Алгоритм Саймона

Квантовые вычисления–2023

17 октября 2023 г.

Outline

Классы сложности

Алгоритм Дойча-Йожи

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

Классы сложности

Алгоритм Дойча-Йожи

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

Класс BPP

- ограниченная ошибка (Bounded): $\Pr[A(x) = f(x)] \geq 2/3$

Классы сложности

Алгоритм Дойча-Йожи

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

Класс BPP

- ограниченная ошибка (Bounded): $\Pr[A(x) = f(x)] \geq 2/3$
- вероятностные вычисления (Probabilistic)

Классы сложности

Алгоритм Дойча-Йожи

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

Класс BPP

- ограниченная ошибка (Bounded): $\Pr[A(x) = f(x)] \geq 2/3$
- вероятностные вычисления (Probabilistic)
- полиномиальное время (Polynomial)

Классы сложности

Алгоритм Дойча-Йожи

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

Класс BPP

- ограниченная ошибка (Bounded): $\Pr[A(x) = f(x)] \geq 2/3$
- вероятностные вычисления (Probabilistic)
- полиномиальное время (Polynomial)

Классы сложности

Алгоритм Дойча-Йожи

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

Класс BPP

- ограниченная ошибка (Bounded): $\Pr[A(x) = f(x)] \geq 2/3$
- вероятностные вычисления (Probabilistic)
- полиномиальное время (Polynomial)

Класс BQP

- квантовые вычисления (Quantum)

Классы сложности

Алгоритм Дойча-Йожи

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

Класс BPP

- ограниченная ошибка (Bounded): $\Pr[A(x) = f(x)] \geq 2/3$
- вероятностные вычисления (Probabilistic)
- полиномиальное время (Polynomial)

Класс BQP

- квантовые вычисления (Quantum)

$$BPP^A \subsetneq BQP^A$$

Задача нахождения периода

Входные данные

Функция $f : \{0,1\}^n \to \{0,1\}^n$

Задача нахождения периода

Входные данные

Функция $f : \{0,1\}^n \to \{0,1\}^n$

Гарантируется

Существует такое $s \in \{0,1\}^n$, что $\forall x, y \in \{0,1\}^n$:

$$f(x) = f(y) \iff x \oplus y \in \{0^n, s\}.$$

Задача нахождения периода

Входные данные

Функция $f : \{0,1\}^n \to \{0,1\}^n$

Гарантируется

Существует такое $s \in \{0,1\}^n$, что $\forall x, y \in \{0,1\}^n$:

$$f(x) = f(y) \iff x \oplus y \in \{0^n, s\}.$$

Найти

Период s

Что такое s?

$s = 0^n$

- функция — перестановка;

Что такое s?

$s = 0^n$

- функция — перестановка;
- $f(x) = f(y) \iff x = y$;

Что такое s?

$s = 0^n$

- функция — перестановка;
- $f(x) = f(y) \iff x = y$;
- отображает различные входные значения в различные выходные («one-to-one»);

Что такое s?

$s = 0^n$

- функция — перестановка;
- $f(x) = f(y) \iff x = y$;
- отображает различные входные значения в различные выходные («one-to-one»);
- или: для каждого выходного значения существует единственное входное.

Что такое s?

$s = 0^n$

- функция — перестановка;
- $f(x) = f(y) \iff x = y$;
- отображает различные входные значения в различные выходные («one-to-one»);
- или: для каждого выходного значения существует единственное входное.

Что такое s?

$s = 0^n$

- функция — перестановка;
- $f(x) = f(y) \iff x = y$;
- отображает различные входные значения в различные выходные («one-to-one»);
- или: для каждого выходного значения существует единственное входное.

$s \neq 0^n$

- функция периодична с периодом s: $f(x) = f(x \oplus s)$;

Что такое s?

$s = 0^n$

- функция — перестановка;
- $f(x) = f(y) \iff x = y$;
- отображает различные входные значения в различные выходные («one-to-one»);
- или: для каждого выходного значения существует единственное входное.

