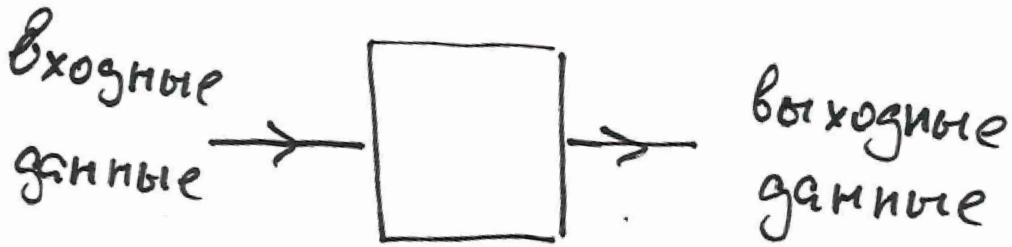
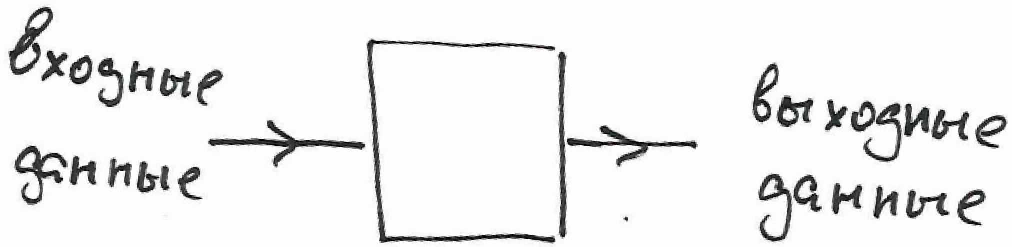
О квантовых вычислениях



$$\mathcal{X} = x_{n-1}\, x_{n-2} \cdots x_0 \qquad x_i \in \mathbb{Z}_2 = \{0, 1\}$$

$$x_{n-1} \cdot 2^{n-1} + \cdots x_1 \cdot 2 + x_0$$

$$0 \leq \mathcal{X} \leq 2^n - 1$$

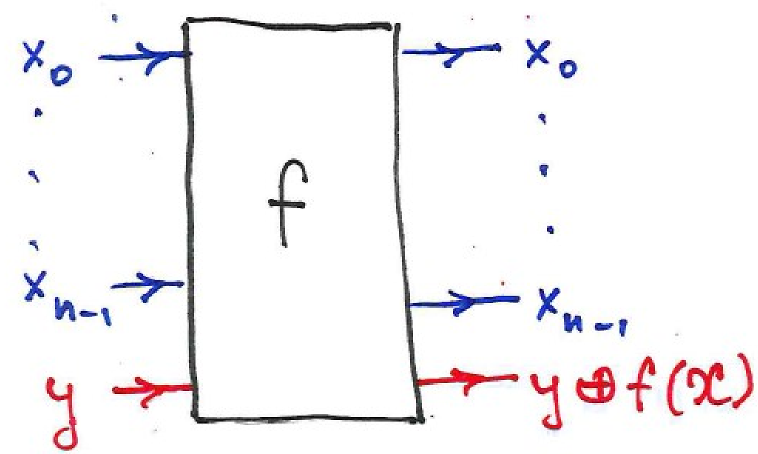


$\mathcal{X} = x_{n-1}\, x_{n-2} \cdots x_0$ $\qquad x_i \in \mathbb{Z}_2 = \{0, 1\}$

$x_{n-1} \cdot 2^{n-1} + \cdots x_1 \cdot 2 + x_0$

$0 \leq \mathcal{X} \leq 2^n - 1$

$f : (\mathbb{Z}_2)^n \to \mathbb{Z}_2$ - булева ф-ция



$$|\psi^{(in)}\rangle \rightarrow \boxed{} \rightarrow |\psi^{(out)}\rangle$$

$$|x\rangle = |x_{n-1}\rangle\, |x_{n-2}\rangle \cdots |x_0\rangle$$

$$|\psi^{(in)}\rangle \longrightarrow \boxed{} \longrightarrow |\psi^{(out)}\rangle$$

