

Квантовые вычисления. Аксиоматическая модель. Примеры алгоритмов.

Сергей Тихомиров

Санкт-Петербургский Государственный Университет.



Санкт-Петербургский
государственный
университет



Факультет математики и
компьютерных наук



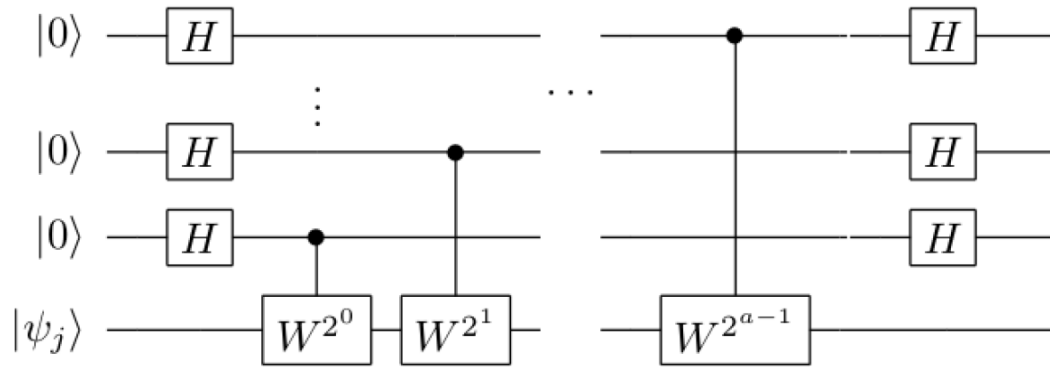
Исследовательская
лаборатория им. П. Л.
Чебышева



Leonhard Euler
International Mathematical Institute
in Saint Petersburg

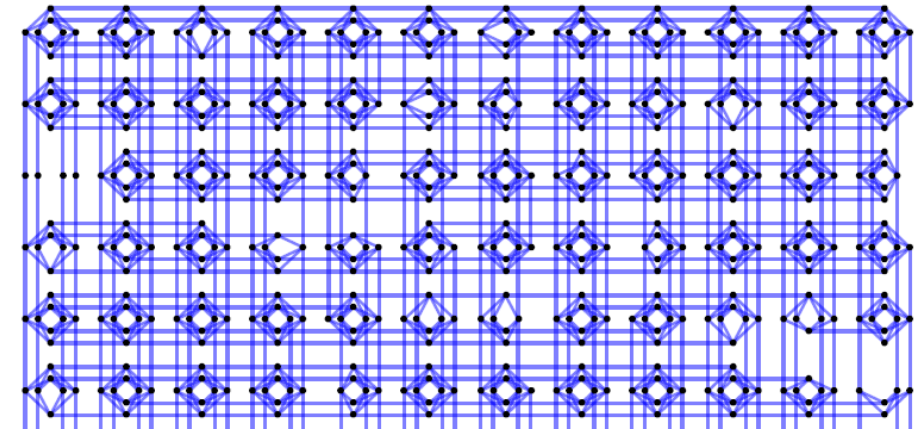
Модели квантовых вычислительных устройств

Схемные квантовые компьютеры



- Основаны на кубитах и операциях над ними
- n кубит соответствует $\sim 2^n$ вещественных чисел
 - Нет оператора присваивания
- Одновременное проведение вплоть до 2^n операций
- Имеют вероятностную природу
- Алгоритм Шора (преобразование Фурье)
- Алгоритм Гровера (Поиск)
- Алгоритм HHL (операции над матрицами)
- ~ 50 кубит

