Алгоритмы Дойча и Дойча-Йожи
(Deutsch-Jozsa algorithm)

Квантовые вычисления–2023

10 октября 2023 г.

Outline

Значение алгоритма

Классы задач

Класс P

Задачи, детерминированно решаемые за полиномиальное время

- максимальное паросочетание

Классы задач

Класс P

Задачи, детерминированно решаемые за полиномиальное время

- максимальное паросочетание
- проверка на простоту

Классы задач

Класс P

Задачи, детерминированно решаемые за полиномиальное время

- максимальное паросочетание
- проверка на простоту
- ...

Классы задач

Класс P

Задачи, детерминированно решаемые за полиномиальное время

- максимальное паросочетание
- проверка на простоту
- ...

Классы задач

Класс P

Задачи, детерминированно решаемые за полиномиальное время

- максимальное паросочетание
- проверка на простоту
- ...

Класс NP

Задачи, недерминированно решаемые за полиномильное время.

Классы задач

Класс *P*

Задачи, детерминированно решаемые за полиномиальное время

- максимальное паросочетание
- проверка на простоту
- ...

Класс *NP*

Задачи, недерминированно решаемые за полиномильное время. или: Проверка решения полиномиальной длины за полиномиальное время

- выполнимость булевой формулы (SAT)?

Классы задач

Класс *P*

Задачи, детерминированно решаемые за полиномиальное время

- максимальное паросочетание
- проверка на простоту
- ...

Класс *NP*

Задачи, недерминированно решаемые за полиномильное время. или: Проверка решения полиномиальной длины за полиномиальное время

- выполнимость булевой формулы (SAT)?
- задача коммивояжера (TSP)?

Классы задач

Класс *P*

Задачи, детерминированно решаемые за полиномиальное время

- максимальное паросочетание
- проверка на простоту
- ...

Класс *NP*

Задачи, недерминированно решаемые за полиномильное время.
или: Проверка решения полиномиальной длины за полиномиальное время

- выполнимость булевой формулы (SAT)?
- задача коммивояжера (TSP)?
- разложение на простые числа?

Квантовые классы задач

Класс *EQP*

Задачи, решаемые на квантовом компьютере за полиномиальное время точно (с нулевой ошибкой)

Квантовые классы задач

Класс *EQP*

Задачи, решаемые на квантовом компьютере за полиномиальное время точно (с нулевой ошибкой)

$$P^A \subsetneq EQP^A$$

Алгоритм Дойча

Задача

Вход алгоритма: оракул U_f для $f : \{0,1\} \to \{0,1\}$.

Задача

Вход алгоритма: оракул U_f для $f : \{0,1\} \to \{0,1\}$.
Гарантируется одно из двух:

- f *константная*, т.е. $\forall x : f(x) = 0$ или $\forall x : f(x) = 1$;

Задача

Вход алгоритма: оракул U_f для $f : \{0,1\} \to \{0,1\}$.
Гарантируется одно из двух:

- f *константная*, т.е. $\forall x : f(x) = 0$ или $\forall x : f(x) = 1$;
- f *сбалансированная*, т.е. ровно на половине входных данных она возвращает 0, а на другой половине — 1.

Задача

Вход алгоритма: оракул U_f для $f : \{0,1\} \to \{0,1\}$.
Гарантируется одно из двух:

- f *константная*, т.е. $\forall x : f(x) = 0$ или $\forall x : f(x) = 1$;
- f *сбалансированная*, т.е. ровно на половине входных данных она возвращает 0, а на другой половине — 1.

Задача

Вход алгоритма: оракул U_f для $f : \{0,1\} \to \{0,1\}$.
Гарантируется одно из двух:

- f *константная*, т.е. $\forall x : f(x) = 0$ или $\forall x : f(x) = 1$;
- f *сбалансированная*, т.е. ровно на половине входных данных она возвращает 0, а на другой половине — 1.

Найти: какая функция f?

