PC 5228 Lecture notes 27/10/2023

① Grover search algorithm

② Simon's algorithm

Grover search algorithm

(I) Algorithm (Review)

- Problem: Given a data set S with a labeled elements $s \in A$ we are able to check if a given $x \in A$ is the solution or not

$$f(x) = \begin{cases} 1 & x = s \\ 0 & x \neq s \end{cases}$$

our goal is to find target element x^* using the fewest queries possible.

- Classical brute-force search $|A| = N$
  - ▷ in the worst case, we must query all N possible elements
  - ▷ on average, query half of the elements
  - ▷ complexity: $O(N)$

- Grover's algorithm
  - ▷ oracle (subroutine): we are still able to check if a given element is the solution or not

$$f(y) = \begin{cases} 1, & x = s \\ 0, & x \neq s \end{cases}$$

Quantum description:

① $\tilde{U}_f^A |x\rangle = (-1)^{f(x)} |x\rangle = \begin{cases} -|x\rangle, & x = s \\ |x\rangle, & x \neq s \end{cases}$ $\tilde{U}_f = \mathbb{I} - 2|s\rangle\langle s|$

② $U_f^{AB} |x\rangle_A |q\rangle_B = |x\rangle_A |q \oplus f(x)\rangle_B$

$$U_f(|x\rangle|-\rangle) = \frac{1}{\sqrt{2}}\left(U_f(|x\rangle|0\rangle) - U_f(|x\rangle|q\rangle)\right)$$
$$= \frac{1}{\sqrt{2}}\left(|x\rangle|f(x)\rangle - |x\rangle|1 \oplus f(x)\rangle\right)$$

$$= (\hat{U}_f |x\rangle)|-\rangle$$

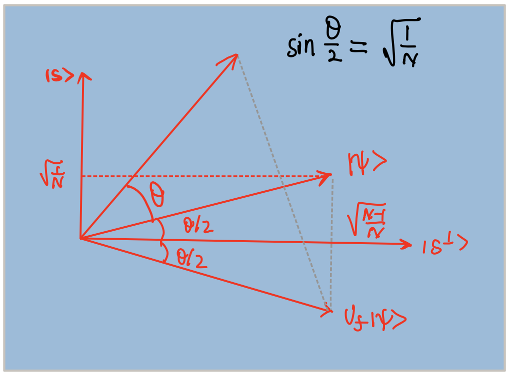
▷ Refection

$$|\psi\rangle = \frac{1}{\sqrt{N}} \Sigma_x |x\rangle = H^{\otimes n} |0\rangle \otimes \cdots \otimes |0\rangle$$

$$U_\psi = 2|\psi\rangle\langle\psi| - \mathbb{I} = H^{\otimes n} (2|0\rangle\langle 0| - \mathbb{I}) H^{\otimes n}$$

▷ Grover operation

$$G = U_\psi \tilde{U}_f$$



$$|s\rangle, \; |s^\perp\rangle = \frac{1}{\sqrt{N-1}} \Sigma_{x\neq s} |x\rangle$$

$$|\psi\rangle = \frac{1}{\sqrt{N}} |s\rangle + \sqrt{\frac{N-1}{N}} |s^\perp\rangle$$

Algorithm: ① initial state $|\psi\rangle = H^{\otimes n}(|0\rangle \otimes \cdots \otimes |0\rangle)$

② apply Grover iteration $G^k |\psi\rangle = |s^{(k)}\rangle \simeq |s\rangle$

③ measure and output $s^{(k)}$

(II) Correctness

(1) Geometric analysis (Done)

(2) Algebraic analysis

- key observation: During the computation, all states are in the plane spanned by $|s\rangle$ and $|s^\perp\rangle$

- Matrix form

▷ $|s\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ $\quad |s^\perp\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