$$|x\rangle = |x_{n-1}\rangle\,|x_{n-2}\rangle \cdots |x_0\rangle$$

Элемент Адамара

$$|x\rangle \longrightarrow \boxed{H} \longrightarrow \frac{1}{\sqrt{2}}\left((-1)^x |x\rangle + |\bar{x}\rangle\right)$$

$$|0\rangle \xrightarrow{\hat{H}} \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$

$$|1\rangle \xrightarrow{\hat{H}} \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

$$|\psi^{(in)}\rangle \longrightarrow \boxed{\quad} \longrightarrow |\psi^{(out)}\rangle$$

$$|x\rangle = |x_{n-1}\rangle\, |x_{n-2}\rangle \dots |x_0\rangle$$

Элемент Адамара

$$|x\rangle \longrightarrow \boxed{H} \longrightarrow \frac{1}{\sqrt{2}}\left((-1)^x |x\rangle + |\bar{x}\rangle\right)$$

$$|0\rangle \xrightarrow{\hat{H}} \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$

$$|1\rangle \xrightarrow{\hat{H}} \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

$$\hat{H}^{\otimes n} |x\rangle = \hat{H}|x_{n-1}\rangle \dots \hat{H}|x_0\rangle =$$

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

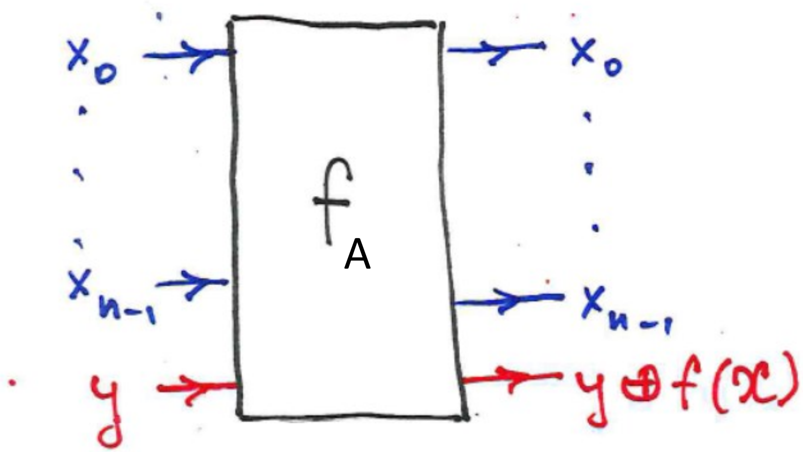
$$x \cdot y \doteq \sum_{i=0}^{n-1} x_i y_i \pmod{2}$$