Классическое решение

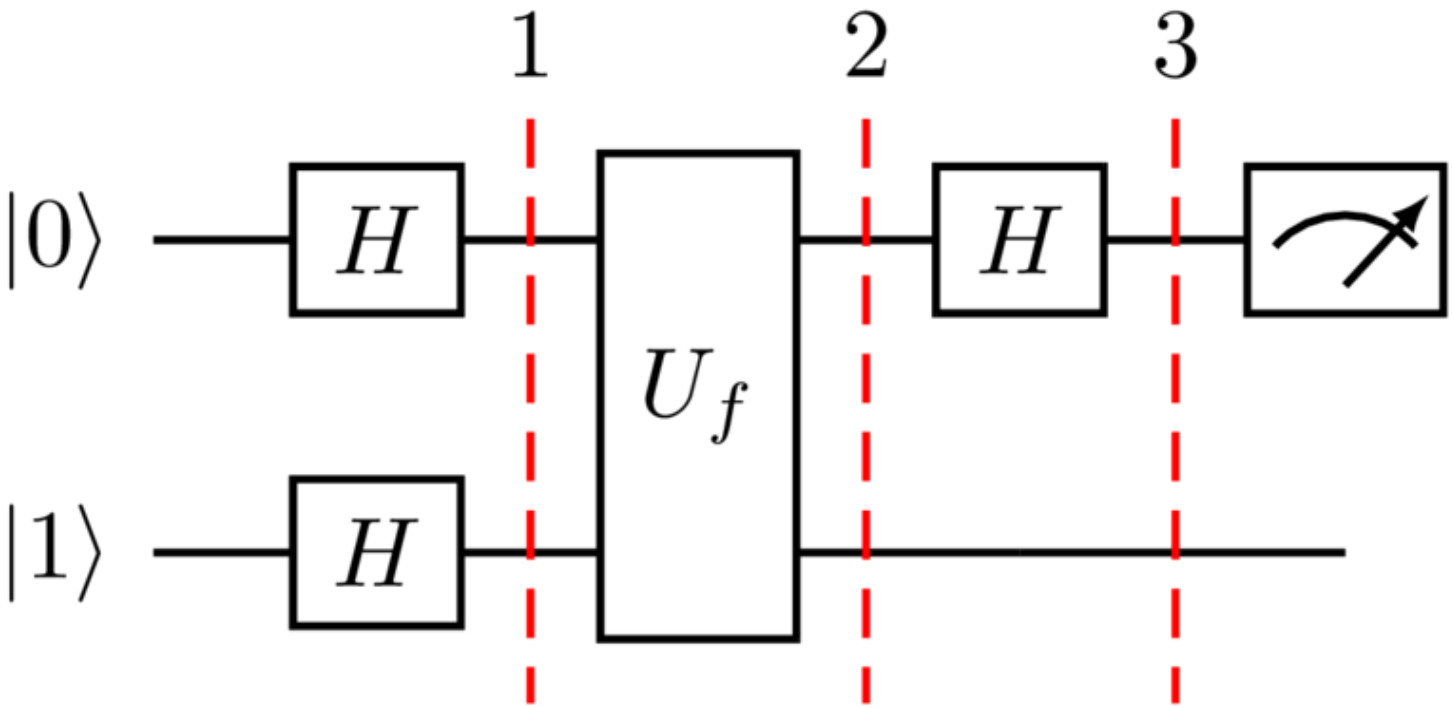
???

Классическое решение

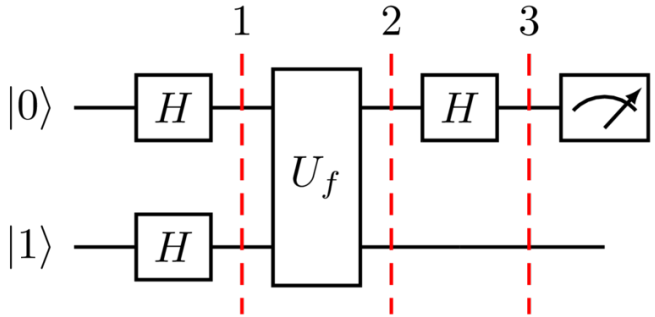
???