▷ $\tilde{U}_f |s\rangle = -|s\rangle$ $\quad \tilde{U}_f |s^\perp\rangle = |s^\perp\rangle$

$$\tilde{U}_f = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

▷
$$\begin{aligned}
U_\psi |s\rangle &= 2|\psi\rangle\langle\psi|s\rangle - |s\rangle \\
&= 2|\psi\rangle\langle\psi|s\rangle - |s\rangle \\
&= 2\sqrt{\tfrac{1}{N}}\left(\frac{1}{\sqrt{N}}|s\rangle + \sqrt{\frac{N-1}{N}}|s^\perp\rangle\right) - |s\rangle \\
&= 2\frac{1}{N}|s\rangle + \frac{2\sqrt{N-1}}{N}|s^\perp\rangle - |s\rangle \\
&= \frac{2-N}{N}|s\rangle + \frac{2\sqrt{N-1}}{N}|s^\perp\rangle
\end{aligned}$$

$$\begin{aligned}
U_\psi |s^\perp\rangle &= 2|\psi\rangle\langle\psi|s^\perp\rangle - |s^\perp\rangle \\
&= 2\sqrt{\frac{N-1}{N}}|\psi\rangle - s^\perp \\
&= 2\sqrt{\frac{N-1}{N}}\left(\frac{1}{\sqrt{N}}|s\rangle + \sqrt{\frac{N-1}{N}}|s^\perp\rangle\right) - |s^\perp\rangle \\
&= \frac{2\sqrt{N-1}}{N}|s\rangle + \left(\frac{2(N-1)}{N} - 1\right)|s^\perp\rangle \\
&= \frac{2\sqrt{N-1}}{N}|s\rangle + \frac{N-2}{N}|s^\perp\rangle
\end{aligned}$$

$$U_\psi = \begin{pmatrix} \frac{N-2}{N} & \frac{2\sqrt{N-1}}{N} \\ \frac{2\sqrt{N-1}}{N} & \frac{2-N}{N} \end{pmatrix}$$

▷ $$G = U_\psi \tilde{U}_f = \begin{pmatrix} \frac{N-2}{N} & -\frac{2\sqrt{N-1}}{N} \\ \frac{2\sqrt{N-1}}{N} & \frac{N-2}{N} \end{pmatrix}$$

Set $\sin\theta = \frac{2\sqrt{N-1}}{N}$

$$G = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \quad \text{rotation matrix}$$

Notice that $\sin\theta = \sin 2\times\frac{\theta}{2}$

$$= 2\sin\theta/2 \cos\frac{\theta}{2}$$

$$= 2\sqrt{\frac{1}{N}}\cdot\sqrt{\frac{N-1}{N}}$$

coincides with the one we give before.

▷ Initial state is $|\psi\rangle = \sqrt{\frac{1}{N}}|s\rangle + \sqrt{\frac{N-1}{N}}|s^\perp\rangle$

$$= \sin\frac{\theta}{2}|s\rangle + \cos\frac{\theta}{2}|s^\perp\rangle$$

$$G^k = \begin{pmatrix} \cos k\theta & -\sin k\theta \\ \sin k\theta & \cos k\theta \end{pmatrix}$$

$$|\text{output}\rangle = G^k|\psi\rangle$$

$$= G^k\begin{pmatrix} \cos\frac{\theta}{2} \\ \sin\frac{\theta}{2} \end{pmatrix}$$

$$= \begin{pmatrix} \cos k\theta & -\sin k\theta \\ \sin k\theta & \cos k\theta \end{pmatrix}\begin{pmatrix} \cos\frac{\theta}{2} \\ \sin\frac{\theta}{2} \end{pmatrix}$$

$$= \begin{pmatrix} \cos k\theta\cos\frac{\theta}{2} - \sin k\theta\sin\frac{\theta}{2} \\ \sin k\theta\cos\frac{\theta}{2} + \cos k\theta\sin\frac{\theta}{2} \end{pmatrix}$$

$$= \begin{pmatrix} \cos(k\theta+\frac{\theta}{2}) \\ \sin(k\theta+\frac{\theta}{2}) \end{pmatrix} \begin{matrix} \rightsquigarrow s^\perp \\ \rightsquigarrow s \end{matrix}$$

