

# Алгоритм Шора. Наскождение периода

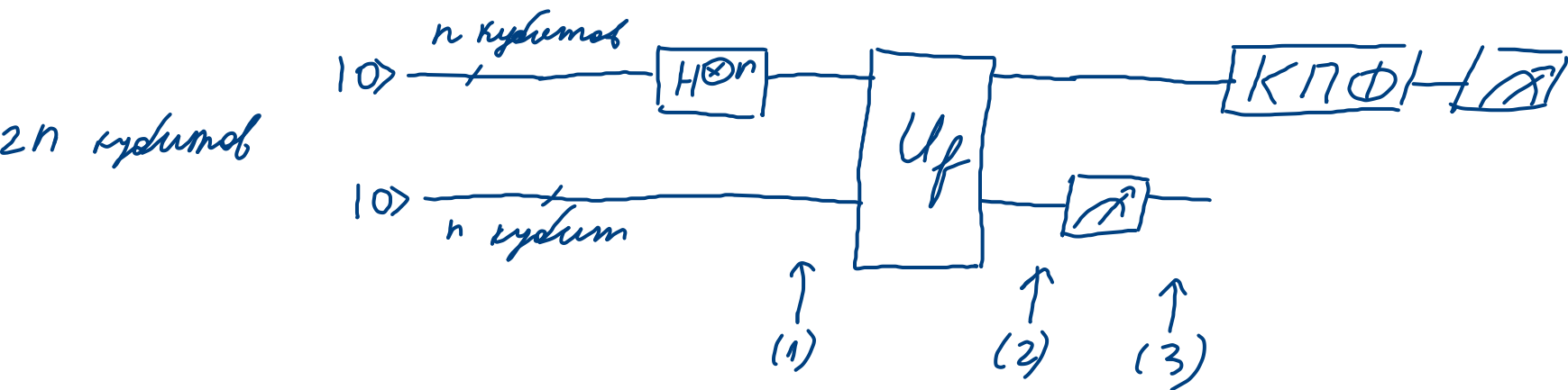
$$\underline{M} = p \cdot q$$

$$\mathbb{Z}_N \ni \{0, \dots, N-1\}$$

$$f: \mathbb{N} \setminus \{0\} \rightarrow \{0, \dots, N-1\} ; f(x) = a^x \bmod N$$

$$f(x+r) = f(x) , \quad r = ? \quad \min r \quad - \text{период}$$

$$N = 2^n ; \quad \underbrace{2^{n-1} < M^2 < 2^n = N} ; \quad \mathbb{C}^{2^n} \ni \{|0\rangle, |1\rangle, |2\rangle, \dots, |N-1\rangle\}$$



$$(1) \quad H^{\otimes n} |0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle ; \quad U_f |x\rangle |z\rangle = |x\rangle |z + f(x) \bmod N\rangle$$

$$H^{\otimes n} |0 \dots 0\rangle = \frac{1}{\sqrt{2^n}} \sum_{\vec{x} \in \{0,1\}^n} |\vec{x}\rangle ; \quad U_f |x\rangle |0\rangle = |x\rangle |f(x)\rangle$$

$$(2): \quad \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |f(x)\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{r-1} \left( \sum_{j=0}^{A_x-1} |x + j r\rangle \right) |f(x)\rangle ; \quad \begin{array}{l} A_x: \\ x + (A_x - 1)r \leq N-1 \\ x + A_x r > N-1 \end{array}$$

$$(3): \quad \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |x_0 + j r\rangle \otimes |f(x_0)\rangle ; \quad A = A_{x_0}$$

# Преобразование Фурье

$$f(x) : \mathbb{R} \rightarrow \mathbb{R} \quad , \quad \tilde{f}(\omega) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} f(x) e^{i\omega x} dx$$

$$\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} f(\underline{x_0+x}) e^{i\omega x} dx =$$

$t-\omega$

$$= \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} f(x) e^{i\omega(x-x_0)} dx = \underline{\underline{e^{-i\omega x_0} \tilde{f}(\omega) \dots}}$$

$$\tilde{f}(\omega) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} f(t) e^{i\omega t} dt$$



КПФ,  $\mathbb{C}^N \ni \{|0\rangle, \dots, |N-1\rangle\}$

$$\text{КПФ: } |x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i xy/N} |y\rangle$$

$$| \tilde{f}(\omega) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} e^{i\omega x} f(x) dx$$

$$\text{КПФ} = \frac{1}{\sqrt{N}} \sum_{x,y=0}^{N-1} \omega^{xy} |y\rangle \langle x|$$

$$\omega = e^{\frac{2\pi i}{N}}$$

Примеры:  $N=2$ ,  $\omega = e^{\frac{2\pi i}{2}} = e^{\pi i} = -1$

$$\text{КПФ} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = H$$

$$N=4, \omega = e^{2\pi i/4} = e^{\frac{\pi i}{2}} = i$$

$$\text{КПФ} = \frac{1}{2} \begin{matrix} & \begin{matrix} 0 & 1 & 2 & 3 \end{matrix} \\ \begin{matrix} 0 \\ 1 \\ 2 \\ 3 \end{matrix} & \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \end{matrix}$$