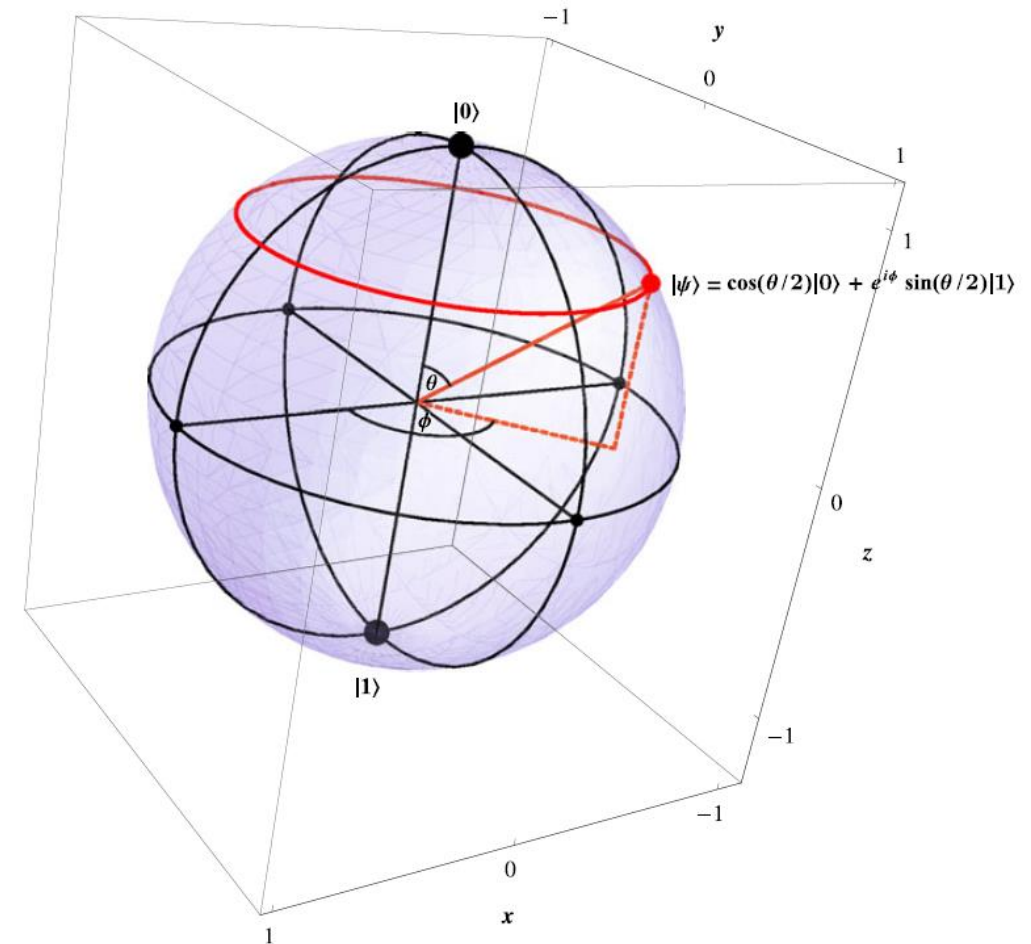
Адиабатические квантовые компьютеры



- Основаны на минимизации функционалов энергии
- Реализация D-Wave основана на минимизации билинейных функционалов
- Задачи булевой разрешимости
- Дискретная оптимизация
- Комбинаторные задачи
- Могут использоваться для сэмплирования
 - Распределение Гиббса
- ~ 2000 (5000) кубит

Кубит

- $|\psi\rangle = a|0\rangle + b|1\rangle$ -- состояние квантового бита
 $a, b \in \mathbb{C}$
 $|0\rangle, |1\rangle$ -- базисные векторы
 $|\psi\rangle \in \mathbb{C}^2$
- $|a|^2 + |b|^2 = 1$
- $a|0\rangle + b|1\rangle \sim e^{i\gamma}(a|0\rangle + b|1\rangle)$
- $|\psi\rangle = e^{i\gamma}(\cos \theta/2 |0\rangle + e^{i\phi} \sin \theta/2 |1\rangle)$
- Сфера Блоха (Bloch)
- Состояние задается 2-мя вещественными числами
- В «каком-то смысле» кубит находится
 - в состоянии $|0\rangle$ с вероятностью $|a|^2$
 - в состоянии $|1\rangle$ с вероятностью $|b|^2$



Несколько кубит

- $|\psi\rangle = c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle$

$$|\psi\rangle = c_0|00\dots 0\rangle + c_1|00\dots 1\rangle + \dots + c_{2^n-1}|11\dots 1\rangle = \sum_{i=0}^{2^n-1} c_i|i\rangle$$

- Условие $\sum_{i=0}^{2^n-1} |c_i|^2 = 1$

- $|\psi\rangle \sim e^{i\gamma}|\psi\rangle$

- Сколько вещественных чисел нужно для представления?

- $r(n) = 2 * 2^n - 2$

- Первый источник «экспоненциального превосходства»

- $r(2) = 6, \quad r(1) = 2$

двухкубитное состояние богаче, чем 2 однокубитных

- $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ -- тензорное произведение

Запутанность. Примеры.

- Прямое произведений

$$|\phi\rangle \otimes |\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a \begin{pmatrix} c \\ d \end{pmatrix} \\ b \begin{pmatrix} c \\ d \end{pmatrix} \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix} = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle$$

- Не представимое в виде прямого произведения является **запутанным**
- Пример: $\frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$

Операции над кубитами. Унитарные операторы.

- Уравнение Шредингера

$$i\hbar \frac{\partial |\psi(t)\rangle}{\partial t} = \mathcal{H}|\psi(t)\rangle$$

- $|\psi(t)\rangle = U(t)|\psi(0)\rangle = \exp(-i\mathcal{H}t/\hbar)|\psi(0)\rangle.$
- \mathcal{H} – самосопряженный оператор
- U – унитарный оператор
 - Вопрос какие унитарные операторы разрешает устройство?
- Можно применять унитарные операторы к малому числу кубит
- Важное замечание – унитарные операторы обратимы
Квантовые вычисления – обратимые вычисления

Измерения

- H – самосопряженный оператор
- λ_i – собственные числа
 V_i – соответствующие собственные пространства
- «Произвести измерение по отношению к H »
 - С вероятностью $|P_i|\psi\rangle|^2$ переходит в состояние $P_i|\psi\rangle$
 - Получаем в результате измерения λ_i
- Измерение кубита
 - $|\psi\rangle = a|0\rangle + b|1\rangle$
с вероятностью $|a|^2$ результат измерения 0, переходит в состояние $|0\rangle$;
с вероятностью $|b|^2$ результат измерения 1, переходит в состояние $|1\rangle$;
 - $$|\psi\rangle = c_0|00\dots 0\rangle + c_1|00\dots 1\rangle + \dots + c_{2^n-1}|11\dots 1\rangle = \sum_{i=0}^{2^n-1} c_i|i\rangle$$

с вероятностью $\sum_{i=0}^{2^{n-1}-1} |c_i|^2$ результат измерения 0, переходит в состояние $\sum_{i=0}^{2^{n-1}-1} \frac{c_i}{\sum_{i=0}^{2^{n-1}-1} |c_i|^2} |i\rangle$
с вероятностью $\sum_{i=2^{n-1}}^{2^n-1} |c_i|^2$ результат измерения 1, переходит в состояние $\sum_{i=2^{n-1}}^{2^n-1} \frac{c_i}{\sum_{i=2^{n-1}}^{2^n-1} |c_i|^2} |i\rangle$