① After k iteration, the probability of observing the target element s is

$$\Pr(\text{output}=s) = |\langle s|\text{output}\rangle|^2$$

$$= [\sin(k\theta+\frac{\theta}{2})]^2$$

② For $N \gg 1$, $\sin\frac{\theta}{2} = \sqrt{\frac{1}{N}} \ll 1$, $\frac{\theta}{2} \simeq \sqrt{\frac{1}{N}}$

if the angular error ε is at most $\sqrt{\frac{1}{N}}$, we see that

$$k\theta + \frac{\theta}{2} \geqslant \frac{\pi}{2} - \frac{\theta}{2}$$

$$\Leftrightarrow \quad (2k+2)\frac{\theta}{2} \geqslant \frac{\pi}{2}$$

$$2k+2 \geqslant \frac{\pi}{\theta} \simeq \frac{\pi}{\sqrt{\frac{1}{N}}} = \pi\sqrt{N}$$

$$k \geqslant \frac{\pi\sqrt{N}-2}{2}$$

$$k^* := \left[\frac{\pi\sqrt{N}-2}{2}\right] + 1$$

☆ complexity: $O(\sqrt{N})$.

(III) More than one solution case

Data set N

solution set $1 \leq M < N$

$$|s\rangle = \frac{1}{\sqrt{M}} \sum_{x:\,sol} |x\rangle$$

$$|s^\perp\rangle = \frac{1}{\sqrt{N-M}} \sum_{x:\,not\ sol} |x\rangle$$

$$|\psi\rangle = H^{\otimes N} |0\rangle^{\otimes N} = \sqrt{\frac{M}{N}}\, |s\rangle + \sqrt{\frac{N-M}{N}}\, |s^\perp\rangle$$

$$\sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}$$

$M \ll N \Rightarrow$ complexity $O(\sqrt{N/M})$

(IV) Grover search is optimal

Theorem: Any quantum algorithm that can realize the search with success probability $Pr(succ) > \frac{1}{2}$ must call the oracle $\Omega(\sqrt{N})$ times.

$\Omega(\sqrt{N/M})$

Proof. ① General k-call quantum algorithm output state

$$|out^{(k)}\rangle = U_k \tilde{U}_f U_{k-1} \tilde{U}_f \cdots U_1 \tilde{U}_f |\psi\rangle$$

where $|\psi\rangle$ is initial state, $U_1, \cdots, U_k$ are unitaries, $\tilde{U}_f$ is oracle operation.

$Pr(succ) = |\langle s | out^{(k)}\rangle|^2$, $|s\rangle$ is solution state.

② Suppose $Pr(succ) > 1/2$, viz., $|\langle s | out^{(k)}\rangle|^2 > 1/2$, we have

$$\| |out^{(k)}\rangle - |s\rangle \|^2 = 2 - 2|\langle s | out^{(k)}\rangle| \le 2 - \sqrt{2}$$

Take average over all possible solution elements

$$\varepsilon_k = \Sigma_s \| |out_s^{(k)}\rangle - |s\rangle \| \le (2-\sqrt{2}) N.$$

③ Denote $|\phi^{(k)}\rangle = U_k \cdots U_1 |\psi\rangle$

$$\mathcal{D}_k = \Sigma_s \| |out_s^{(k)}\rangle - |\phi^{(k)}\rangle \|^2$$

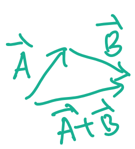
Claim: $\mathcal{D}_k \le 4k^2$

proof: Mathematical induction. (Exercise)

