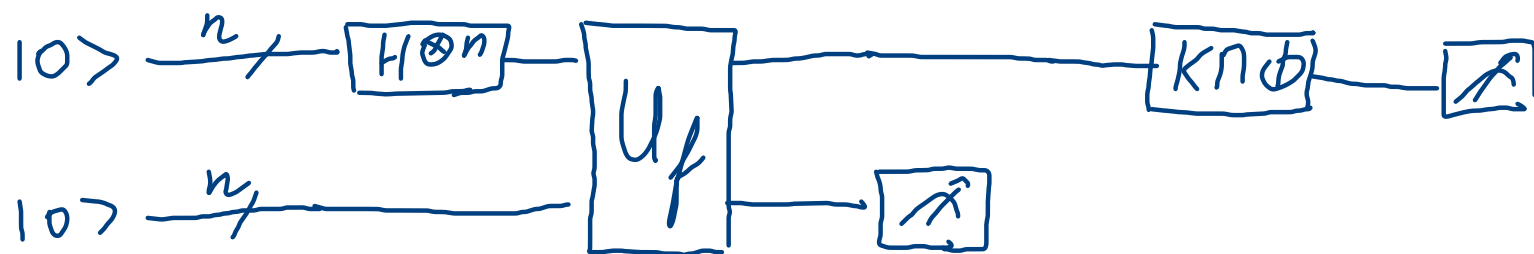


Алгоритм Шора

$$M = p \cdot q, \quad f(x) = a^x \bmod M, \quad \underline{f(x+z) = f(x)}$$

$$N = 2^n, \quad 2^{n-1} < M^2 < 2^n = N, \quad M < \sqrt{N}$$



$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |0\rangle \quad \xrightarrow{U_f} \quad \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |f(x)\rangle =$$

$$A \equiv A(x_0)$$

$$= \frac{1}{\sqrt{N}} \sum_{x_0=0}^{z-1} \left(\sum_{j=0}^{A-1} |x_0 + jz\rangle \right) |f(x_0)\rangle$$

$$(*) \quad \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |x_0 + jz\rangle$$

$$N: z \Rightarrow A = \frac{N}{z}$$

$$N - z \leq x_0 + (A-1)z < N$$

$$\boxed{A-1 < \frac{N}{z} < A+1}$$

$$/z : \frac{N}{z} - 1 \leq \frac{x_0 - 1 + A}{z} < \frac{N}{z}$$

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

$$\frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |x_0 + jz\rangle \xrightarrow{\text{KHF}} \frac{1}{\sqrt{NA}} \sum_{y=0}^{N-1} e^{\frac{2\pi i}{N} x_0 y} \sum_{j=0}^{A-1} e^{\frac{2\pi i}{N} jzy} |y\rangle$$

$\begin{array}{c} \uparrow \\ \frac{1}{\sqrt{A}} \left[\begin{array}{c} \leftarrow z \rightarrow \leftarrow z \rightarrow \dots \end{array} \right] \\ x_0 \quad x_0+z \quad x_0+2z \end{array}$

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

$$\sum_{j=0}^{n-1} q^j = \frac{q^n - 1}{q - 1}, \quad q = e^{\frac{2\pi i}{N} (zy \bmod N)}$$

$$q = e^{i\theta_y}, \quad \theta_y = 2\pi \frac{zy \bmod N}{N}$$

Even $N:z$, no $P(y) = \begin{cases} \frac{1}{z}, & y \text{ кратно } A = \frac{N}{z} \\ 0, & \text{иначе} \end{cases} \Rightarrow y = k \frac{N}{z}$

$\begin{array}{c} \uparrow \\ \frac{1}{\sqrt{N}} \left[\begin{array}{c} \leftarrow \frac{N}{z} \rightarrow \leftarrow \frac{N}{z} \rightarrow \dots \end{array} \right] \\ 0 \end{array}$

$$\frac{N}{\text{MOD}(y, y_1)}$$

$y_1 = \frac{k_1 N}{z}, y_2 = \frac{k_2 N}{z}$
 even $\text{MOD}(k_1, k_2) = 1$
 no $\text{MOD}(y_1, y_2) = \frac{N}{z}$

Пусть $z > 2$

$\exists$ ровно z значений $y \in \{0, 1, \dots, N-1\}$,
удовлетворяющих

$$-\frac{z}{2} \leq yz \pmod{N} \leq \frac{z}{2} \quad - \text{ "хорошие" } y$$

$$\exists k: \quad kN - \frac{z}{2} \leq yz \leq kN + \frac{z}{2} \quad /z, \quad /N$$

$$k \frac{N}{z} - \frac{1}{2} \leq \underline{y} \leq k \frac{N}{z} + \frac{1}{2} \quad /N$$