Обратимые вычисления

- Важное замечание – унитарные операторы обратимы
Квантовые вычисления – обратимые вычисления.
- Классические вычисления – не все обратимо
 - $b := a$ – необратимо
 - $(a, b) \rightarrow (a, a \text{ and } b)$ – необратимо
 - $(a, b) \rightarrow (a, a \text{ or } b)$ – необратимо
 - $(a, b) \rightarrow (a, a \text{ xor } b)$ – обратимо
- Все что можно сделать классическими **обратимыми** вычислениями можно сделать и квантовыми

1-кубитные «гейты»

- U – унитарная матрица 2×2 действующая на 1м кубите
- Тогда на n -кубитах происходит операция – тензорное произведение $U \otimes Id \otimes Id \otimes \dots \otimes Id$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \begin{aligned} H|0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ H|1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$

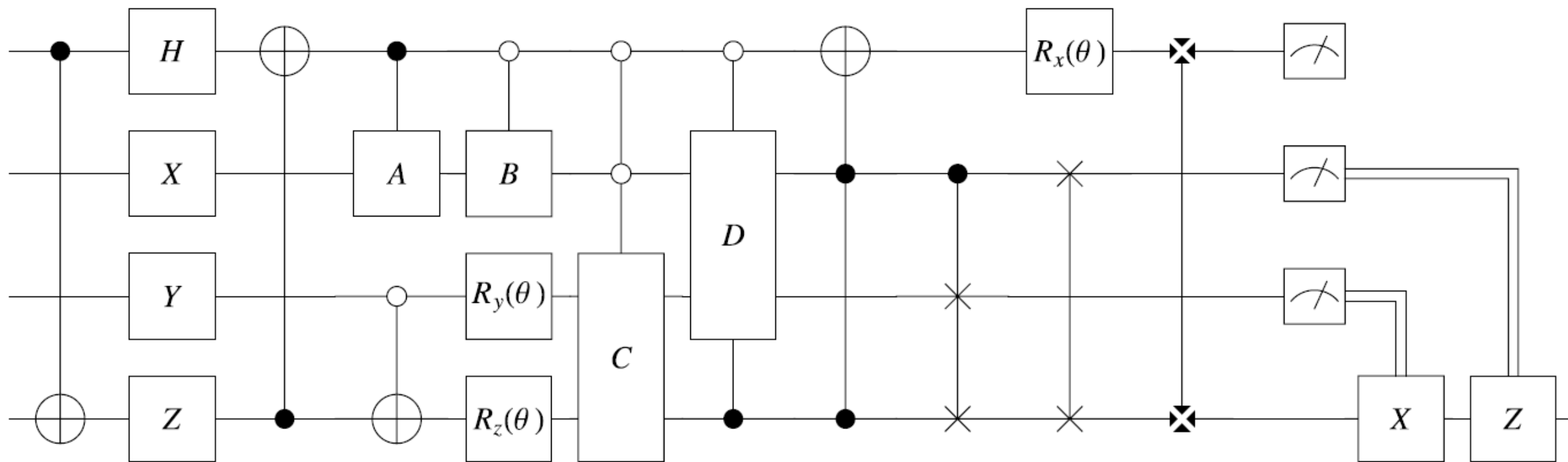
$$|\psi\rangle = c_0|00\dots 0\rangle + c_1|00\dots 1\rangle + \dots + c_{2^n-1}|11\dots 1\rangle = \sum_{i=0}^{2^n-1} c_i|i\rangle$$

$$\begin{aligned} H \otimes Id \otimes Id \otimes \dots \otimes Id |\psi\rangle &= H \otimes Id \otimes Id \otimes \dots \otimes Id (|0\rangle (c_0|0\dots 0\rangle + c_1|0\dots 1\rangle + \dots + c_{2^{n-1}-1}|1\dots 1\rangle) + \\ &\quad |1\rangle (c_{2^{n-1}}|0\dots 0\rangle + c_{2^{n-1}+1}|0\dots 1\rangle + \dots + c_{2^n-1}|1\dots 1\rangle)) = \\ &= \frac{1}{\sqrt{2}} ((c_0 + c_{2^{n-1}})|00\dots 0\rangle + (c_0 - c_{2^{n-1}})|10\dots 0\rangle + \sum (c_i + c_{i+2^{n-1}})|0i\rangle + (c_i - c_{i+2^{n-1}})|1i\rangle) \end{aligned}$$

- Одновременно происходит 2^n сложений-вычитаний – параллелизм

Quantum circuit. Квантовая схема.