▷ $k = 0$, true

∘ suppose k case true

$$\mathcal{D}_{k+1} = \sum_s \| |out_s^{(k)}\rangle - |\phi^{(k)}\rangle \|^2$$



$$= \sum_s \| U_k \tilde{U}_f U_{k-1} \tilde{U}_f \cdots \tilde{U}_f |\psi\rangle - U_k \cdots U_1 |\psi\rangle \|^2$$

$$= \Sigma_s \| U_k [\tilde{U}_f U_{k-1} \cdots \tilde{U}_f |\psi\rangle - U_{k-1} \cdots U_1 |\psi\rangle] \|^2$$

$$= \Sigma_s \| \tilde{U}_f |out_s^{(k-1)}\rangle - |\phi^{(k-1)}\rangle \|^2$$

$\| \vec{A} + \vec{B} \|^2 \le \|\vec{A}\|^2 + \|B\|^2 + 2\|A\| \cdot \|B\|$

$$= \Sigma_s \| \tilde{U}_f |out_s^{(k-1)}\rangle - \tilde{U}_f |\phi^{(k-1)}\rangle + \tilde{U}_f |\phi^{(k-1)}\rangle - \phi^{(k-1)} \|^2$$

$$= \Sigma_s \| \underbrace{\tilde{U}_f (|out_s^{(k-1)}\rangle - |\phi^{(k-1)}\rangle)}_{A} + \underbrace{(\tilde{U}_f - I)\, \phi^{(k-1)}}_{B} \|^2$$

$$\le \Sigma_s \|A\|^2 + 2\|A\|\|B\| + \|B\|^2$$

Notice $B = (\tilde{U}_f - I)|\phi^{(k-1)}\rangle$

$$= -2|s\rangle\langle s|\phi^{(k-1)}\rangle$$

$$D_{k+1} \leq D_k + 2\|A\|\|B\| + \sum_s 4|\langle s|\phi^{(k-1)}\rangle|^2$$

$$= D_k + 2\|A\|\|B\| + 4$$

$$2\|A\|\cdot\|B\| = 4\ \|U_f(|out_s^{k-1}\rangle - |\phi^{k-1}\rangle)\|\cdot|\langle s|\phi^{(k-1)}\rangle|$$

$$= 4\quad a_s\cdot b_s$$

$$\Sigma_s\, a_s\cdot b_s \leq (\Sigma_s a_s^2)^{1/2}(\Sigma_s b_s^2)^{1/2}$$

$$= \sqrt{D_k}\cdot 1$$

$$D_{k+1} \leq D_k + 4\sqrt{D_k} + 4$$

$$\leq 4k^2 + 4\sqrt{4k^2} + 4$$

$$= 4k^2 + 8k + 4 = 4(k+1)^2$$

④. $D_k = \Sigma_s \| |out_s^k\rangle - |\phi^k\rangle \|^2$

$$= \Sigma_s \| \underbrace{(|out_s^k\rangle - |s\rangle}_{J_s} + \underbrace{|s\rangle - |\phi^k\rangle}_{K_s} \|^2$$

$$\geq \Sigma_s\ J_s^2 - 2|J_s|\cdot|K_s| + K_s^2$$

$$= \mathcal{E}_k + \underbrace{\Sigma_s \| |\phi^k\rangle - |s\rangle \|^2}_{\mathcal{F}_k} - \Sigma_s\, 2\,|J_s|\cdot|K_s|$$

$$\Sigma_s\, 2\,|J_s|\cdot|K_s| \leq 2\,(\Sigma_s |J_s|^2)^{1/2}(\Sigma_s |K_s|^2)^{1/2}$$

$$\leq 2\sqrt{\mathcal{E}_k\mathcal{F}_k}$$

$$D_k \geq \mathcal{E}_k + \mathcal{F}_k - 2\sqrt{\mathcal{E}_k\mathcal{F}_k}$$

$$= (\sqrt{\mathcal{F}_k} - \sqrt{\mathcal{E}_k})^2$$

Using the fact that for N basis $|s\rangle$ and a $|\Psi\rangle$

$$\Sigma_s \| |s\rangle - |\Psi\rangle \|^2 \geq 2N - 2\sqrt{N}.$$

we see $\mathcal{F}_k \geq 2N - 2\sqrt{N}$

⑤ Now using ② and ④ we have

$$D_k \geq (\sqrt{\mathcal{F}_k} - \sqrt{\mathcal{E}_k})^2$$

$$\geq M\cdot\sqrt{N}$$ M is a constant.