ровно 1 число y на отрезке $\left[k \frac{N}{z} - \frac{1}{2}, k \frac{N}{z} + \frac{1}{2} \right]$

для каждого
 $k \in \{0, 1, 2, \dots, z-1\}$

$$\frac{k}{z} - \frac{1}{2N} \leq \frac{y}{N} \leq \frac{k}{z} + \frac{1}{2N}$$

$$\Downarrow$$
$$\left| \frac{y}{N} - \frac{k}{z} \right| \leq \frac{1}{2N}$$

1. Оценить ^{сумму} $\sum_{\text{хорошие } y} P(y)$ того, что y - хороший

$$\sum_{\text{хорошие } y} P(y)$$

2. Найти $k \frac{N}{2}$, если y - хороший

$$|\frac{y}{N} - \frac{k}{2}| \leq \frac{1}{2N}$$

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

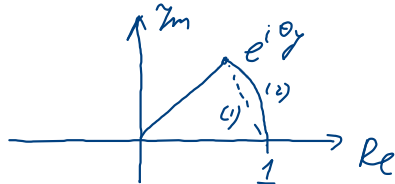
$$\theta_y = \frac{2\pi}{N} (zy \bmod N)$$

$$y \text{ - хороший} \Rightarrow kN - \frac{N}{2} \leq zy \leq kN + \frac{N}{2} \Rightarrow -\pi \frac{N}{N} \leq \theta_y \leq \pi \frac{N}{N}$$

$A-1 < \frac{N}{2} \Rightarrow$ все слагаемые $e^{i\theta_y j}$ лежат в узле perpendicular первой полуокружности



$$\textcircled{1} |e^{i\theta_y} - 1| \leq |\theta_y|$$

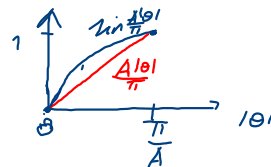


$$\textcircled{2} \text{ Чтб. Если } A|\theta| \leq \pi, \text{ то } |1 - e^{iA\theta}| \geq \frac{2A|\theta|}{\pi}$$

До-во Следует из формулы $|1 - e^{iA\theta}|$ по θ и формулам пер-ва ма кривых отрезка $\theta \in [\frac{\pi}{A}, \frac{\pi}{A}]$

$$|1 - e^{iA\theta}| = |\cos A\theta + i \sin A\theta - 1| = \sqrt{(\cos A\theta - 1)^2 + \sin^2 A\theta} =$$

$$= \sqrt{2 - 2\cos A\theta} = \sqrt{2 \cdot 2 \sin^2 \frac{A\theta}{2}} = 2 \sin \frac{A|\theta|}{2}$$



Следствие Если $A|\theta| \leq \pi$, то

$$P(y) \geq \frac{1}{AN} \cdot \left(\frac{2A|\theta|}{\pi} \right)^2 = \frac{4A}{\pi^2 N} \approx \frac{4}{\pi^2 N} ; \sum_{y \text{ - хорошие}} P(y) \approx \frac{4}{\pi^2} = \underline{\underline{O(1)}}$$

$$A < \frac{N}{2} + 1, |\theta| \leq \pi \frac{N}{N}, \Rightarrow A|\theta| < \left(\frac{N}{2} + 1 \right) \pi \frac{N}{N} = \pi \left(1 + \frac{2}{N} \right)$$

$$\left| \frac{e^{iA\theta} - 1}{e^{i\theta} - 1} \right| = \left| \frac{e^{i(A-1)\theta} - 1}{e^{i\theta} - 1} + e^{i(A-1)\theta} \right| \geq \frac{2(A-1)|\theta|}{\pi|\theta|} - 1 = \frac{2A}{\pi} - \left(1 + \frac{2}{N} \right)$$

$$A-1 < \frac{N}{2}, (A-1)|\theta| \leq \frac{N}{2} \cdot \pi \frac{N}{N} = \pi \Rightarrow \left| \frac{e^{i(A-1)\theta} - 1}{e^{i\theta} - 1} \right| \geq 1 \quad / \quad z < M \leq \sqrt{N}, A = \frac{N}{2} - \text{дискретное}$$

$$P(y) \geq \frac{1}{AN} \left[\frac{2A}{\pi} - \left(1 + \frac{2}{N} \right) \right]^2 \approx \frac{4}{\pi^2 N} = O\left(\frac{1}{N}\right); \sum_{y \text{ - хорошие}} P(y) \approx \frac{4}{\pi^2}, \text{ т.е.}$$