- С многокубитными гейтами то же самое
- Программа – это программа 😊



Controlled-гейты

- CNOT(q1, q2)

Если $q1 == 0$ – ничего не делать

Если $q1 == 1$ – заменить $q2$ на $\text{not } q2$

$$|00\rangle \xrightarrow{\text{CNOT}} |00\rangle$$

$$|01\rangle \xrightarrow{\text{CNOT}} |01\rangle$$

$$|10\rangle \xrightarrow{\text{CNOT}} |11\rangle$$

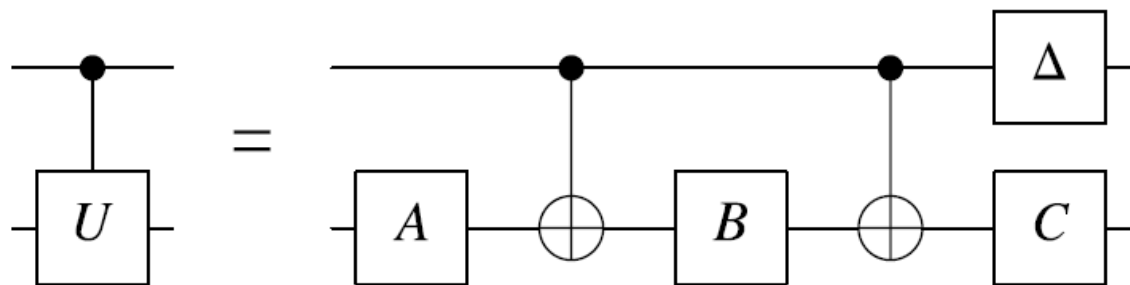
$$|11\rangle \xrightarrow{\text{CNOT}} |10\rangle$$

- Controlled-U(q1, q2)

Если $q1 == 0$ – ничего не делать

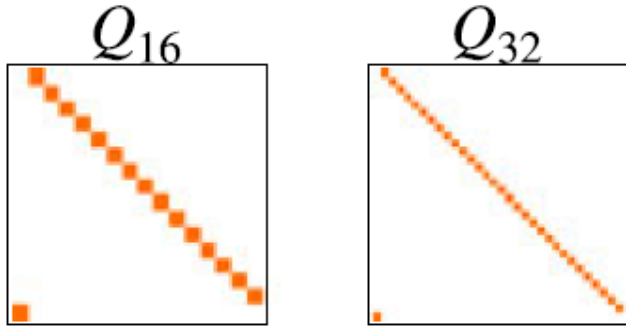
Если $q1 == 1$ – заменить $q2$ на $Uq2$

$$\text{controlled-}U \equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{11} & U_{12} \\ 0 & 0 & U_{21} & U_{22} \end{pmatrix}$$

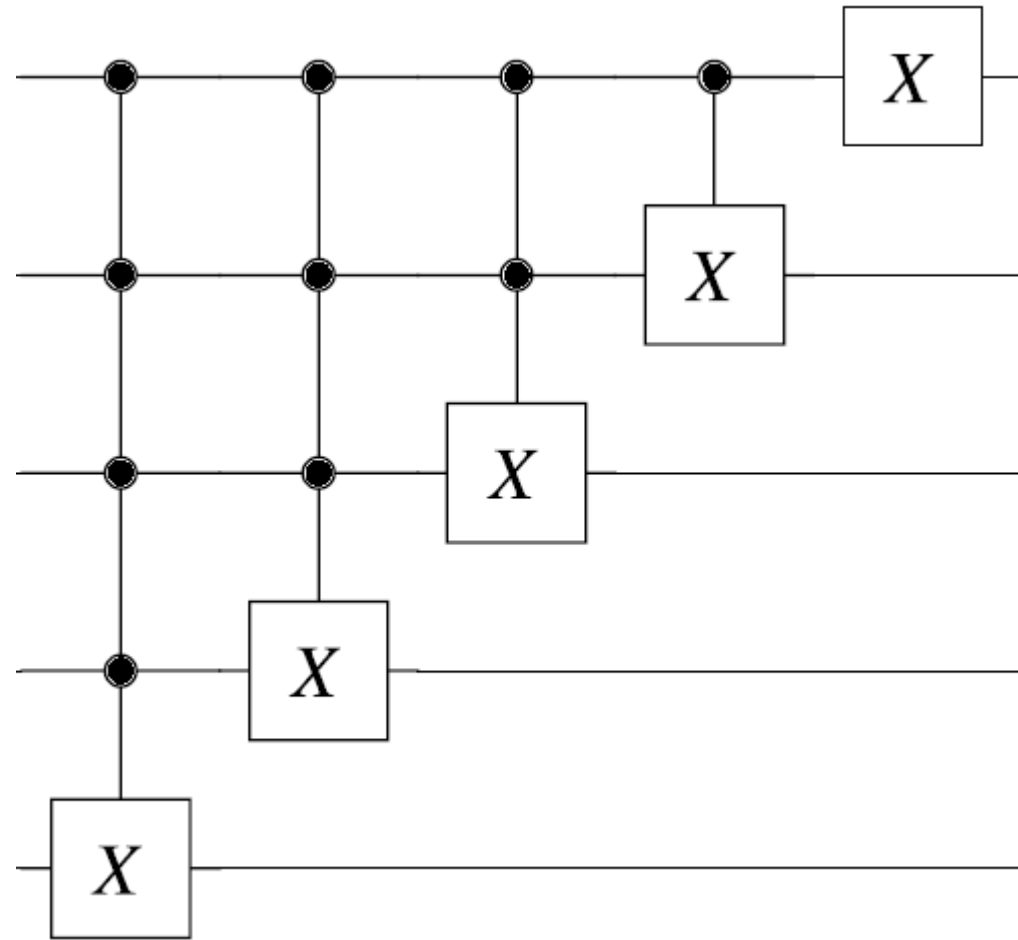


Квантовая перестановка. Q_{2^n}

- $Q_{2^n}: |k\rangle \rightarrow |k+1\rangle$.