Проверить $f(0)$, проверить $f(1)$ — 2 запроса к f

Квантовое решение

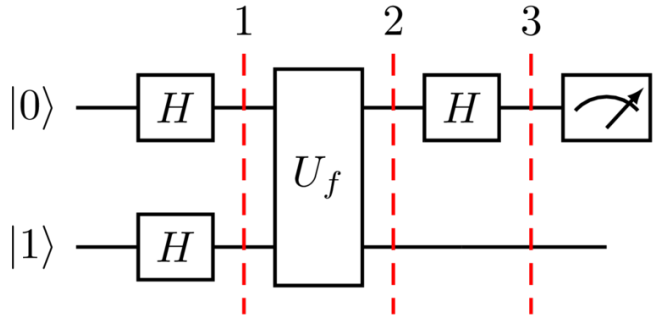


Разбор



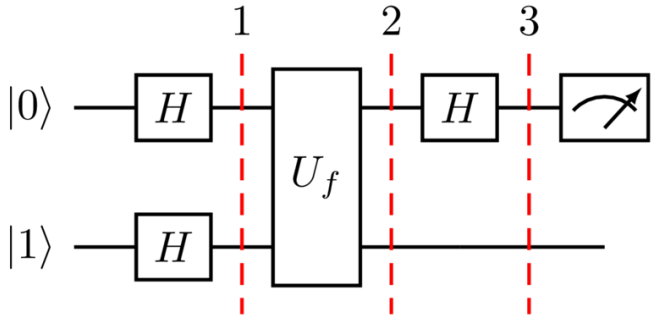
- $|\psi_0\rangle = |0\rangle|1\rangle$

Разбор



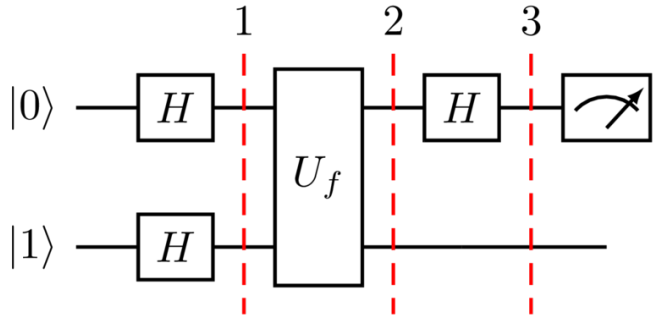
- $|\psi_0\rangle = |0\rangle|1\rangle$
- $|\psi_1\rangle = \frac{1}{2}\big(|0\rangle + |1\rangle\big)\big(|0\rangle - |1\rangle\big) = \frac{1}{2}\big(|00\rangle - |01\rangle + |10\rangle - |11\rangle\big)$

Разбор



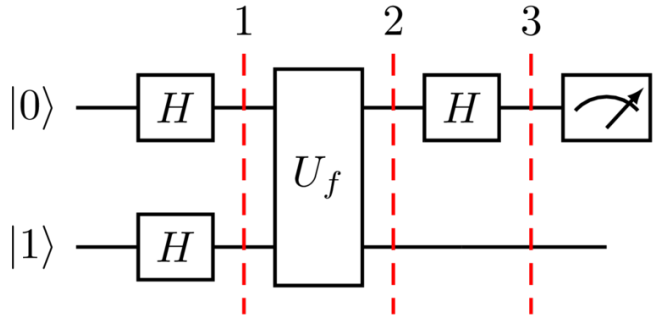
- $|\psi_0\rangle = |0\rangle|1\rangle$
- $|\psi_1\rangle = \frac{1}{2}\big(|0\rangle + |1\rangle\big)\big(|0\rangle - |1\rangle\big) = \frac{1}{2}\big(|00\rangle - |01\rangle + |10\rangle - |11\rangle\big)$
- $|\psi_2\rangle = \frac{1}{2}\big(|0\rangle|f(0)\rangle - |0\rangle|f(0)\oplus 1\rangle + |1\rangle|f(1)\rangle - |1\rangle|f(1)\oplus 1\rangle\big) =$

Разбор



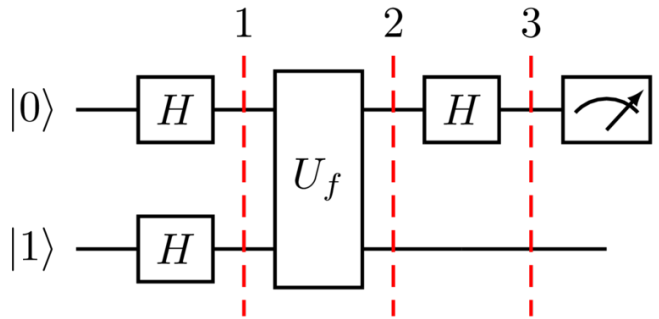
- $|\psi_0\rangle = |0\rangle|1\rangle$
- $|\psi_1\rangle = \frac{1}{2}\big(|0\rangle + |1\rangle\big)\big(|0\rangle - |1\rangle\big) = \frac{1}{2}\big(|00\rangle - |01\rangle + |10\rangle - |11\rangle\big)$
- $|\psi_2\rangle = \frac{1}{2}\big(|0\rangle|f(0)\rangle - |0\rangle|f(0)\oplus 1\rangle + |1\rangle|f(1)\rangle - |1\rangle|f(1)\oplus 1\rangle\big) =$
- $\ldots = \frac{1}{\sqrt{2}}\Big((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\Big) \otimes \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big)$