$s \neq 0^n$

- функция периодична с периодом s: $f(x) = f(x \oplus s)$;
- для каждого выходного значения существует два входных («two-to-one»).

Классический алгоритм

???

Классический алгоритм

???

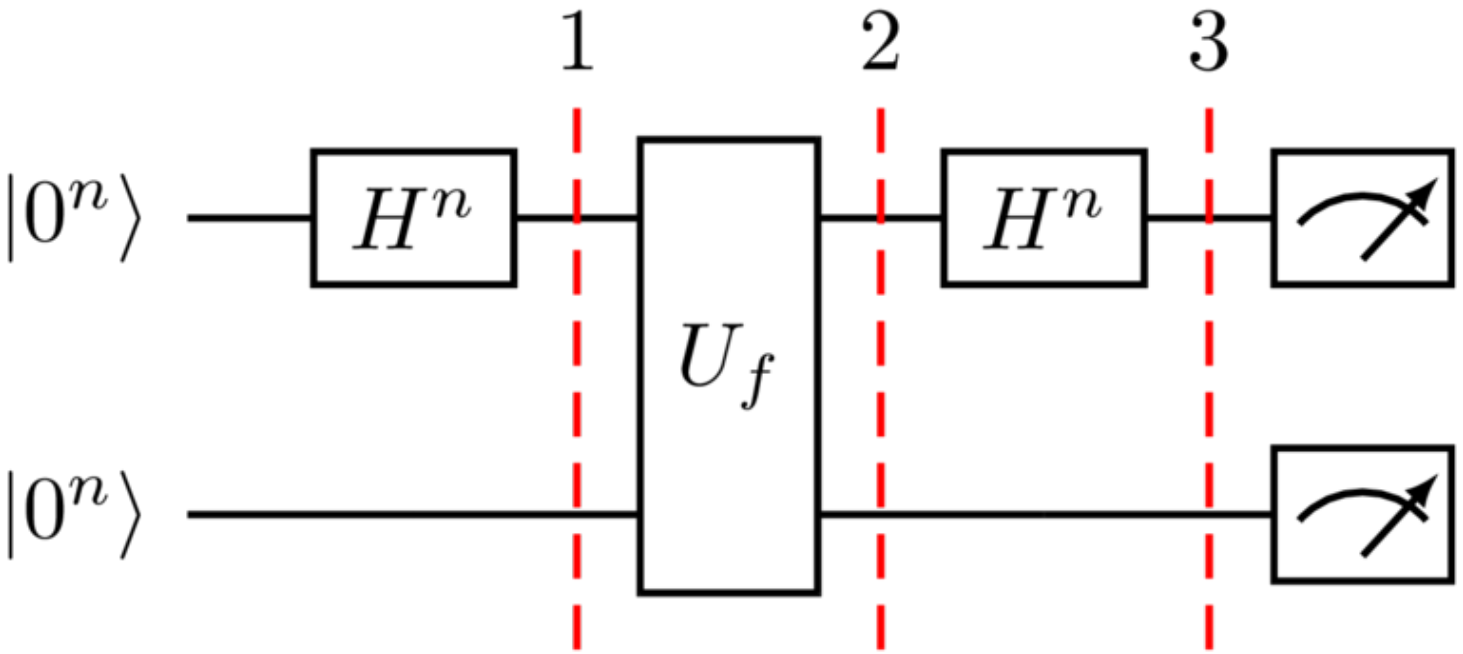
- $\Omega(\sqrt{2^n})$ вычислений f

Классический алгоритм

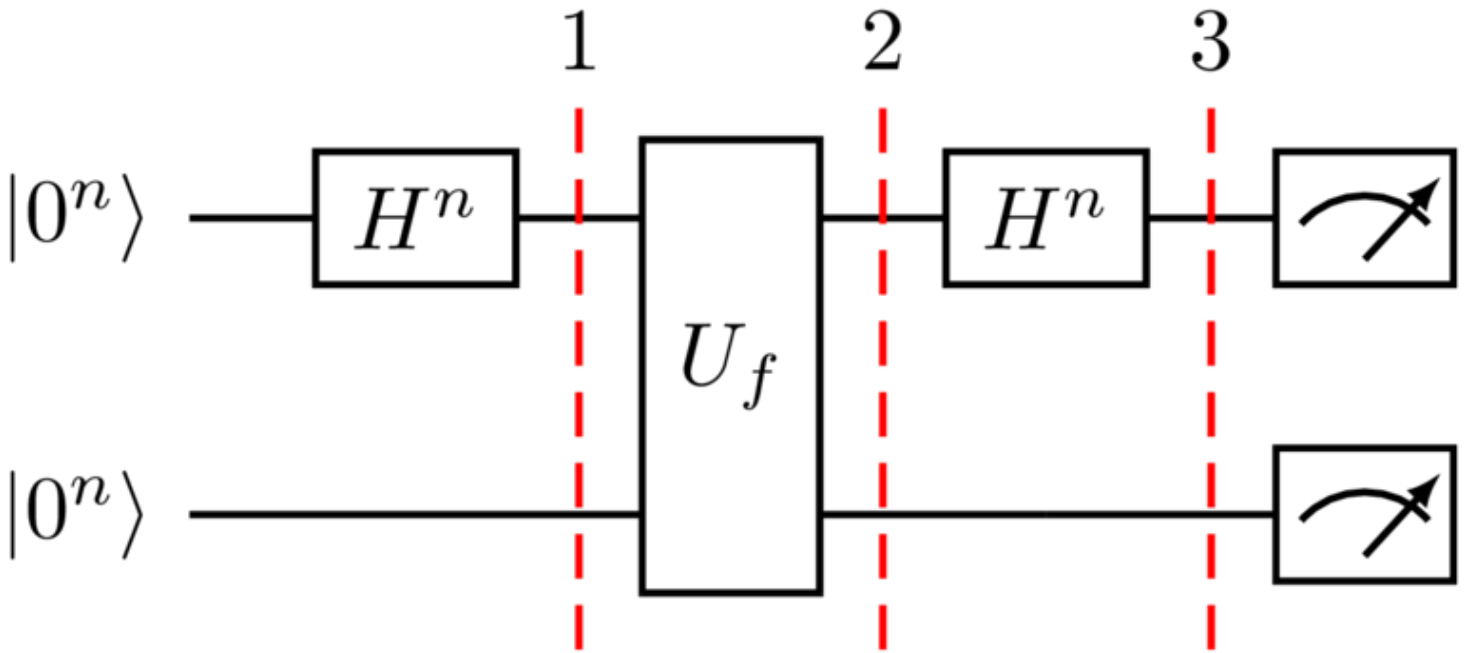
???

- $\Omega(\sqrt{2^n})$ вычислений f
- (парадокс дней рождений)