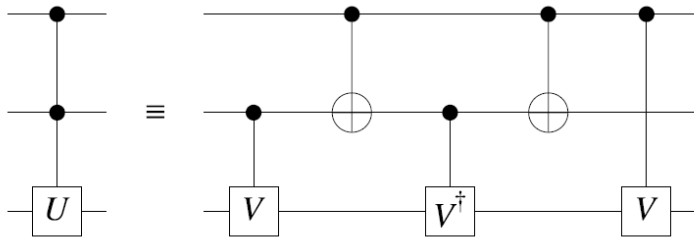


- X – это NOT
- Почему схема работает?
- Как реализовать C-C-C-...-X?
- Сколько операций понадобится для n ?



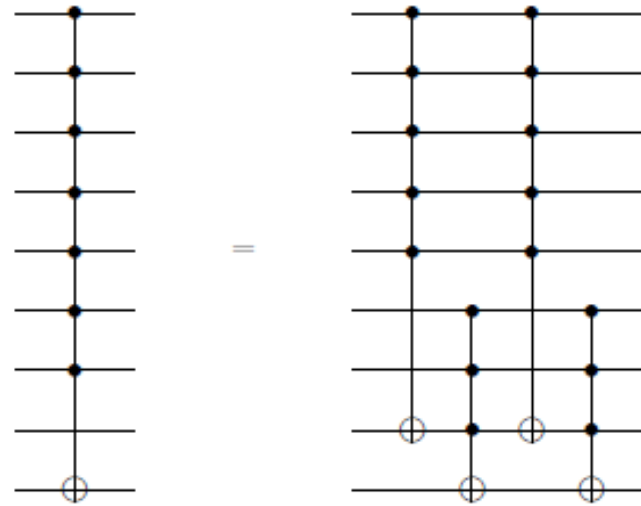
Варианты реализации. Q_2^n

- Без дополнительных кубит



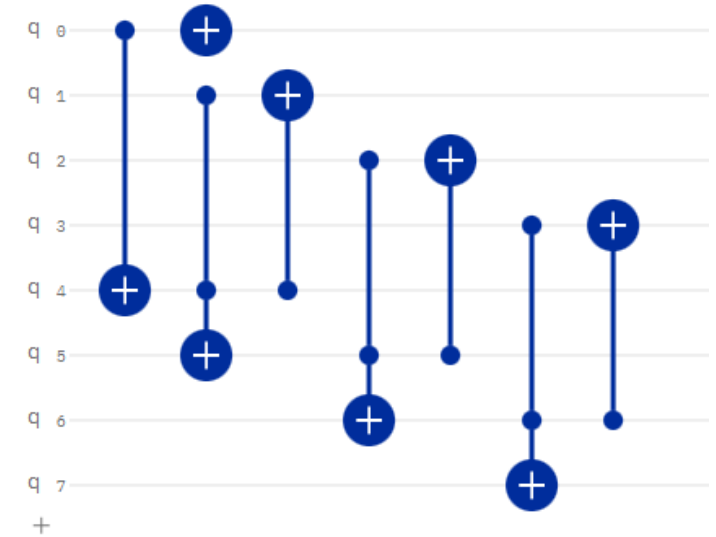
Экспоненциальное время

- Один дополнительный кубит



Квадратичное время

- $n-1$ дополнительных кубит

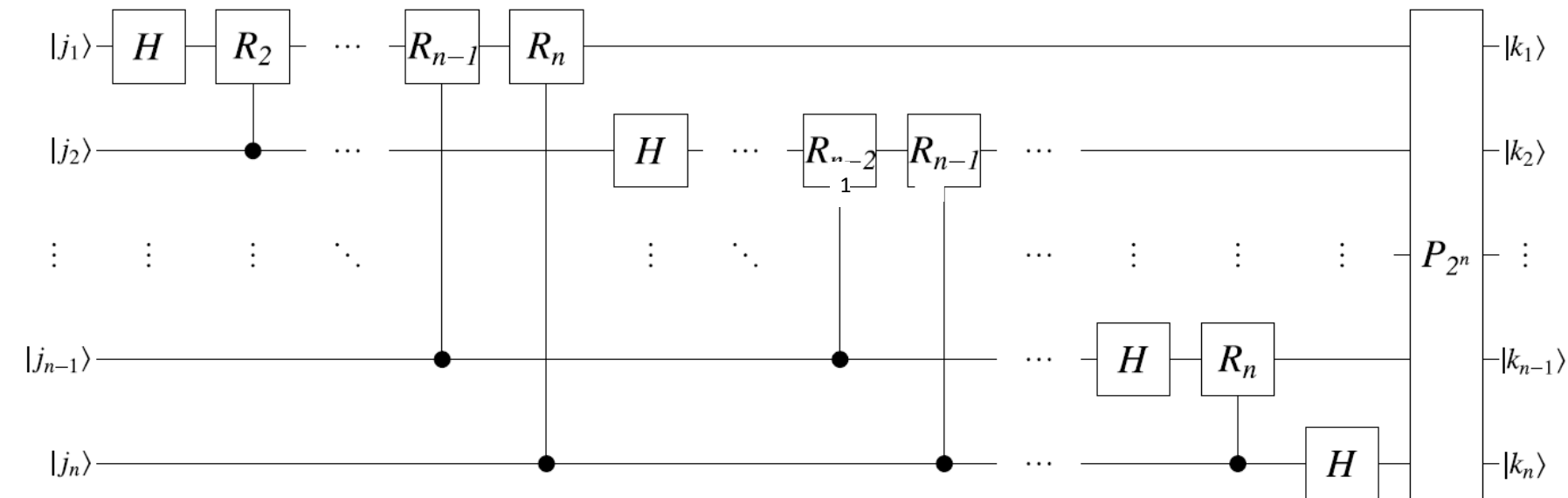


линейное время

Квантовое преобразование Фурье

- Квантовое преобразование Фурье – линейный оператор

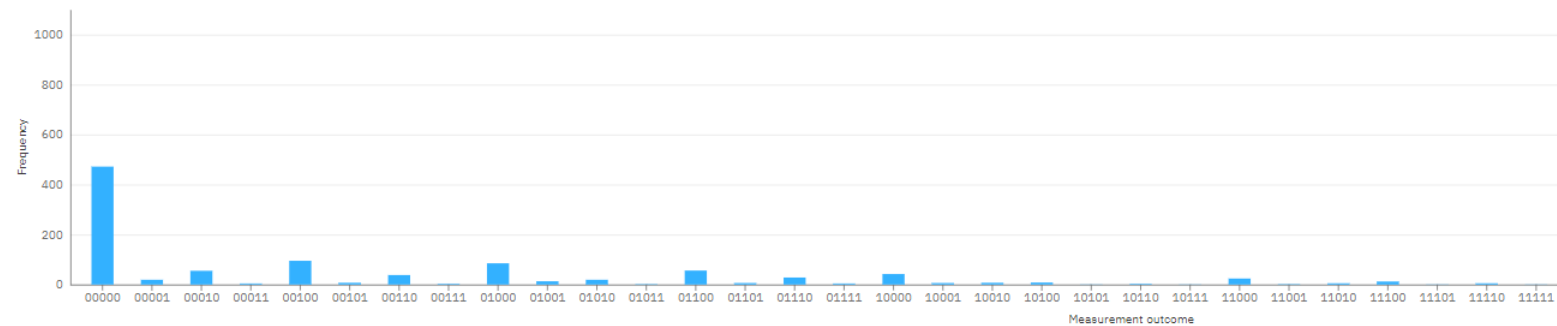
$$\text{QFT}_{2^n} := \frac{1}{\sqrt{2^n}} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega^1 & \omega^2 & \dots & \omega^{(2^n-1)} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(2^n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{(2^n-1)} & \omega^{(2^n-1)2} & \dots & \omega^{(2^n-1)(2^n-1)} \end{pmatrix} \quad \omega = \exp(2\pi i / N)$$



$$R_n = \begin{pmatrix} 1 & 0 \\ 0 & \exp(2\pi i / 2^n) \end{pmatrix}$$

