Kvantumalgoritmusok
Kvantum diszkrét logaritmus algoritmus

Diszkrét logaritmus probléma

A fázis becslés és perióduskereső algoritmus segít a diszkrét logaritmus probléma megoldásában is, sőt kvantum polinomiális időben megoldható a probléma.

Probléma

Input: Egy páratlan egész szám $N, a, b \in \mathbb{Z}_N^*$ úgy, hogy $b \equiv a^t \mod N$, ahol $t \in \mathbb{Z}_r$ és r az a rendje $\mod N$

Output: t

A t hatványt az a alapú b *diszkrét logaritmusának* hívjuk modulo N.

Megjegyzés: Ezt a problémát DL-problémának is szokták hívni.

Kvantum polinomiális idő

Ahhoz, hogy kvantum polinomiális időben találjunk megoldást a diszkrét logaritmus problémára a következőekben tegyük fel, hogy az a rendje r modulo N egy prímszám.

Továbbá, feltesszük, hogy $t > 1$, mivel a $t = 0$ és $t = 1$ eset ránézésre megoldható.

Fő ötletek

- Becslünk egy paramétert $n \in \mathbb{N}$

Fő ötletek

- Becslünk egy paramétert $n \in \mathbb{N}$
- Alkalmazzunk az U_a és U_b unitér operátort, melynek sajátértékei $e^{2\pi i \frac{k}{r}}$ és $e^{2\pi i \frac{tk}{r}}$, $0 \leq k < r$, mivel $b \equiv a^t \mod N$

Fő ötletek

- Becslünk egy paramétert $n \in \mathbb{N}$
- Alkalmazzunk az U_a és U_b unitér operátort, melynek sajátértékei $e^{2\pi i \frac{k}{r}}$ és $e^{2\pi i \frac{tk}{r}}$, $0 \leq k < r$, mivel $b \equiv a^t \mod N$
- Használjuk a kvantum fázisbecslést, így találunk (x, y) párt, hogy $\frac{x}{2^n}$ és $\frac{y}{2^n}$ közel legyen $\frac{k}{r}$ és $\frac{tk \mod r}{r}$-hez valamilyen $k \in \mathbb{Z}_r^*$ esetén és így

$$k = \lfloor \frac{rx}{2^n} \rceil \text{ és } r = \lfloor \frac{ry}{2^n} \rceil$$

Fő ötletek

- Becslünk egy paramétert $n \in \mathbb{N}$
- Alkalmazzunk az U_a és U_b unitér operátort, melynek sajátértékei $e^{2\pi i \frac{k}{r}}$ és $e^{2\pi i \frac{tk}{r}}$, $0 \leq k < r$, mivel $b \equiv a^t \mod N$
- Használjuk a kvantum fázisbecslést, így találunk (x, y) párt, hogy $\frac{x}{2^n}$ és $\frac{y}{2^n}$ közel legyen $\frac{k}{r}$ és $\frac{tk \mod r}{r}$-hez valamilyen $k \in \mathbb{Z}_r^*$ esetén és így

$$k = \lfloor \frac{rx}{2^n} \rceil \text{ és } r = \lfloor \frac{ry}{2^n} \rceil$$

- Mivel r prímszám, tudjuk hogy $gcd(k, r) = 1$.

Fő ötletek

- Becslünk egy paramétert $n \in \mathbb{N}$
- Alkalmazzunk az U_a és U_b unitér operátort, melynek sajátértékei $e^{2\pi i \frac{k}{r}}$ és $e^{2\pi i \frac{tk}{r}}$, $0 \leq k < r$, mivel $b \equiv a^t \mod N$
- Használjuk a kvantum fázisbecslést, így találunk (x, y) párt, hogy $\frac{x}{2^n}$ és $\frac{y}{2^n}$ közel legyen $\frac{k}{r}$ és $\frac{tk \mod r}{r}$-hez valamilyen $k \in \mathbb{Z}_r^*$ esetén és így

$$k = \lfloor \frac{rx}{2^n} \rceil \text{ és } r = \lfloor \frac{ry}{2^n} \rceil$$

- Mivel r prímszám, tudjuk hogy $gcd(k, r) = 1$.
- Most kiszámíthatjuk k'-t: $kk' \equiv 1 \mod r$ és kapunk

$$t = k' \lfloor \frac{ry}{2^n} \rceil \mod r$$

Az algoritmus

A következő kvantum diszkrét logaritmus algoritmus megoldja a diszkrét logaritmus problémát legalább 32% valószínűséggel és $\mathcal{O}((logN)^3)$ időben.

Input: N, a, b, r such that r is the order of a modulo N, r is a prime number, and $b \equiv a^t \bmod N$ for some $t \in \mathbb{Z}_r^*$.

Output: The discrete logarithm t of b to base a modulo N or "FAILURE"

1: DL(N, a, b, r)
2: $n \leftarrow \lceil \log_2 r \rceil + 1$
3: Apply the quantum circuit Q_{DL} from Figure 6.6.1 and obtain $(x, y) \in \mathbb{Z}_{2^n}^2$
4: $k \leftarrow \lfloor xr/2^n \rceil \bmod r$
5: **if** $k \neq 0$ **then**
6: $l \leftarrow \lfloor yr/2^n \rceil \bmod r$
7: $t \leftarrow lk^{-1} \bmod r$
8: **return** t
9: **end if**
10: **return** "FAILURE"
11: **end**

Az alábbi kvantum áramkör $\frac{64(r-1)}{r\pi^4}$ valószínűséggel talál két egész számot $x, y \in \mathbb{Z}_{2^n}$ úgy hogy

$$k = \lfloor \frac{rx}{2^n} \rfloor \text{ és } r = \lfloor \frac{ry}{2^n} \rfloor$$