Chapter 7. Quantum Search and Quantum Counting ①

Problem:

Input: $n \in \mathbb{N}$ and a black-box that implements a function

$f: \{0,1\}^n \longrightarrow \{0,1\}$.

$|\{0,1\}^n| = 2^n := N$.

if $|\{\vec{x}: f(\vec{x})=1\}| = M$.

Output: A string $\vec{x} \in \{0,1\}^n$ with $f(\vec{x})=1$. then.

Probability: $\frac{M}{N}$.

classic search $O(N) \leftarrow N-M+1$ times (worst case) to get the object.

✡ Grover's search algorithm. → quadratic speedup. $O(\sqrt{N})$

Applications: unstructured search / brute force.

Cryptography (key search / hash preimages)

① Grover search algorithm with a known number of solutions.

② ~~Geo~~ Las Vegas algorithm with a unknown number of solutions.

③ Quantum Counting.

7.1.2.

"Measure the quantum state"

$P(f(\vec{x})=1) = \sin^2\theta = \frac{M}{N}$.

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{\vec{x}\in\{0,1\}^n} |\vec{x}\rangle := \sqrt{\frac{N-M}{N}}\,|s_0\rangle + \sqrt{\frac{M}{N}}\,|s_1\rangle = \cos\theta\,|s_0\rangle + \sin\theta\,|s_1\rangle.$$

with $|s_0\rangle = \frac{1}{\sqrt{N-M}} \sum_{\substack{\vec{x}\in\{0,1\}^n \\ f(\vec{x})=0}} |\vec{x}\rangle$. $|s_1\rangle = \frac{1}{\sqrt{M}} \sum_{\substack{\vec{x}\in\{0,1\}^n \\ f(\vec{x})=1}} |\vec{x}\rangle$.

$\sin\theta = \sqrt{\frac{M}{N}} \Leftrightarrow \theta = \arcsin\sqrt{\frac{M}{N}}$.

"Amplitude amplification": increase the amplitude of state $|s_1\rangle$.

"G". $G(\cos\alpha|s_0\rangle + \sin\alpha|s_1\rangle) = \cos(\alpha+2\theta)|s_0\rangle + \sin(\alpha+2\theta)|s_1\rangle$.

Grover iterator (unitary operator) then $G(|s\rangle) = \cos(3\theta)|s_0\rangle + \sin(3\theta)|s_1\rangle$.

$\Rightarrow G^k(|s\rangle) = \cos((2k+1)\theta)|s_0\rangle + \sin((2k+1)\theta)|s_1\rangle$

$k \nearrow \left\lfloor \frac{\pi}{4\theta} - \frac{1}{2} \right\rfloor$.