QFT. 5 кубит. ННННН

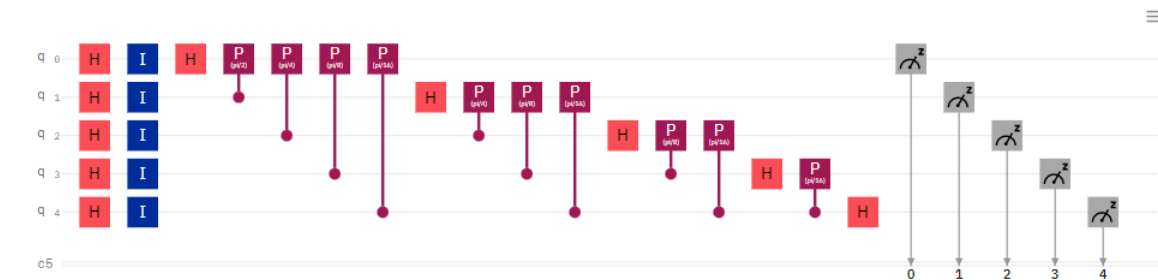
Histogram



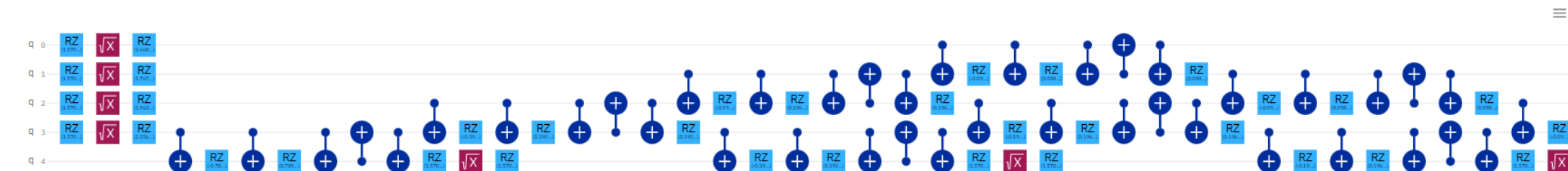
Circuit

Diagram Qasm Qiskit

Original circuit



Transpiled circuit



Квантовый поиск. Постановка задачи.

Дана функция

$$f_t(x) = \begin{cases} 0 & \text{if } x \neq t \\ 1 & \text{if } x = t \end{cases}$$

Задача найти t .

- Классический алгоритм – перебор $O(N)$
- Вопрос – можно ли на квантовом компьютере быстрее?

Квантовый поиск. Алгоритм.

- Что такое «квантовое f »?
- Оператор $\mathbb{I}_t = Id - 2|t\rangle\langle t|$
 $\mathbb{I}_t|x\rangle = |x\rangle \quad x \neq t$
 $\mathbb{I}_t|x\rangle = -|x\rangle \quad x = t$
- Мы считаем, что нам дан \mathbb{I}_t
- Пусть $|s\rangle$ -- начальное состояние и оператор U :

$$\langle t|U|s\rangle \neq 0$$

- Пример

$$|s\rangle = |0\rangle$$

$$U = H \otimes \dots \otimes H$$

$$\langle t|U|s\rangle = \langle t|\frac{1}{\sqrt{2^n}}\sum |x\rangle = \frac{1}{\sqrt{2^n}}$$

Квантовый поиск. Алгоритм.