Разбор



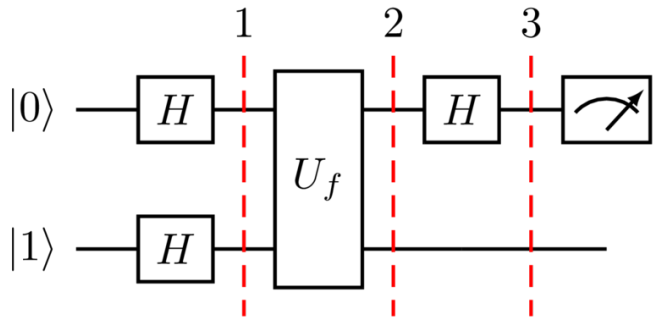
- $|\psi_0\rangle = |0\rangle|1\rangle$
- $|\psi_1\rangle = \frac{1}{2}\big(|0\rangle + |1\rangle\big)\big(|0\rangle - |1\rangle\big) = \frac{1}{2}\big(|00\rangle - |01\rangle + |10\rangle - |11\rangle\big)$
- $|\psi_2\rangle = \frac{1}{2}\big(|0\rangle|f(0)\rangle - |0\rangle|f(0)\oplus 1\rangle + |1\rangle|f(1)\rangle - |1\rangle|f(1)\oplus 1\rangle\big) =$
- $\ldots = \frac{1}{\sqrt{2}}\Big((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\Big) \otimes \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big)$
- $|\psi_3\rangle = ?$

Разбор



- $|\psi_3\rangle = H\frac{1}{\sqrt{2}}\Big((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\Big)$

Разбор

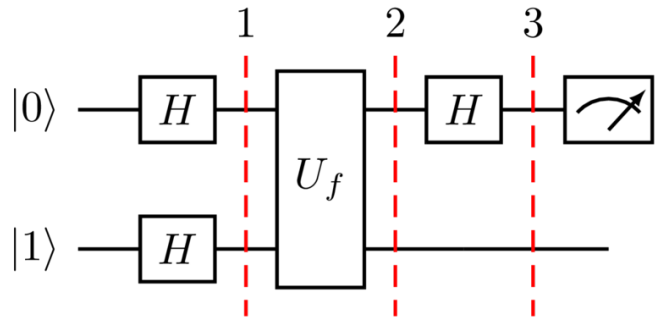


- $|\psi_3\rangle = H\frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right)$

Константная f

- $f(0) = f(1) = c$

Разбор

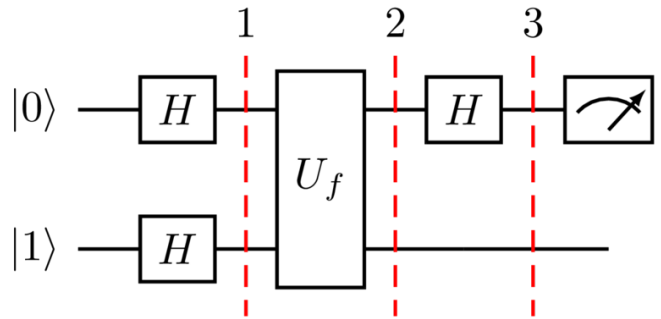


- $|\psi_3\rangle = H\frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right)$

Константная f

- $f(0) = f(1) = c$
- $|\psi_3\rangle = H\frac{(-1)^c}{2}\left(|0\rangle + |1\rangle\right) = (-1)^c|0\rangle$

Разбор

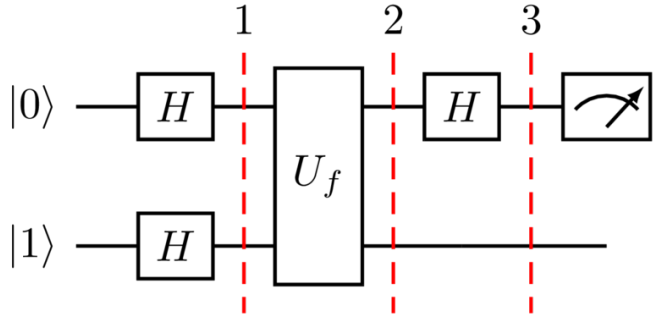


- $|\psi_3\rangle = H\frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right)$

Константная f

- $f(0) = f(1) = c$
- $|\psi_3\rangle = H\frac{(-1)^c}{2}\left(|0\rangle + |1\rangle\right) = (-1)^c|0\rangle$

Разбор



- $|\psi_3\rangle = H\frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right)$

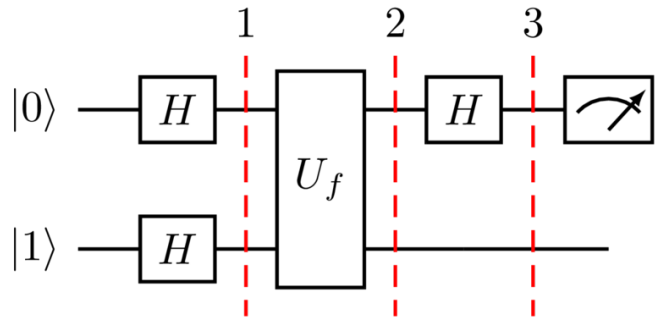
Константная f

- $f(0) = f(1) = c$
- $|\psi_3\rangle = H\frac{(-1)^c}{2}\left(|0\rangle + |1\rangle\right) = (-1)^c|0\rangle$