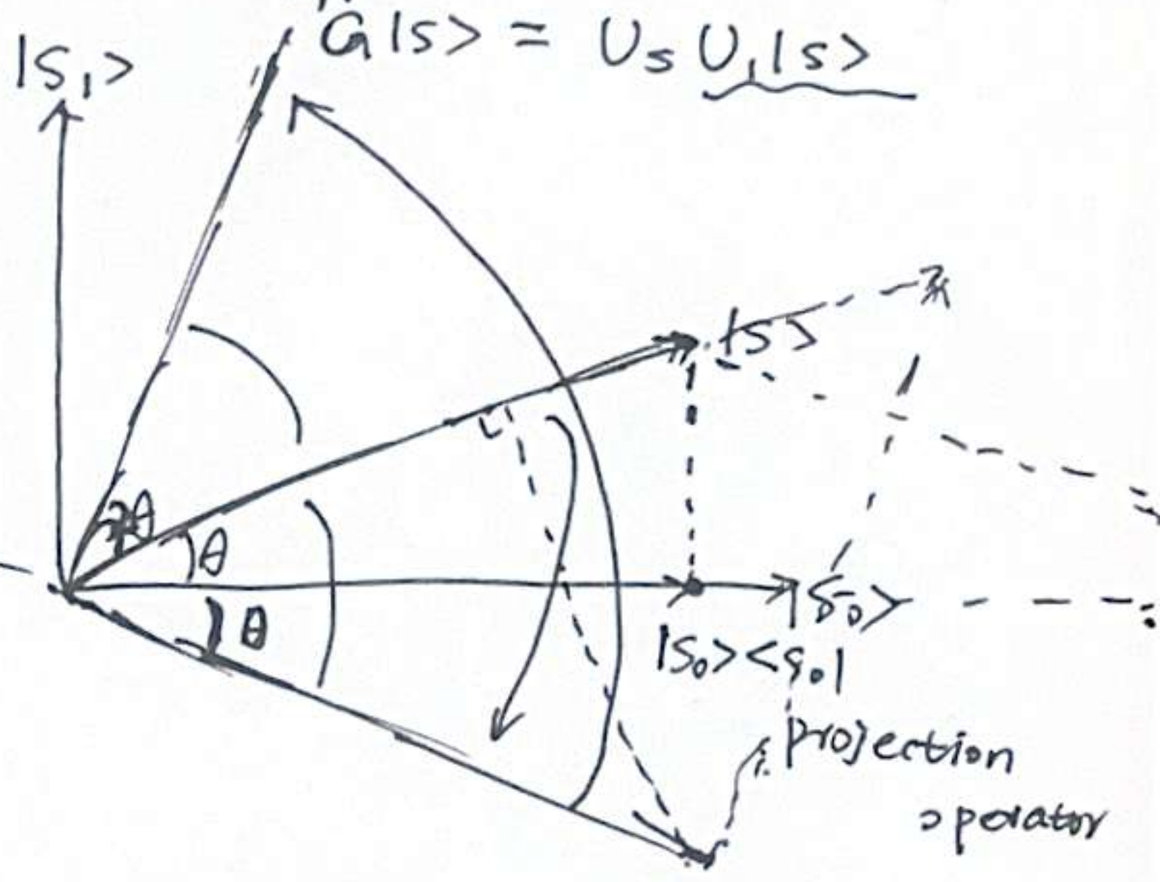
"Quantum circuit for Grover's search algorithm"

$G^k|s\rangle = \cos((2k+1)\theta)|s_0\rangle + \sin((2k+1)\theta)|s_1\rangle$

$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. $H|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \Rightarrow |s\rangle = H^{\otimes n}|0\rangle_n = \left(\frac{1}{\sqrt{2^n}}\right)\sum_{x=0}^{2^n-1}|x\rangle_n$.

"The Grover iterator"

idea.



① oracle U_1

② diffusion operator U_s

$U = U_s U_1$

$= (2|s\rangle\langle s| - I)(I - 2|s_1\rangle\langle s_1|)$.

$\Rightarrow$ 1° $U_1 = 2|s_0\rangle\langle s_0| - I = I - 2|s_1\rangle\langle s_1|$.

then $U_1|s\rangle = 2|s_0\rangle\langle s_0|s\rangle - |s\rangle$

2°. $U_s = 2|s\rangle\langle s| - I$.

~~How to~~

"Implementation of the Grover iterator".

For oracle U_1.

$U_1|s\rangle = U_1(\cos\theta|s_0\rangle + \sin\theta|s_1\rangle)$

$= \cos\theta|s_0\rangle - \sin\theta|s_1\rangle$.

$(-1)^0\cos\theta|s_0\rangle + (-1)^1\sin\theta|s_1\rangle$

P207. (5.1.2)

$U_f : \mathbb{H}_2 \to \mathbb{H}_2 \quad |x\rangle|y\rangle \longmapsto |x\rangle|f(x)\oplus y\rangle = |x\rangle X^{f(x)}|y\rangle$.

