Trovare il periodo di f.

Sia f una funzione periodica a valori in $\{0,1\}$ t.c.

$f(j) = f(j+r)$ per $0 < r < 2^t$

$j, r \in \mathbb{N}$. Data una black-box U, t.c. $U|x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle$

Esiste un alg. quantistico che usa $\underline{1}$ interrogazione e

$O(L^2)$ operazioni

Oss. In pratica il dominio di f è finito e dipende dall'accuratezza scelta per r

e severa trasformata di Fourier inversa. Osserviamo che vale:

Proprietà di invarianza rispetto allo shift della FT.

Sia G un insieme di indici per gli stati rispetto a una base ortonormale (es. se è un sistema con t qubits $G = \{0, \dots, 2^{t-1}\}$) e sia $H \subset G$. Consideriamo

$$\sum_{h \in H} \alpha_h \cdot |h\rangle \to \sum_{g \in G} \underbrace{\sum_{h \in H} \alpha_h e^{\frac{2\pi i g h}{|G|}}}_{\tilde{\alpha}_g} |g\rangle$$

e supponiamo di applicare un operatore unitario $U_k |g\rangle \to |g+k\rangle$

e poi la FT. Allora

$$U_k\left(\sum_{h\in H} \alpha_h |h\rangle\right) = \sum_{h\in H} \alpha_h |h+k\rangle \longrightarrow$$

$$\sum_{g\in G}\sum_{h\in H} \alpha_h e^{\frac{2\pi i g(h+k)}{G}} |g\rangle =$$

$$\sum_{g\in G}\sum_{h\in H} e^{\frac{2\pi i g k}{|G|}} \cdot \tilde{\alpha}_g \cdot |g\rangle =$$

$$\sum_{g\in G} \tilde{\alpha}_g |g\rangle .$$

Ossia FT di f è invariante sulle classi laterali di H se f su G è costante sulle classi laterali di H.

Vediamo l'algoritmo.

Input: 1. Black box $U|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$

2. $|0\rangle$ per la valutazione di f

3. $t = O(L + \log(\frac{1}{\varepsilon}))$ qbits $|0\rangle$

OUTPUT: il minimo r t.c $f(x+r) = f(x)$

Runtime Una chiamata di U e $O(L^2)$ operazioni. successo $O(1)$

1. $|0\rangle|0\rangle$ stato iniziale

2. $\frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle|0\rangle$ sovrapposizione

3. $\frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle|f(j)\rangle$ applica U

$\approx \frac{1}{\sqrt{r\,2^t}} \sum_{l=0}^{r-1} \sum_{j=0}^{2^t-1} e^{\frac{2\pi i l j}{r}} |\hat{f}(l)\rangle$ **

4 $\frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} |\widetilde{\frac{l}{r}}\rangle|\hat{f}(l)\rangle$ inversa FT

5 $|\widetilde{\frac{l}{r}}\rangle$ misura 1° registro 6. r FC

** ? Introduciamo stato

$$|\hat{f}(l)\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{-\frac{2\pi i l j}{r}} |f(j)\rangle$$

che è la FT ristretta a $H=\{0,\dots,r-1\}$ usando "come stati" $|f(j)\rangle \in \{0,\dots,r-1\}$

Vale:

⊗ $$|f(j)\rangle = \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} e^{\frac{2\pi i l j}{r}} |\hat{f}(l)\rangle$$

Dal momento che f e le altre che in ⊗ sono periodiche

⊗ vale $\forall\, j \in \{0,\dots,2^t-1\}$

e quindi possiamo scrivere

$$|\psi\rangle = \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle\,|f(j)\rangle =$$

$$\frac{1}{\sqrt{2^t-1}} \sum_{j=0}^{2^t-1} |j\rangle \left(\frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} e^{\frac{-2\pi i l j}{r}} |\hat{f}(l)\rangle \right)$$

$$= \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} \left(\frac{1}{\sqrt{2^t-1}} \sum_{j=0}^{2^t-1} e^{\frac{-2\pi i l j}{r}} |j\rangle \right) |\hat{f}(l)\rangle$$

In questo modo se misuriamo il secondo registro che ci "sceglie" $l \in \{0, \dots, r-1\}$ otteniamo nel primo registro

$$\frac{1}{\sqrt{2^t-1}} \sum_{j=0}^{2^t-1} e^{-\frac{2\pi i j l}{r}} |j\rangle$$

applicando l'inversa di FT (se $\{0, \ldots, 2^{t-1}\}$) stimiamo una fase $|\tilde{\frac{\ell}{r}}\rangle$ nel primo registro. Applicando FC troviamo r.