Сбалансированная f

- $f(0) = f(1) \oplus 1 = c$

Разбор



- $|\psi_3\rangle = H\frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right)$

Константная f

- $f(0) = f(1) = c$
- $|\psi_3\rangle = H\frac{(-1)^c}{2}\left(|0\rangle + |1\rangle\right) = (-1)^c|0\rangle$

Сбалансированная f

- $f(0) = f(1) \oplus 1 = c$
- $|\psi_3\rangle = H\frac{(-1)^c}{2}\left(|0\rangle - |1\rangle\right) = (-1)^c|1\rangle$

Алгоритм Дойча-Йожи

Задача

Вход алгоритма: оракул U_f для $f : \{0,1\}^n \to \{0,1\}$.

Задача

Вход алгоритма: оракул U_f для $f : \{0,1\}^n \to \{0,1\}$.
Гарантируется одно из двух:

- f *константная*, т.е. $\forall x : f(x) = 0$ или $\forall x : f(x) = 1$;

Задача

Вход алгоритма: оракул U_f для $f : \{0,1\}^n \to \{0,1\}$.
Гарантируется одно из двух:

- f *константная*, т.е. $\forall x : f(x) = 0$ или $\forall x : f(x) = 1$;
- f *сбалансированная*, т.е. ровно на половине входных данных она возвращает 0, а на другой половине — 1.

Задача

Вход алгоритма: оракул U_f для $f : \{0,1\}^n \to \{0,1\}$.
Гарантируется одно из двух:

- f *константная*, т.е. $\forall x : f(x) = 0$ или $\forall x : f(x) = 1$;
- f *сбалансированная*, т.е. ровно на половине входных данных она возвращает 0, а на другой половине — 1.

Задача

Вход алгоритма: оракул U_f для $f : \{0,1\}^n \to \{0,1\}$.
Гарантируется одно из двух:

- f *константная*, т.е. $\forall x : f(x) = 0$ или $\forall x : f(x) = 1$;
- f *сбалансированная*, т.е. ровно на половине входных данных она возвращает 0, а на другой половине — 1.

Найти: какая функция f?

Задача

Вход алгоритма: оракул U_f для $f : \{0,1\}^n \to \{0,1\}$.
Гарантируется одно из двух:

- f *константная*, т.е. $\forall x : f(x) = 0$ или $\forall x : f(x) = 1$;
- f *сбалансированная*, т.е. ровно на половине входных данных она возвращает 0, а на другой половине — 1.

Найти: какая функция f?

Частный случай

При $n = 1$ получаем алгоритм Дойча

Классическое решение

???

Классическое решение

???