Simon's algorithm

(I) Simon's problem ⊆ Hidden subgroup problem.

- Given a periodic function $f: \{0,1\}^n \to \{0,1\}^n$. find the period s of the function such that
  $$f(x \oplus s) = f(y).$$
  where addition is bit-wise and modulo 2.

- $f(x) = f(y)$ if and only if $x \oplus y \in \{0^n, s\}$.
- $x \oplus s = y \Leftrightarrow x = y \oplus s \Leftrightarrow s = x \oplus y$

• Example. $n=3$, $s = 110$

x	$x \oplus s$
000	110
001	111
⋮	⋮

(II) Classical solution.

① Input pair x, y, check if $f(x) = f(y)$

② If $f(x) = f(y)$, $s = x \oplus y$.

Complexit $O(2^{n-1} + 1) = O(\sqrt{N} + 1)$

brute-force check

(III) Simon's algorithm.

- Oracle $U_f(|x\rangle |y\rangle) = |x\rangle |y \oplus f(x)\rangle$

- Hadamard gate $H^{\otimes n}$

$$|0\cdots 0\rangle\, |0\cdots 0\rangle \mapsto |+\cdots +\rangle\, |0\cdots 0\rangle$$

Recall $H|x\rangle = \frac{1}{\sqrt{2}} |0\rangle + (-1)^x |1\rangle = \frac{1}{\sqrt{2}} \sum_z (-1)^{x\cdot z} |z\rangle$

$$H^{\otimes n} |x_1 \cdots x_n\rangle = \frac{1}{\sqrt{2^n}} \sum_{\vec{z}} (-1)^{\vec{z}\cdot\vec{x}} |z_1 \cdots z_n\rangle$$

- Algorithm:

① initial state $|0\cdots 0\rangle_A |0\cdots 0\rangle_B$

② Apply $H^{\otimes}_A$ $\quad \frac{1}{\sqrt{2^n}} \sum_x |x\rangle |0\cdots 0\rangle$

③ Apply oracle $\quad \frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle$

④ Apply $H^{\otimes n}_A$ $\quad \sqrt{\frac{1}{2^n}} \sum_x \frac{1}{\sqrt{2^n}} \sum_z (-1)^{x\cdot z} |z\rangle |f(x)\rangle$

⑤ if $x' = x'' \oplus s$, $\quad f(x') = f(x'' \oplus s) = q$

by measuring $|q\rangle$ over B part, we obtain

$$\frac{1}{\sqrt{2}} \frac{1}{\sqrt{2^n}} \sum_z \left[(-1)^{x'\cdot z} + (-1)^{x''\cdot z}\right] |z\rangle |q\rangle$$

⑥ Now measure A part

$$(-1)^{x'\cdot z} + (-1)^{x''\cdot z} = \begin{cases} \pm 2 & x'\cdot z = x''\cdot z \\ 0 & x'\cdot z \neq x''\cdot z \end{cases}$$

determine z such that

$$x'\cdot z = x''\cdot z$$

This is esuvalent to

$$(x' \oplus x'')\cdot z = 0$$

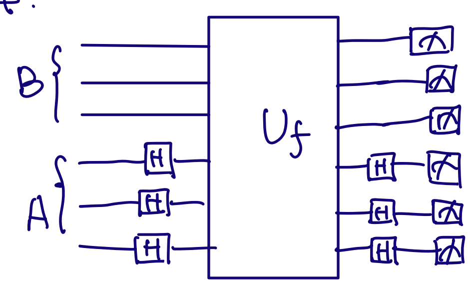
$$\Longleftrightarrow \quad s\cdot z = 0$$

$$s_1 z_1 \oplus \cdots \oplus s_n z_n = 0$$

We obtain one equalition.

⑦ Repeat $O(n)$ times, we obtain n equations, from which we can solve s.

Circuit:



Complexity $\Theta(n) = \Theta(\log N)$