② Умеем $y: \left| \frac{y}{N} - \frac{k}{z} \right| \leq \frac{1}{2N} \quad (*)$

$$k \frac{N}{z} - \frac{1}{2} \leq y \leq k \frac{N}{z} + \frac{1}{2}$$

$$z < M \leq \sqrt{N}, \quad N \geq M^2$$

Ум.1 $\left| \frac{k}{z} - \frac{k'}{z} \right| > \frac{1}{M^2}$

Ум.2 Если $\exists k \neq k': \left| \frac{y}{N} - \frac{k}{z} \right| \leq \frac{1}{2N}$
 $\left| \frac{y}{N} - \frac{k'}{z} \right| \leq \frac{1}{2N}$

Д-во: $\Rightarrow \left| \frac{k-k'}{z} \right| > \frac{1}{M}$

но $\left| \frac{k'}{z} - \frac{k}{z} \right| \leq \frac{1}{N} \leq \frac{1}{M^2}$

Следствие $\exists! k: \text{fun.} (*)$

Задача: Найти граф с размерами $< M: \text{fun.} (*)$

Ум.3 Такая граф существует.

В самом деле, пусть $\exists$ две ^{разные} графы $\frac{a}{b}$ и $\frac{c}{d}$, где $b < M$ и $d < M$

Тогда $\left| \frac{a}{b} - \frac{c}{d} \right| = \frac{|ad - bc|}{bd} > \frac{1}{M^2}$

С др. стороны, если $\exists$ две разл. графы $\frac{a}{b}$ и $\frac{c}{d}$, где $\text{ком } \left| \frac{y}{N} - \frac{a}{b} \right| \leq \frac{1}{2M^2}$
 то $\left| \frac{a}{b} - \frac{c}{d} \right| \leq \frac{1}{M^2}$, что невозможно $\left| \frac{y}{N} - \frac{c}{d} \right| \leq \frac{1}{2M^2}$

Целые дроби

Пример

$$n=10, N=2^n=1024, M=32$$

$$y=139$$

$$\frac{y}{N} = \frac{139}{1024}, \text{ хотим приблизить дробь } \\ \text{с знаменателем } < M$$

$$\frac{139}{1024} = \frac{1}{\frac{1024}{139}} = \frac{1}{7 + \frac{51}{139}} \approx \frac{1}{7}$$

$$\overset{11}{\frac{1}{7 + \frac{1}{\frac{139}{51}}}} = \frac{1}{7 + \frac{1}{2 + \frac{37}{51}}} \approx \frac{1}{7 + \frac{1}{2}} = \frac{2}{15}$$

$$\overset{11}{\frac{1}{7 + \frac{1}{2 + \frac{1}{\frac{51}{37}}}}} = \frac{1}{7 + \frac{1}{2 + \frac{1}{1 + \frac{14}{37}}}} \approx \frac{1}{7 + \frac{1}{2 + \frac{1}{2}}} = \frac{3}{22}$$

$$\overset{11}{\frac{1}{7 + \frac{1}{2 + \frac{1}{1 + \frac{1}{\frac{37}{14}}}}}} = \frac{1}{7 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2 + \frac{2}{14}}}}} \approx \frac{8}{57}$$

$$\underline{59 > 32}$$

Искомое приближение: $\frac{3}{22} = \frac{k}{z}$

Если $\text{НОД}(k, z) = 1$,

то $z = 22$

Если это не так, то $\overset{\text{получили } z_1 < z, z = a \cdot z_1, z_1 - \text{делитель } z}{\text{запускаем 2-й раз, получили } \frac{k'}{z}}$

Если $\text{НОД}(k', z) = 1$, то получили z

Иначе, $\overset{\text{получили } z_2 - \text{делитель } z}{\text{если } \text{НОД}(k, k') = 1, \text{ то } z = \text{НОК}(z_1, z_2)}$

$$z = 44, k = 6, \frac{k}{z} = \frac{6}{44} = \frac{3}{22}, z_1 = 22$$

$$k' = 11, \frac{k'}{z} = \frac{11}{44} = \frac{1}{4}, z_2 = 4$$

$$\underline{\text{НОК}(z_1, z_2) = 44 = z}$$

Д.З. Алгоритм Уорда для $M=15$