- делаем $2^{n-1}+1$ запрос к оракулу
- проверяем более половины входных данных

Классическое решение

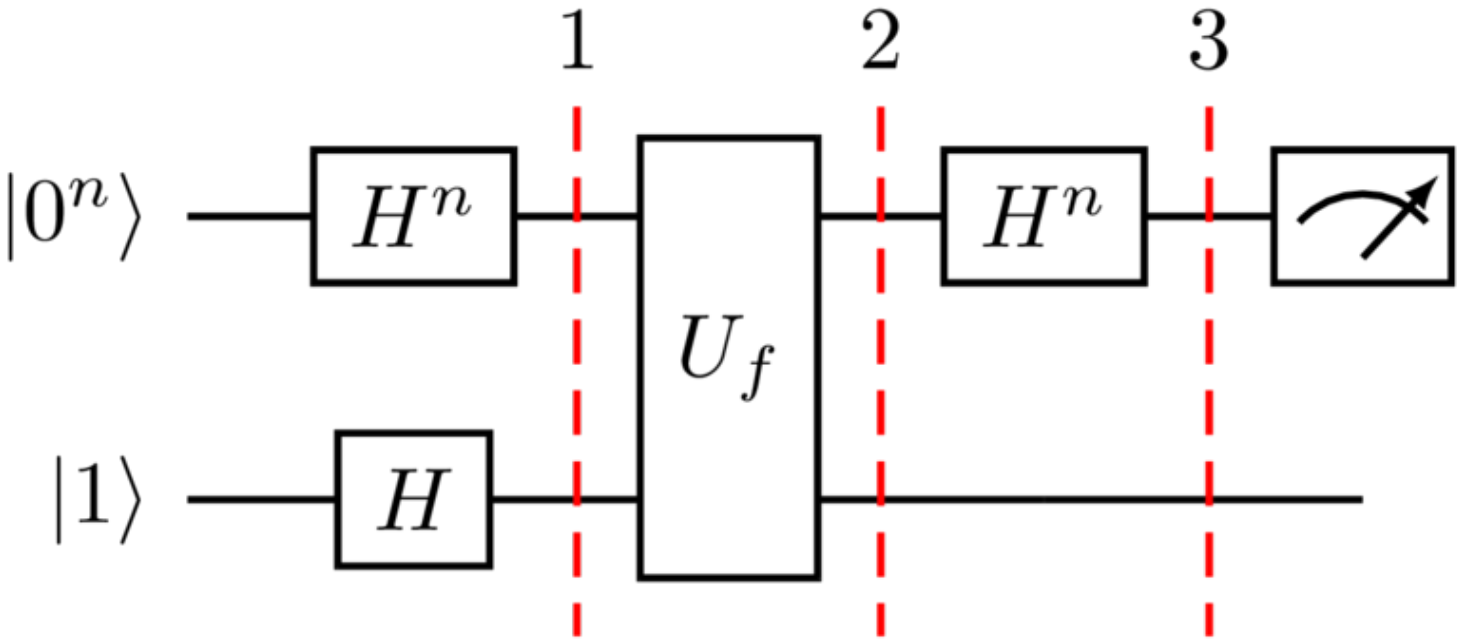
???

- делаем $2^{n-1}+1$ запрос к оракулу
- проверяем более половины входных данных

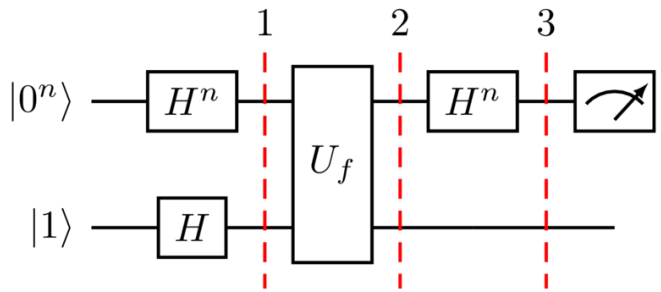
Квантовое преимущество

Квантовому алгоритму хватит всего одного (!) запроса

Алгоритм Дойча-Йожи

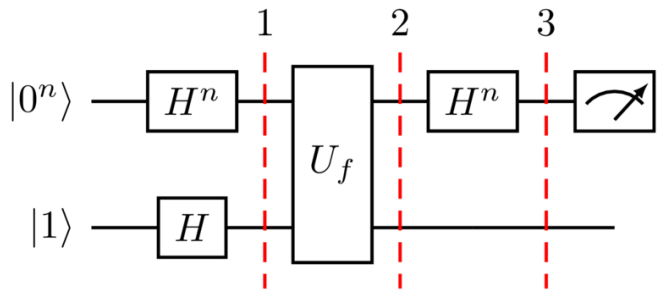


Разбор



- $|\psi_0\rangle = |0^n\rangle|1\rangle$

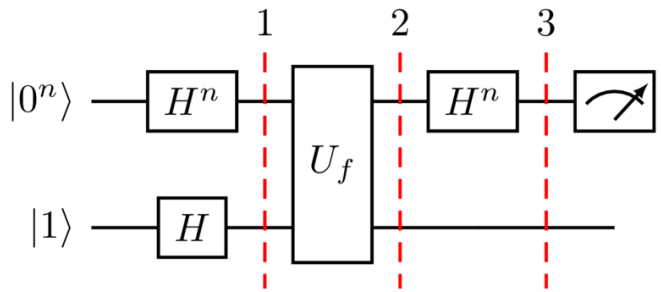
Разбор



- $|\psi_0\rangle = |0^n\rangle|1\rangle$
-

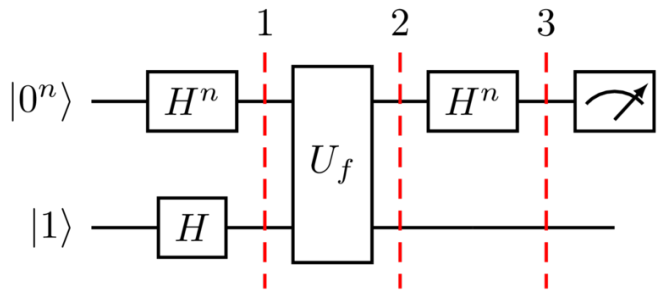
$$|\psi_1\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle(|0\rangle - |1\rangle)$$