- Даны $\mathbb{I}_t, \mathbb{I}_s, U$
- Рассмотрим

$$Q = -U\mathbb{I}_sU^\dagger\mathbb{I}_t$$

- Выполним (для наших U и $|s\rangle$)

$$|\psi\rangle = Q^k U|s\rangle$$

$$k = \frac{\pi}{4}\sqrt{N}$$

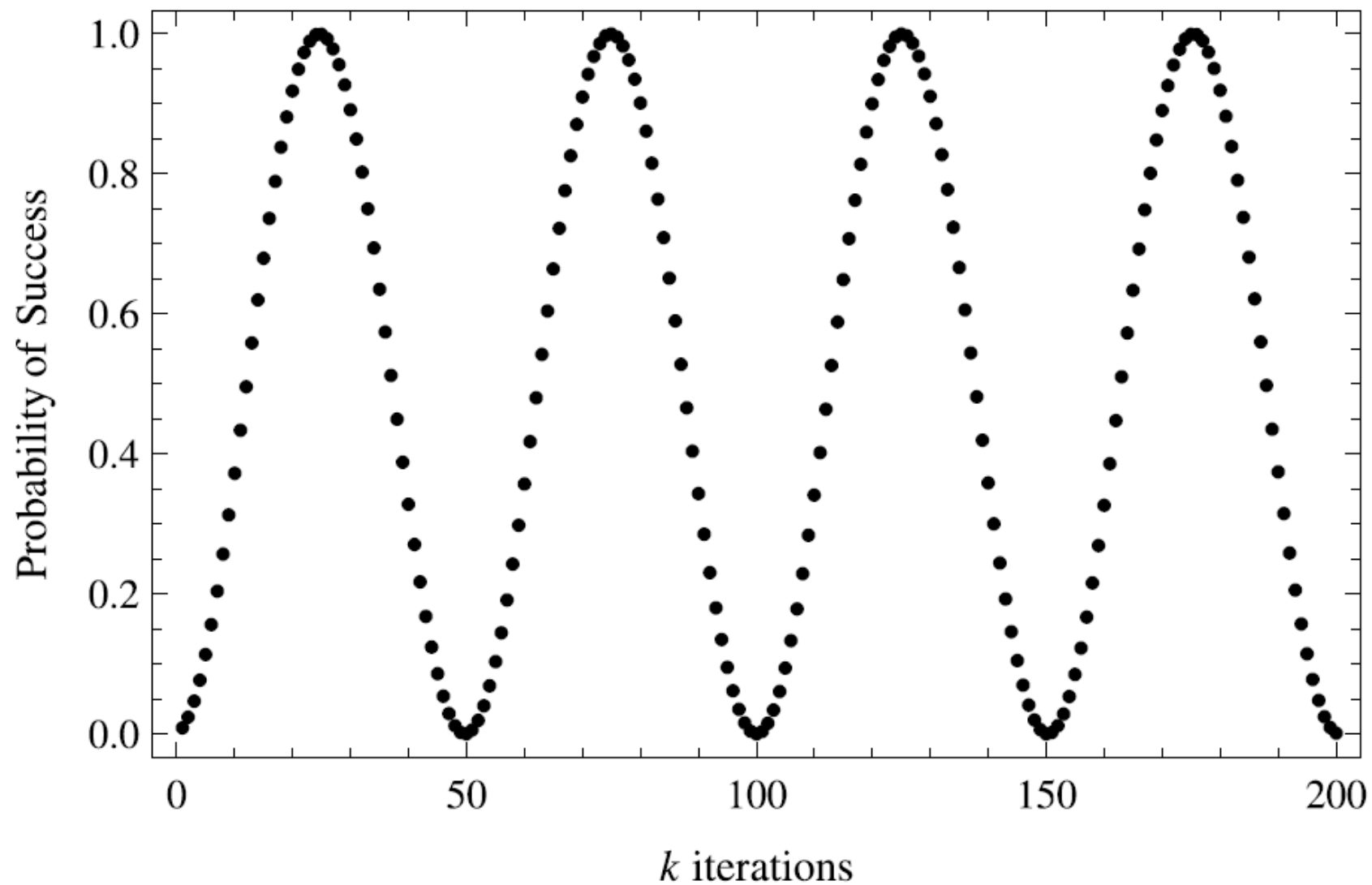
- Измерим полученное состояние $|\psi\rangle$
- Результат с высокой вероятностью $|t\rangle$
- Почему работает?

Квантовый поиск. Почему работает.

