которое может позволить нам природа».

Возьмем кубит вида:  
|ψ⟩=12–√|0⟩+12–√|1⟩  
то есть коэффициенты c0=c1=12–√c0=c1=12 и вероятность при измерении кубита получить единицу равна вероятности получить ноль и равна 50% поскольку ∣∣∣12–√∣∣∣2=0.5|12|2=0.5. Подадим его на вход следующей схемы.



Операция F изменяет коэффициенты c0,c1c0,c1  кубита следующим образом:

|ψ⟩=[12–√(−1)f(0)]|0⟩+[12–√(−1)f(1)]|1⟩|ψ⟩=[12(−1)f(0)]|0⟩+[12(−1)f(1)]|1⟩

По сути F есть квантовомеханический аналог классического черного ящика f. Заметьте, что измерив кубит сразу за блоком F вне зависимости от вида функции f(x)f(x)  мы продолжим получать 50%-ю вероятность нуля и единицы, поскольку она может изменить только знак, а  ∣∣∣12–√∣∣∣2=∣∣∣−12–√∣∣∣2=0.5|12|2=|−12|2=0.5.

Применяя к кубиту [преобразование Адамара](https://en.wikipedia.org/wiki/Quantum_gate#Hadamard_gate) H, мы опять меняем амплитуды вероятностей и получаем:

|ψ⟩=12[(−1)f(0)+(−1)f(1)]|0⟩|ψ⟩=12[(−1)f(0)+(−1)f(1)]|0⟩ +12[(−1)f(0)−(−1)f(1)]|1⟩+12[(−1)f(0)−(−1)f(1)]|1⟩

Теперь можно измерять кубит последним блоком. Убедитесь, что для константных функций мы получим c0=1,c1=0c0=1,c1=0, а для сбалансированных наоборот c0=0,c1=1c0=0,c1=1. То есть если в результате измерения будет ноль — функция константная, если единица — сбалансированная.

Заметьте, что в отличие от классического случая, операция F выполнялась только один раз (на квантовом компьютере)), но мы можем однозначно сказать к какой категории относится функция (хотя ее конкретный вид остается неясным). Это пример так называемого квантового параллелизма. Теоретически мы можем получить экспоненциальный рост производительности при линейном росте количества кубит. Для описания двухкубитного состояния требуется уже четыре комплексных числа c00…c11c00…c11:

|ψ⟩=c00|00⟩+c01|01⟩+c10|10⟩+c11|11⟩|ψ⟩=c00|00⟩+c01|01⟩+c10|10⟩+c11|11⟩,

а для N-кубитного 2N2N чисел, то есть имеет место экспоненциальный рост.

Значимость алгоритма заключается в том, что с его помощью (при использовании квантового компьютера с несколькими сотнями логических кубитов) становится возможным взлом криптографических систем с открытым ключом. К примеру, RSA использует открытый ключ M,M,являющийся произведением двух больших простых чисел. Один из способов взломать шифр RSA — найти множители M.M. При достаточно большом MM это практически невозможно сделать, используя известные классические алгоритмы. Наилучшие из известных классических детерминированных доказанных алгоритмов факторизации, такие как метод квадратичных форм Шенкса и алгоритм Полларда — Штрассена, требуют времени порядка  M1/4. Так же метод квадратичных форм Шенкса может работать за время порядка M1/5 если верна Гипотеза Римана. Среди вероятностных алгоритмов лидером факторизации является специальный метод решета числового поля, который способен с вероятностью 1/2 найти простой делитель. Алгоритм Шора, используя возможности квантовых компьютеров, способен произвести факторизацию числа не просто за полиномиальное время, а за время, не намного превосходящее время умножения целых чисел (то есть практически так же быстро, как происходит само шифрование). Таким образом, реализация масштабируемого квантового компьютера поставила бы крест на большей части современной криптографической защиты.

Алгоритм Шора имеет вероятностный характер. Первый источник случайности встроен в классическое вероятностное сведение разложения на множители к нахождению периода некоторой функции. Второй источник появляется из необходимости наблюдения квантовой памяти, которое также даёт случайные результаты.