Разбор



- $|\psi_0\rangle = |0^n\rangle|1\rangle$
- $$|\psi_1\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle(|0\rangle - |1\rangle)$$
- $$|\psi_2\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)$$

Разбор



- $|\psi_0\rangle = |0^n\rangle|1\rangle$
- $$|\psi_1\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle(|0\rangle - |1\rangle)$$
- $$|\psi_2\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)$$
- $$|\psi_3\rangle = H\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)}|x\rangle$$

Разбор

Рассмотрим отдельное базисное состояние $|x\rangle$:

$$H^n|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{s(x,y)}|y\rangle,$$

где $s(x, y)$ — либо 0, либо 1.

Разбор

Рассмотрим отдельное базисное состояние $|x\rangle$:

$$H^n|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{s(x,y)}|y\rangle,$$

где $s(x, y)$ — либо 0, либо 1.

Что такое $s(x, y)$?

- Если $x = 0^n$, то $s(0^n, y) = 0$ — при любых y

Разбор

Рассмотрим отдельное базисное состояние $|x\rangle$:

$$H^n|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{s(x,y)}|y\rangle,$$

где $s(x, y)$ — либо 0, либо 1.

Что такое $s(x, y)$?

- Если $x = 0^n$, то $s(0^n, y) = 0$ — при любых y
- Если в x ровно одна 1, будет множитель со знаком «минус» — если в y на этом месте стоит единица:

$$H^4|0100\rangle = \frac{1}{4}|+\rangle|-\rangle|+\rangle|+\rangle = \ldots + |0011\rangle - |0100\rangle - |0101\rangle \pm \ldots$$

Разбор

Рассмотрим отдельное базисное состояние $|x\rangle$:

$$H^n|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{s(x,y)}|y\rangle,$$

где $s(x, y)$ — либо 0, либо 1.

Что такое $s(x, y)$?

- Если $x = 0^n$, то $s(0^n, y) = 0$ — при любых y
- Если в x ровно одна 1, будет множитель со знаком «минус» — если в y на этом месте стоит единица:

$$H^4|0100\rangle = \frac{1}{4}|+\rangle|-\rangle|+\rangle|+\rangle = \ldots + |0011\rangle - |0100\rangle - |0101\rangle \pm \ldots$$

Разбор

Рассмотрим отдельное базисное состояние $|x\rangle$:

$$H^n|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{s(x,y)}|y\rangle,$$

где $s(x, y)$ — либо 0, либо 1.

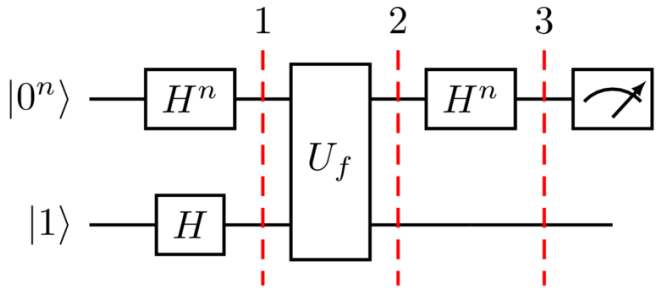
Что такое $s(x, y)$?

- Если $x = 0^n$, то $s(0^n, y) = 0$ — при любых y
- Если в x ровно одна 1, будет множитель со знаком «минус» — если в y на этом месте стоит единица:

$$H^4|0100\rangle = \frac{1}{4}|+\rangle|-\rangle|+\rangle|+\rangle = \ldots+|0011\rangle-|0100\rangle-|0101\rangle\pm\ldots$$

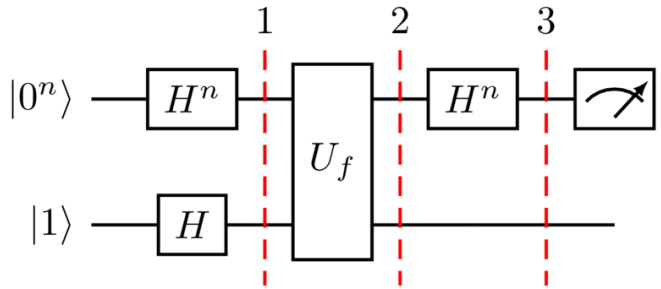
$$s(x, y) = x \cdot y = x_1y_1 \oplus x_2y_2 \oplus \ldots \oplus x_ny_n$$