Реализация КПФ:

Кулосен-Чанг, Сисоев

$$H^{\otimes 2} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Реализация  $f(x) = a^x \bmod N$

Дасунта, Ратнагунимпруг, Вазуранни. Алгоритмы

Возвращаемся к алгоритму

$$\frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |x_0 + jz\rangle \xrightarrow{\text{КНФ}} \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} \frac{1}{N} \sum_{y=0}^{N-1} \underbrace{e^{\frac{2\pi i}{N}(x_0 + jz)y}}_{e^{\frac{2\pi i}{N}x_0 y} \cdot e^{\frac{2\pi i}{N}jzy}} |y\rangle =$$

$$= \frac{1}{\sqrt{NA}} \sum_{y=0}^{N-1} \left( \underbrace{e^{\frac{2\pi i}{N}x_0 y}}_{=1} \sum_{j=0}^{A-1} e^{\frac{2\pi i}{N}jzy} \right) |y\rangle \quad \left| \theta_j = 2\pi \frac{zy}{N} \right|$$

□:  $P(y) = \frac{A}{N} \left| \frac{1}{A} \sum_{j=0}^{A-1} e^{\frac{2\pi i}{N}jzy} \right|^2 = \frac{A}{N} \left| \frac{1}{A} \frac{e^{iA\theta_y} - 1}{e^{i\theta_y} - 1} \right|^2$

Распределение  $P(y)$  резко выделяет такие значения  $y$ , при кот.  $\frac{zy}{N}$  близко к целому

Пусть  $\frac{N}{z} = 2^n$  — целое,  $\frac{N}{z} = A$ ;

$$\sum_{j=0}^{A-1} |x_0 + jz\rangle = |x_0\rangle + |x_0 + z\rangle + |x_0 + 2z\rangle + \dots + |x_0 + (\frac{N}{z} - 1)z\rangle \quad ; \quad |x_0 + \frac{N}{z}z\rangle = |x_0 + N\rangle = |x_0\rangle$$

$$P(y) = \frac{1}{z} \left| \sum_{j=0}^{\frac{N}{z}-1} \omega^{zyj} \right|^2 = \frac{1}{z} \left| \sum_{j=0}^{\frac{N}{z}-1} e^{2\pi i j \frac{zy}{N}} \right|^2$$

1)  $y$  кратно  $A$ ,  $y = kA$ , то  $P(y) = \frac{1}{z} \left| \sum_{j=0}^{\frac{N}{z}-1} 1 \right|^2 = \frac{1}{z} \left( \frac{N}{z} \right)^2 = \frac{1}{z}$

2)  $y$  не кратно  $A$ ,  $\omega^{2\pi i \frac{y}{A}} \neq 1$ ,  $P(y) = \frac{1}{z} \left| \sum_{j=0}^{\frac{N}{z}-1} \omega^{zyj} \right|^2 = \frac{1}{z} \left| \sum_{j=0}^{\frac{N}{z}-1} \frac{\omega^{zy \frac{N}{z}} - 1}{\omega^{zy} - 1} \right|^2 = 0$

$$\sum_{n=0}^{N-1} q^n = \frac{q^N - 1}{q - 1}$$

$$P(y) = \begin{cases} \frac{1}{z}, & y \text{ кратно } A \\ 0, & \text{иначе} \end{cases}$$



Получили  $y = k \cdot \frac{N}{z}$

$$y_1 = k_1 \frac{N}{z} \quad \text{НОД}(y_1, y_2) = \frac{N}{z} \quad ; \quad z = \frac{N}{\text{НОД}(y_1, y_2)}$$

$$y_2 = k_2 \frac{N}{z} \quad \text{Пусть } \text{НОД}(k_1, k_2) = 1$$

Оценим  $P(\text{НОД}(k_1, k_2) \neq 1)$

$$P(p \text{ делит } k) = \frac{1}{p}$$

$$P(p \text{ делит } k_1 \text{ и } k_2) = \frac{1}{p^2}$$

$$P(\text{НОД}(k_1, k_2) = 1) = \prod_p \left( 1 - P(p \text{ делит } k_1 \text{ и } k_2) \right) = \prod_p \left( 1 - \frac{1}{p^2} \right) =$$

$$= \frac{1}{\zeta(2)} = \frac{6}{\pi^2} \approx 0.607 \quad \text{рез. от } z$$

Д.З. Разобрать наш алгоритм для

$$f(x) = x \bmod 2, \quad N=8 \quad \text{in} \rightarrow \boxed{?} \rightarrow \text{out}$$

$$\begin{matrix} 107 \\ 127 \end{matrix} \rightarrow \begin{bmatrix} U_1 \\ I \end{bmatrix} \rightarrow \begin{matrix} 1x \\ -120f(2) \end{matrix}$$

критерий  $\{ = -$

критерий 107, 112, ..., 127