Квантовый алгоритм Саймона

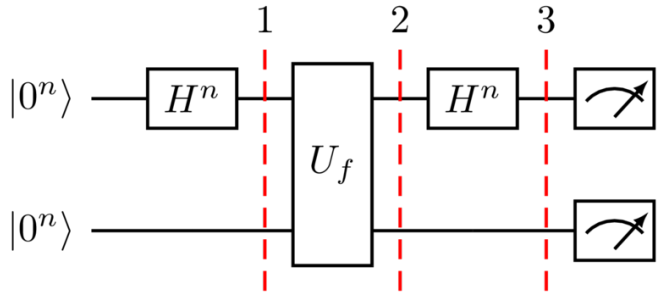


Квантовый алгоритм Саймона

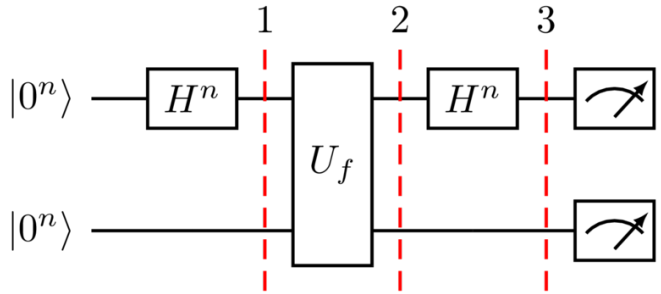


И небольшой классический пост-процессинг

Доказательство

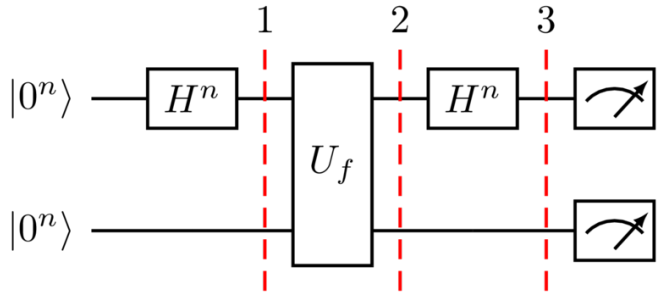


Доказательство



$$|\Psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \left(|x\rangle \otimes |0^n\rangle\right)$$

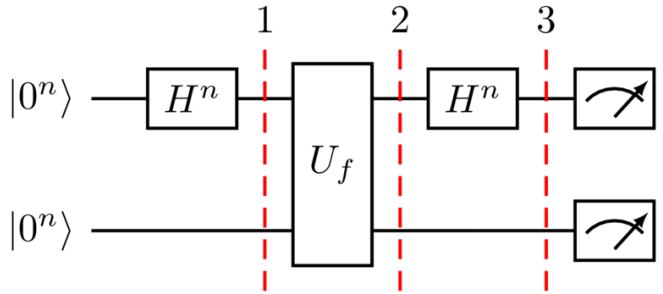
Доказательство



$$|\Psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \left(|x\rangle \otimes |0^n\rangle\right)$$

$$|\Psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \left(|x\rangle \otimes |f(x)\rangle\right)$$

Доказательство



$$|\Psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \left(|x\rangle \otimes |0^n\rangle\right)$$

$$|\Psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \left(|x\rangle \otimes |f(x)\rangle\right)$$

$$|\Psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \left(\frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x\cdot y} |y\rangle\right) \otimes |f(x)\rangle,$$

Случай $s = 0^n$

- перед измерением:

$$|\Psi_3\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \left(|y\rangle \otimes \sum_{x=0}^{2^n-1} (-1)^{x \cdot y} |f(x)\rangle \right);$$

Случай $s = 0^n$

- перед измерением:

$$|\Psi_3\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \left(|y\rangle \otimes \sum_{x=0}^{2^n-1} (-1)^{x \cdot y} |f(x)\rangle \right);$$

- вероятность измерить y:

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

Случай $s = 0^n$

- перед измерением:

$$|\Psi_3\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \left(|y\rangle \otimes \sum_{x=0}^{2^n-1} (-1)^{x \cdot y} |f(x)\rangle \right);$$

- вероятность измерить y:

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

- функция f — перестановка, поэтому $f(\{0,1\}^n) = \{0,1\}^n$;

Случай $s = 0^n$

- перед измерением:

$$|\Psi_3\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \left(|y\rangle \otimes \sum_{x=0}^{2^n-1} (-1)^{x \cdot y} |f(x)\rangle \right);$$

- вероятность измерить y:

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

- функция f — перестановка, поэтому $f(\{0,1\}^n) = \{0,1\}^n$;
- получаем произвольную $y \in \{0,1\}^n$ с $p_y = 2^{-n}$.

Случай $s \neq 0^n$

- перед измерением:

$$|\Psi_3\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \left(|y\rangle \otimes \sum_{x=0}^{2^n-1} (-1)^{x \cdot y} |f(x)\rangle \right)$$

Случай $s \neq 0^n$

- перед измерением:

$$|\Psi_3\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \left(|y\rangle \otimes \sum_{x=0}^{2^n-1} (-1)^{x \cdot y} |f(x)\rangle \right)$$

- функция f — «2-к-1».