Разбор



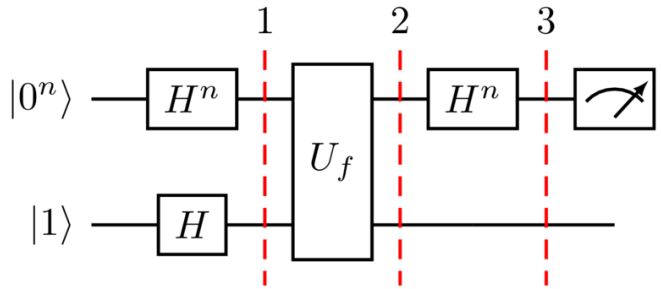
- $$|\psi_3\rangle = H\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle$$

Разбор



- $$|\psi_3\rangle = H\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle$$
- $$\ldots = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}\left(\frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1}(-1)^{x\cdot y}|y\rangle\right) =$$

Разбор



- $$|\psi_3\rangle = H\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle$$
- $$\ldots = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}\left(\frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1}(-1)^{x\cdot y}|y\rangle\right) =$$
- $$\ldots = \frac{1}{2^n}\sum_{y=0}^{2^n-1}\left(\sum_{x=0}^{2^n-1}(-1)^{f(x)+x\cdot y}\right)|y\rangle.$$

Разбор

$$|\psi_3\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \left(\sum_{x=0}^{2^n-1} (-1)^{f(x)+x\cdot y} \right) |y\rangle$$

Что может быть получено в результате измерения?

Вероятность того, что будут все нули ($y = 0^n$):

$$p_0 = \Pr[\mathcal{M}|\psi_3\rangle = 0^n] = \left| \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \right|^2.$$

Разбор

Вероятность измерить $y = 0^n$

$$p_0 = \Pr[\mathcal{M}|\psi_3\rangle = 0^n] = \left|\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{f(x)}\right|^2.$$

Разбор

Вероятность измерить $y = 0^n$

$$p_0 = \Pr[\mathcal{M}|\psi_3\rangle = 0^n] = \left|\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{f(x)}\right|^2.$$

Константная f

- Все $(-1)^{f(x)}$ совпадают.
- Сумма равна 2^n, и $p_0 = 1$.

Разбор

Вероятность измерить $y = 0^n$

$$p_0 = \Pr[\mathcal{M}|\psi_3\rangle = 0^n] = \left|\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{f(x)}\right|^2.$$

Константная f

- Все $(-1)^{f(x)}$ совпадают.
- Сумма равна 2^n, и $p_0 = 1$.

Сбалансированная f

- Ровно половина слагаемых 1, а вторая половина -1.
- Слагаемые сокращаются, и $p_0 = 0$.

Разбор

Результат работы алгоритма Дойча-Йожи

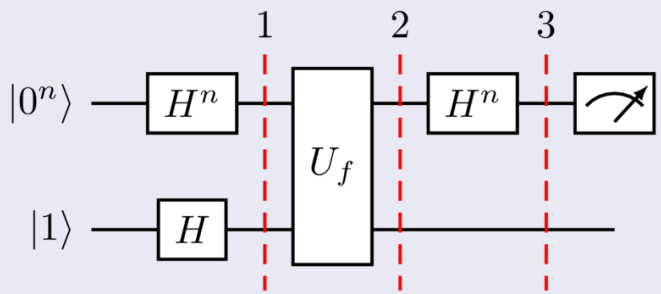
- Если f — константная, то всегда получаем 0^n.
- Если f — сбалансированная, то никогда не получаем 0^n.

Разбор

Результат работы алгоритма Дойча-Йожи

- Если f — константная, то всегда получаем 0^n.
- Если f — сбалансированная, то никогда не получаем 0^n.

Количество запросов и сравнение с классическим случаем



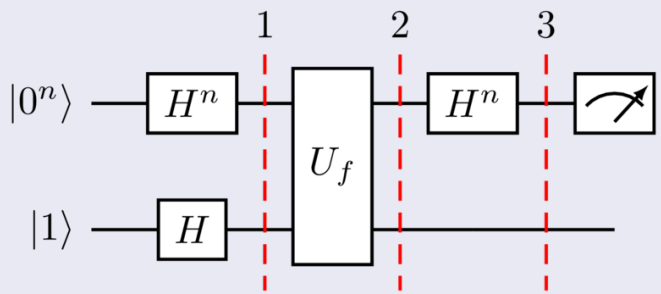
- На квантовом компьютере — одно вычисление функции f

Разбор

Результат работы алгоритма Дойча-Йожи

- Если f — константная, то всегда получаем 0^n.
- Если f — сбалансированная, то никогда не получаем 0^n.

Количество запросов и сравнение с классическим случаем



- На квантовом компьютере — одно вычисление функции f
- В классическом случае — $\Omega(2^n)$ вычислений.