$(a\vee b)\wedge\neg(a\wedge b)$

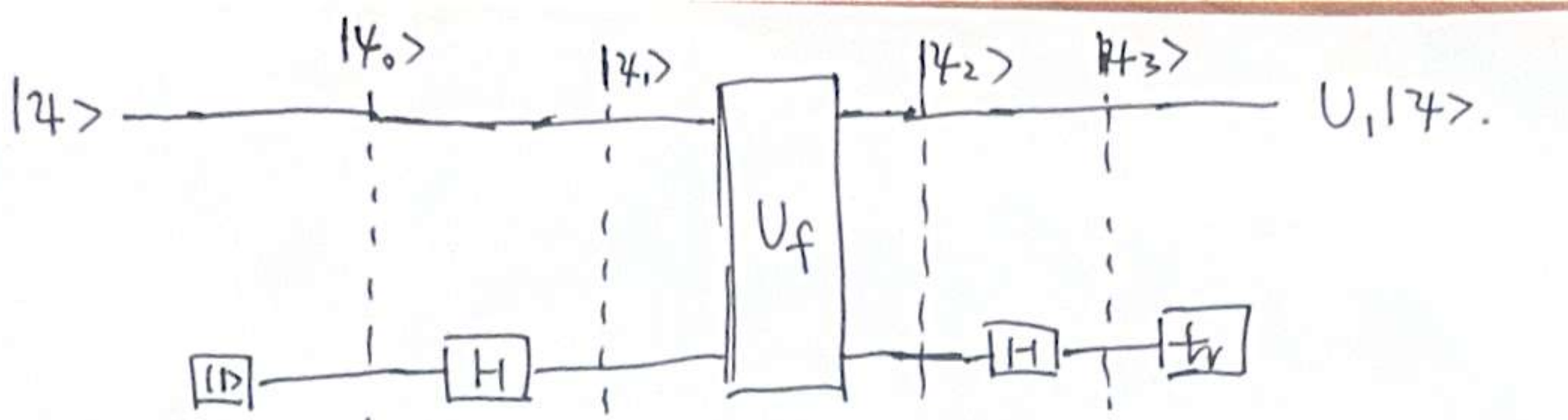
"$\oplus$" Xor.

$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

flip.

$U_f|x\rangle|1\rangle = |x\rangle|f(x)\oplus 1\rangle = \begin{cases} \text{if } f(x)=0. & = |x\rangle|0\oplus 1\rangle = |x\rangle|1\rangle \\ \text{if } f(x)=1. & = |x\rangle|1\oplus 1\rangle = |x\rangle|0\rangle. \end{cases}$

$U_f|x\rangle|0\rangle = |x\rangle|f(x)\oplus 0\rangle = \begin{cases} |x\rangle|0\oplus 0\rangle = |x\rangle|0\rangle. & f(x)=0. \\ |x\rangle|1\oplus 0\rangle = |x\rangle|1\rangle. & f(x)=1. \end{cases}$



(3)

$|\psi\rangle = \cos\alpha|s_0\rangle + \sin\alpha|s_1\rangle$.

$|4_0\rangle = |4\rangle|1\rangle = \cos\alpha|s_0\rangle|1\rangle + \sin\alpha|s_1\rangle|1\rangle$

$|4_1\rangle = |4\rangle \underline{H|1\rangle} = |4\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$|4_2\rangle = U_f|4_1\rangle = U_f|4\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$= \frac{1}{\sqrt{2}}\left(U_f|4\rangle|0\rangle - U_f|4\rangle|1\rangle\right)$

$= \frac{1}{\sqrt{2}}\left(\cos\alpha\, U_f|s_0\rangle|0\rangle + \sin\alpha\, U_f|s_1\rangle|1\rangle - \cos\alpha\, U_f|s_0\rangle|1\rangle - \sin\alpha\, U_f|s_1\rangle|1\rangle\right)$