Случай $s \neq 0^n$

- перед измерением:

$$|\Psi_3\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \left(|y\rangle \otimes \sum_{x=0}^{2^n-1} (-1)^{x \cdot y} |f(x)\rangle \right)$$

- функция f — «2-к-1».
- пусть $A = f(\{0,1\}^n)$.

Случай $s \neq 0^n$

- перед измерением:

$$|\Psi_3\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \left(|y\rangle \otimes \sum_{x=0}^{2^n-1} (-1)^{x \cdot y} |f(x)\rangle \right)$$

- функция f — «2-к-1».
- пусть $A = f(\{0,1\}^n)$.
- $\forall x_1 \in \{0,1\}^n$: $\exists! x_2 = x_1 \oplus s \in \{0,1\}^n$: $x_1 \neq x_2$ и $f(x_1) = f(x_2) = z \in A$;

Случай $s \neq 0^n$

- перед измерением:

$$|\Psi_3\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \left(|y\rangle \otimes \sum_{x=0}^{2^n-1} (-1)^{x \cdot y} |f(x)\rangle \right)$$

- функция f — «2-к-1».
- пусть $A = f(\{0,1\}^n)$.
- $\forall x_1 \in \{0,1\}^n$: $\exists! x_2 = x_1 \oplus s \in \{0,1\}^n$: $x_1 \neq x_2$ и $f(x_1) = f(x_2) = z \in A$;
- вероятность измерить y:

$$p_y = \frac{1}{2^n} \left| \sum_{x=0}^{2^n-1} (-1)^{x \cdot y} |f(x)\rangle \right|^2 = \frac{1}{2^n} \left| \sum_{z \in A} \left((-1)^{x_1 \cdot y} + (-1)^{x_2 \cdot y} \right) |z\rangle \right|^2.$$

Случай $s \neq 0^n$ - варианты

- вероятность измерить y:

$$p_y = \frac{1}{2^n} \left| \sum_{z \in A} \left((-1)^{x_1 \cdot y} + (-1)^{x_2 \cdot y} \right) |z\rangle \right|^2.$$

Случай $s \neq 0^n$ - варианты

- вероятность измерить y:

$$p_y = \frac{1}{2^n} \left| \sum_{z \in A} \left((-1)^{x_1 \cdot y} + (-1)^{x_2 \cdot y} \right) |z\rangle \right|^2.$$

- коэффициент при $|z\rangle$:

$$\ldots = (-1)^{x_1 \cdot y} + (-1)^{(x_1 \oplus s) \cdot y} = (-1)^{x_1 \cdot y} (1 + (-1)^{s \cdot y}).$$

Случай $s \neq 0^n$ - варианты

- вероятность измерить y:

$$p_y = \frac{1}{2^n} \left| \sum_{z \in A} \left((-1)^{x_1 \cdot y} + (-1)^{x_2 \cdot y} \right) |z\rangle \right|^2.$$

- коэффициент при $|z\rangle$:

$$\ldots = (-1)^{x_1 \cdot y} + (-1)^{(x_1 \oplus s) \cdot y} = (-1)^{x_1 \cdot y} (1 + (-1)^{s \cdot y}).$$

Случай $s \neq 0^n$ - варианты

- вероятность измерить y:

$$p_y = \frac{1}{2^n} \left| \sum_{z \in A} \left((-1)^{x_1 \cdot y} + (-1)^{x_2 \cdot y} \right) |z\rangle \right|^2.$$

- коэффициент при $|z\rangle$:

$$\ldots = (-1)^{x_1 \cdot y} + (-1)^{(x_1 \oplus s) \cdot y} = (-1)^{x_1 \cdot y} (1 + (-1)^{s \cdot y}).$$

Варианты

- если $s \cdot y = 1$, то $p_y = 0$

Случай $s \neq 0^n$ - варианты

- вероятность измерить y:

$$p_y = \frac{1}{2^n} \left| \sum_{z \in A} \left((-1)^{x_1 \cdot y} + (-1)^{x_2 \cdot y} \right) |z\rangle \right|^2.$$

- коэффициент при $|z\rangle$:

$$\ldots = (-1)^{x_1 \cdot y} + (-1)^{(x_1 \oplus s) \cdot y} = (-1)^{x_1 \cdot y} (1 + (-1)^{s \cdot y}).$$