Un'osservazione: Se $r \mid 2^t = N$ più semplice. Infatti se ci 3. abbiamo

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

e misuriamo il 2° registro ci troviamo in uno stato

$$|\psi_1\rangle = \frac{1}{\sqrt{\frac{N}{r}}} \sum_{j=0}^{r-1} |j\rangle |z\rangle$$

$$\underline{j \mid f(j)=z}$$

e $z \in \{f(0), \dots, f(r-1)\}$ $\frac{N}{r}$

perché tanti sono i valori di

j t.c. $f(j)=z$. Se chiamiamo

j_0 il minimo j nella somma

dato che f ha periodo r

possiamo scrivere

$$|\psi_1\rangle = \frac{1}{\sqrt{\frac{N}{r}}} \sum_{j=0}^{\frac{N}{r}-1} |j_0 + rj\rangle |z\rangle$$

Applicando l'inversa FT (su $\{0,\dots,N-1\}$)

al primo stato

$$F^{-1}|\psi_1\rangle = \frac{1}{\sqrt{N/r}} \sum_{j=0}^{N/r-1} \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} e^{\frac{-2\pi i (j_0 + rj) l}{N}} |l\rangle =$$

$$= \frac{\sqrt{r}}{N} \sum_{l=0}^{N-1} e^{\frac{-2\pi i j_0 l}{N}} \cdot \underbrace{\sum_{j=0}^{N/r-1} \left(e^{\frac{-2\pi i r l}{N}}\right)^j}_{= \begin{cases} N/r & \text{se } \frac{rl}{N} \in \mathbb{N} \\ 0 & \text{altrimenti} \end{cases}} |l\rangle$$

Così se misuriamo osserviamo

solo uno stato $|l\rangle$ con l multiplo

di $\frac{N}{r}$. Quindi se applichiamo

l'algoritmo due volte troviamo

$$l_1 = a\left(\frac{N}{r}\right) \quad l_2 = b\left(\frac{N}{r}\right)$$

Con buona probabilità $(a,b)=1$

$\Rightarrow \gcd(\ell_1, \ell_2) = \frac{N}{r}$ e dato

che conosciamo N, troviamo r

—

Esercizio. Sia U_y d'operatore t.c $U_y |f(x)\rangle = |f(x+y)\rangle$ per f periodica $f(x+r) = f(x)$.

1. Provare che gli autovettori di U_f sono $|\hat{f}(\ell)\rangle$ e calcolare gli autovalori associati

(Notazioni di prima)

Logaritmo discreto

Problema dati a e $b = a^s$

trovare s.

Consideriamo la funzione

$$f(x_1, x_2) = a^{sx_1 + x_2} \bmod N$$

questa funzione è periodica

perché $f(x_1 + \ell, x_2 - \ell s) = f(x_1, x_2)$

ma il periodo $(\ell, -\ell s)$

Vediamo come usare f

per trovare il logaritmo

discreto di $b = a^s$

Definiamo la black box

$$U|x_1\rangle|x_2\rangle|y\rangle = |x_1\rangle|x_2\rangle|y \oplus f(x_1, x_2)\rangle$$

e sia $r = O(a) \bmod N$

LOG Discreto

Input: 1. $U|x_1\rangle|x_2\rangle|y\rangle = |x_1\rangle|x_2\rangle|y \oplus f(x_1,x_2)\rangle$

con $f(x_1,x_2) = b^{x_1} \cdot a^{x_2}$

2. $|0\rangle$ stato per la val. della funzione

3. due registri con $t = \Theta\left(\lceil \log r \rceil + \log\left(\frac{1}{\varepsilon}\right)\right)$ qbits inizializzati a $|0\rangle$

output il minimo s t.c. $a^s = b$

Runtime Un uso di U e $O(\lceil \log r \rceil^2)$ operaz.

Probabilità di successo $\Theta(1)$.

---

① cfr Nielsen Chuang.

② Supponiamo di conoscere $\langle g \rangle = \mathbb{Z}_N^*$

e $R = \varphi(N)$ (fattorizzazione)

Dato $b \in \mathbb{Z}_N^*$ vogliamo trovare

l t.c. $g^l \equiv b \ (N)$

Consideriamo $f(x_1,x_2) = b^{x_1} \cdot g^{x_2} = g^{l x_1 + x_2}$

lo stato

$$|\psi\rangle = \frac{1}{R} \sum_{j_1, j_2 = 0}^{R-1} |j_1\rangle |j_2\rangle |f(j_1, j_2)\rangle$$

se misuriamo il terzo registro otteniamo un valore q^z con $z \in \{0, \dots, R-1\}$ quindi i primi due registri sono nello stato

$$|\psi_1\rangle = \frac{1}{R} \sum_{(j_1, j_2) \in \Lambda} |j_1\rangle |j_2\rangle$$

dove $\Lambda = \{(j_1, j_2) \cdot l j_1 + j_2 = z\}$ e quindi

$$|\psi_1\rangle = \frac{1}{\sqrt{R}} \sum_{j=0}^{R-1} |j\rangle |z - lj\rangle$$

se applichiamo l'inversa FT a entrambi i registri ($\in \{0, \dots, R-1\}$)

otteniamo

$$|\psi_2\rangle = \frac{1}{R^{3/2}} \sum_{j=0}^{R-1} \sum_{s,k=0}^{R-1} e^{\frac{-2\pi i (sj + k(z-q_j))}{R}} |s\rangle|k\rangle$$

se vi scriviamo questo stato

otteniamo

$$\alpha_{sk} = \frac{1}{R^{3/2}} e^{\frac{-2\pi i k z}{R}} \cdot \sum_{j=0}^{R-1} \left(e^{-2\pi i (s - lk)} \right)^j$$

e quindi possiamo solo osservare

gli stati t.c. $s \equiv lk \ (R)$

altrimenti somma $= 0$

questo ci dà uno stato $|k, ls \ (R)\rangle$

quindi se calcoliamo $\bar{k}'$ ok.

$\bar{k}'$ esiste se $(k, R) = 1$ che

vale con $\frac{1}{2} = \frac{\varphi(R)}{R}$. (N, C)