11 - Algorytm Shora

Saturday, 22 June 2024 21:01

Będziemy chcieli znaleźć okres funkcji $f(x) = a^x \pmod A$

f jest okresowa i różnowartościowa między okresami.

f nie musi być określona na całym $\mathbb{N}$. Wystarczy na $N = 2^n$.

Skonstruujmy bramkę O_f.

$\otimes$ oznacza konkatenację dwóch ciągów bitowych

$O_f : 2^{2N} \to 2^{2N}$

$O_f(x \otimes y) = x \otimes (f(x) \oplus y)$ żeby było odwracalne :)

- Bierzemy $2n$ kubitów w stanie 0: $|0^{2n}\rangle$
- Na pierwsze N qubitów nakładamy H,

otrzymujemy stan to: $\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \otimes |0^n\rangle$

- Na całość nakładamy O_f:

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

Dokonujemy pomiaru, ale tylko N ostatnich q-bitów

Załóżmy znamy $f(x) = y$, a pierwsze N bitów równomiernie przyjmuje te wartości x', że $f(x') = y$. Niech T to zbiór tych x'.

Stan całego układu $\frac{1}{\sqrt{T}} \sum_{x \in T} x \otimes y$

Przyjrzyjmy się zbiorowi T:

f jest okresowa o okresie r, więc $T = \{s, s+r, s+2r, \dots\}$

Załóżmy, że $r \mid N$:) $d := N/r$

Zatem $|T| = d$

Nasz stan to $\frac{1}{\sqrt{d}} \sum_{x=0}^{N-1} b_x |x\rangle$ gdzie

$b_x = \begin{cases} 1 : x = s \pmod r \\ 0 : \text{else} \end{cases}$

Chcemy wyznaczyć r.

Kwantowa transformata Fouriera

$$Q = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & w & w^2 & \cdots & w^{N-1} \\ \vdots & w^2 & w^4 & \cdots & w^{2(N-1)} \\ & \vdots & & & \\ 1 & w^{N-1} & \cdots & & w^{(N-1)(N-1)} \end{bmatrix}$$

Q jest unitarna, więc można ją skonstruować z bramek.

Fakt: Da się ją skonstruować z $O(n^2)$ bramek H i $R(\phi)$

Jak wygląda stan $v = \frac{1}{\sqrt{d}} \sum_{x=0}^{N-1} b_x |x\rangle$ $\quad b_x = \begin{cases} 1 : x \equiv s \pmod r \\ 0 : \text{else} \end{cases}$

po przepuszczeniu przez Q?

$w := Q \cdot v$

$w_j = b_0 + b_1 \cdot w^j + b_2 \cdot w^{2j} + \dots + b_{N-1} \cdot w^{j(N-1)}$

Zatem $w_j = \frac{1}{\sqrt{d}} \left(w^{sj} + w^{(s+r)j} + \dots \right) = \frac{1}{\sqrt{d}} w^{sj} \sum_{i=0}^{d-1} w^{i \cdot r \cdot j}$

Jeśli $N \mid r \cdot j$ to $w^{r \cdot j} = 1$, zatem $w_j = w^{sj} \sqrt{d}$

Jeśli $N \nmid r \cdot j$ to $w_j = \frac{1}{\sqrt{d}} w^{sj} \frac{w^{r \cdot j \cdot d} - 1}{w^{rj} - 1} = 0$

$N \mid r \cdot j$ iff $d \mid j$ zatem wynikowy stan to $\sqrt{d} \cdot w^{sj} \sum_{d \mid x} |x\rangle$

Wykonując wiele pomiarów można zabrać gcd wyników.

Jeśli $r \nmid N$ to „da się" odtworzyć wynik to wyniki bliskie ułamkowi $\frac{j \cdot N}{r}$ są najbardziej prawdopodobne. □