Варианты

- если $s \cdot y = 1$, то $p_y = 0$
- если $s \cdot y = 0$, то $p_y = \frac{1}{2^{n-1}}$

Случай $s \neq 0^n$ - варианты

- вероятность измерить y:

$$p_y = \frac{1}{2^n} \left| \sum_{z \in A} \left((-1)^{x_1 \cdot y} + (-1)^{x_2 \cdot y} \right) |z\rangle \right|^2.$$

- коэффициент при $|z\rangle$:

$$\ldots = (-1)^{x_1 \cdot y} + (-1)^{(x_1 \oplus s) \cdot y} = (-1)^{x_1 \cdot y} (1 + (-1)^{s \cdot y}).$$

Варианты

- если $s \cdot y = 1$, то $p_y = 0$
- если $s \cdot y = 0$, то $p_y = \frac{1}{2^{n-1}}$

Случай $s \neq 0^n$ - варианты

- вероятность измерить y:

$$p_y = \frac{1}{2^n} \left| \sum_{z \in A} \left((-1)^{x_1 \cdot y} + (-1)^{x_2 \cdot y} \right) |z\rangle \right|^2.$$

- коэффициент при $|z\rangle$:

$$\ldots = (-1)^{x_1 \cdot y} + (-1)^{(x_1 \oplus s) \cdot y} = (-1)^{x_1 \cdot y} (1 + (-1)^{s \cdot y}).$$

Варианты

- если $s \cdot y = 1$, то $p_y = 0$
- если $s \cdot y = 0$, то $p_y = \frac{1}{2^{n-1}}$

Получаем только такие y, что $y \cdot s = 0$.

Классический пост-процессинг

- Запустим n раз.

Классический пост-процессинг

- Запустим n раз.
- Получим строки $y_1, \ldots, y_n$.

Классический пост-процессинг

- Запустим n раз.
- Получим строки $y_1, \ldots, y_n$.
- Составим систему уравнений $y_j \cdot s = 0$, где s - вектор неизвестных.

Классический пост-процессинг

- Запустим n раз.
- Получим строки $y_1, \ldots, y_n$.
- Составим систему уравнений $y_j \cdot s = 0$, где s - вектор неизвестных.
- Решаем её:

Классический пост-процессинг

- Запустим n раз.
- Получим строки $y_1, \ldots, y_n$.
- Составим систему уравнений $y_j \cdot s = 0$, где s - вектор неизвестных.
- Решаем её:
  - система неразрешима — $s = 0^n$,

Классический пост-процессинг

- Запустим n раз.
- Получим строки $y_1, \ldots, y_n$.
- Составим систему уравнений $y_j \cdot s = 0$,
  где s - вектор неизвестных.
- Решаем её:
  - система неразрешима — $s = 0^n$,
  - решение $s \neq 0^n$ (с вероятностью $> 1/4$ — единственное).

Классический пост-процессинг

- Запустим n раз.
- Получим строки $y_1, \ldots, y_n$.
- Составим систему уравнений $y_j \cdot s = 0$,
  где s - вектор неизвестных.
- Решаем её:
  - система неразрешима — $s = 0^n$,
  - решение $s \neq 0^n$ (с вероятностью $> 1/4$ — единственное).
- Пост-процессинг за полиномиальное время.

Значение

- квантовый алгоритм экспоненциально быстрее:

Значение

- квантовый алгоритм экспоненциально быстрее:
- $O(n)$ запросов вместо $\Omega(\sqrt{2^n})$;

Значение

- квантовый алгоритм экспоненциально быстрее:
- $O(n)$ запросов вместо $\Omega(\sqrt{2^n})$;
- можно модифицировать для функций с «примерным» периодом;

Значение

- квантовый алгоритм экспоненциально быстрее:
- $O(n)$ запросов вместо $\Omega(\sqrt{2^n})$;
- можно модифицировать для функций с «примерным» периодом;
- применение пост-процессинга.