Алгоритм Бернштейна – Вазирани

$$f_A : (\mathbb{Z}_2)^n \to \mathbb{Z}_2$$

$$x \longmapsto x \cdot A = x_0 a_0 \oplus \cdots \oplus x_{n-1} a_{n-1}$$

$$A = ?$$

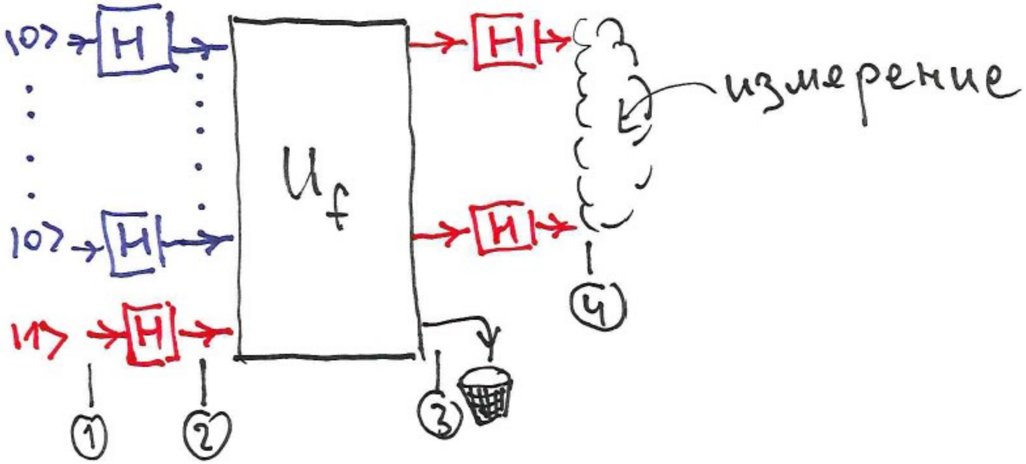


Алгоритм Бернштейна – Вазирани

$$f_A : (\mathbb{Z}_2)^n \to \mathbb{Z}_2$$

$$x \mapsto x \cdot A = x_0 a_0 \oplus \dots \oplus x_{n-1} a_{n-1}$$

$A = ?$

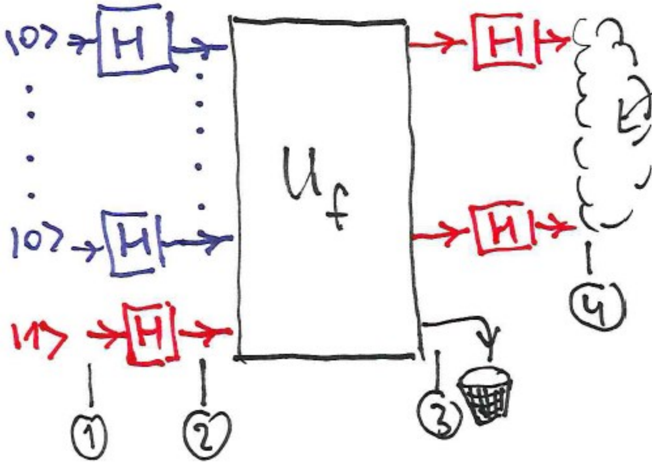


Алгоритм Бернштейна – Вазирани

$$f_A : (\mathbb{Z}_2)^n \to \mathbb{Z}_2$$

$$x \mapsto x \cdot A = x_0 a_0 \oplus \dots \oplus x_{n-1} a_{n-1}$$

$$\boxed{A = ?}$$



$$1: \quad |0\rangle \otimes |1\rangle$$

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

$$3: \quad \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes \frac{1}{\sqrt{2}}\left(|f(x)\rangle - |1 \oplus f(x)\rangle\right) =$$

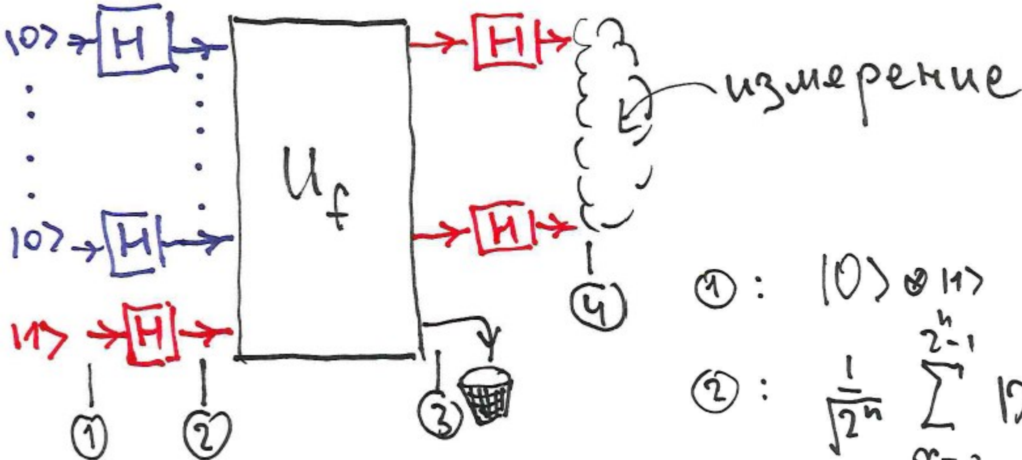
$$= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \otimes \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

Алгоритм Бернштейна–Вазирани

$$f_A : (\mathbb{Z}_2)^n \to \mathbb{Z}_2$$

$$x \mapsto x\cdot A = x_0 a_0 \oplus \dots \oplus x_{n-1} a_{n-1}$$

$$\boxed{A = ?}$$



① : $|0\rangle \otimes |1\rangle$

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

③ : $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes \frac{1}{\sqrt{2}}\left(|f(x)\rangle - |1 \oplus f(x)\rangle\right) =$

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

④ : $\frac{1}{2^n} \sum_{y=0}^{2^n-1} \left(\sum_{x=0}^{2^n-1} (-1)^{x\cdot A + x\cdot y} \right) |y\rangle = |A\rangle$