- \mathbb{I}_t -- отражение относительно плоскости перпендикулярной $|t\rangle$
- $U\mathbb{I}_sU^\dagger$ отражение относительно плоскости перпендикулярной $U|s\rangle$
- Их композиция – поворот на угол $2(\pi/2 - \alpha)$, где α – угол между $|t\rangle$ и $U|s\rangle$
- $\cos \alpha = \langle t|U|s \rangle = \sin(\pi/2 - \alpha) \sim \pi/2 - \alpha$
- После k итераций угол между $|t\rangle$ и $|\psi\rangle = Q^k U|s\rangle$ равен $\alpha - 2k(\pi/2 - \alpha)$
- И почти равен 0 при

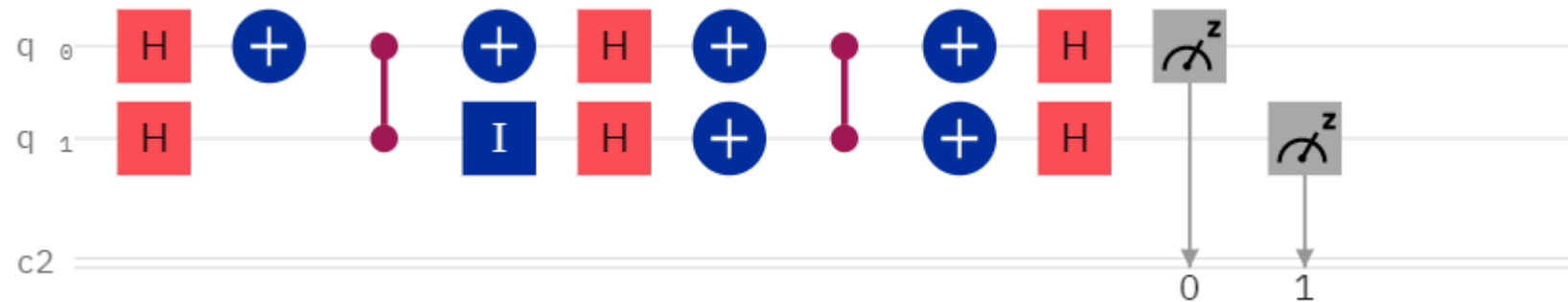
$$k = \frac{\alpha}{2\left(\frac{\pi}{2} - \alpha\right)} \sim \frac{\frac{\pi}{2}}{2\langle t|U|s\rangle} = \frac{\pi}{4}\sqrt{2^n} = \frac{\pi}{4}\sqrt{N}$$

Квантовый поиск. Вероятность успеха.

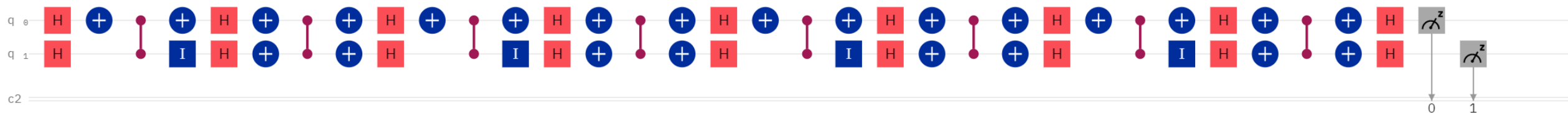


Алгоритм Гровера. Схема

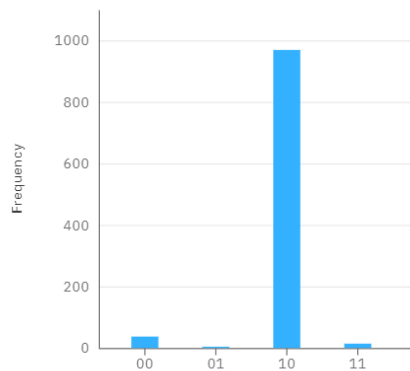
1 итерация



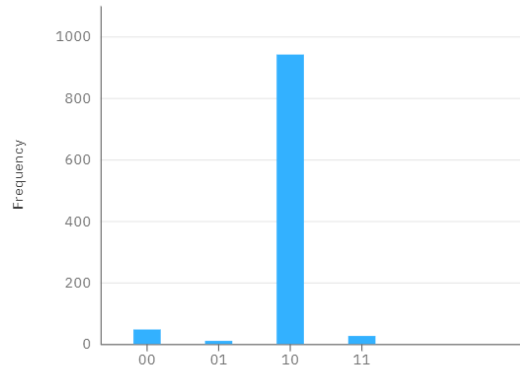
4 итерации



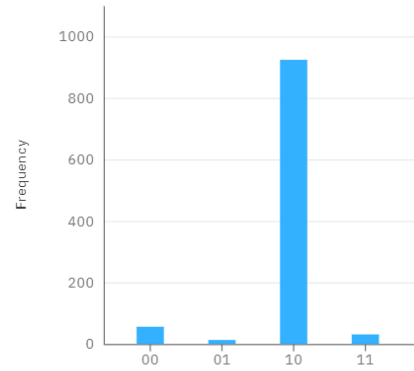
1 итерация



4 итерации



7 итераций



Какие еще есть квантовые алгоритмы?

- Алгоритм Шора. Разложение числа в произведение двух.
Суть ускорения – квантовое преобразование Фурье
- Запись данных в квантовый компьютер QRAM
- Симуляция Гамильтониана
- Решение линейных уравнений (алгоритм сложный – есть тонкости)
Запись данных занимает больше времени, чем решение уравнения.
Для разреженных – экспоненциальное ускорение по N .
Хуже чем классические алгоритмы по числу обусловленности.
- Сэмплирование из распределений,
например «ускорение MCMC»
Нужно «много» кубит
- Решение уравнений в частных производных
- <https://quantumalgorithmzoo.org/>

Задачи над которыми думаю я?

- Ускорение сэмплирования из Гаусовских полей
 - Вычислительная сложность сосредоточена в линейной алгебре
 - Неточность не так страшна, поскольку решается задача сэмплирования
- Моделирование волновых уравнений
 - Прикладной смысл – сейсмическая инверсия
 - Эволюция несамосопряженных операторов
 - Обратные задачи
- Теоретическая оценка влияния «неточности» квантовых компьютеров