$H|x-\rangle = |1\rangle$

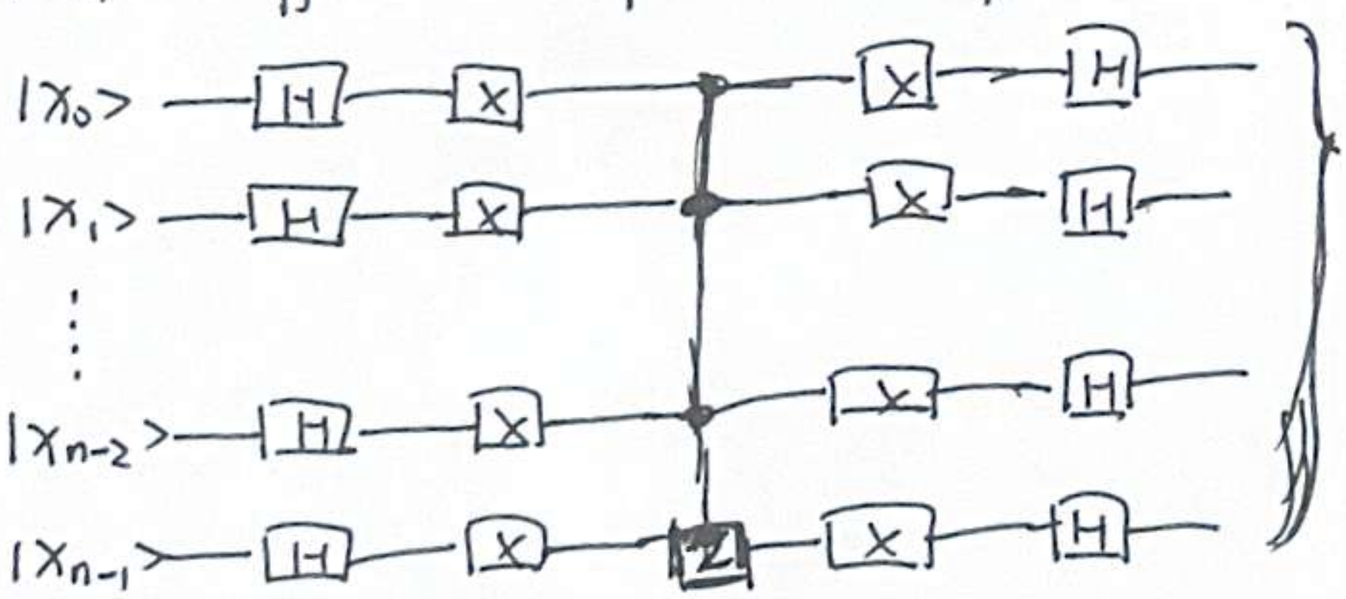
$= \frac{1}{\sqrt{2}}\left(\underline{\cos\alpha|s_0\rangle}|0\rangle + \sin\alpha|s_1\rangle|1\rangle - \underline{\cos\alpha|s_0\rangle}|1\rangle - \sin\alpha|s_1\rangle|0\rangle\right)$

$= \cos\alpha|s_0\rangle|x-\rangle - \sin\alpha|s_1\rangle|x-\rangle$

$\Rightarrow |4_3\rangle = \cos\alpha|s_0\rangle H|x-\rangle - \sin\alpha|s_1\rangle H|x-\rangle = (\cos\alpha|s_0\rangle - \sin\alpha|s_1\rangle)|1\rangle$

$\Rightarrow U_1|4\rangle = \cos\alpha|s_0\rangle - \sin\alpha|s_1\rangle$.

For diffusion operator U_s.



$-U_s|x_0 \cdots x_{n-1}\rangle$.

O(n) elementary quantum gates

$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ $Z|0\rangle = |0\rangle$, $Z|1\rangle = -|1\rangle$.

$-U_s = H^{\otimes n} R_0 H^{\otimes n} = -(2|s\rangle\langle s| - I)$

with $R_0 = I - 2|0\cdots 0\rangle\langle 0\cdots 0|$.

Let's show that $V = 2|0\rangle_n\langle 0|_n - I = -X^{\otimes n} C^{n-1}(Z) X^{\otimes n}$.

Let $\vec{x} \in \{0,1\}^n$, then

(4)

$$V|\vec{x}\rangle = (2|0\rangle_n\langle 0|_n - I)|\vec{x}\rangle = \begin{cases} |\vec{x}\rangle. & \text{if } \vec{x} = \vec{0}. \\ -|\vec{x}\rangle. & \text{if } \vec{x} \neq \vec{0}. \end{cases}$$

Since $X^{\otimes n}|\vec{x}\rangle = |\neg\vec{x}\rangle$, $\Rightarrow$.

$$C^{n-1}(Z)\,X^{\otimes n}|\vec{x}\rangle = \underbrace{C^{n-1}(Z)}_{|1\cdots1\rangle \text{ flip.}}|\neg\vec{x}\rangle = \begin{cases} -|\neg\vec{x}\rangle. & \text{if } \vec{x} = \vec{0} \\ |\neg\vec{x}\rangle. & \text{if } \vec{x} \neq \vec{0}. \end{cases}$$

otherwise. no.

$$\Rightarrow \quad X^{\otimes n}\,C^{n-1}(Z)\,X^{\otimes n}|\vec{x}\rangle = \begin{cases} -|\vec{x}\rangle. & \text{if } \vec{x} = \vec{0} \\ |\vec{x}\rangle. & \text{if } \vec{x} \neq \vec{0}. \end{cases}$$

$$\Rightarrow \quad V = -X^{\otimes n}\,C^{n-1}(Z)\,X^{\otimes n}.$$

2°. check. $U_s = H^{\otimes n}(2|0\cdots0\rangle\langle 0\cdots1| - I)H^{\otimes n}$

$$= 2H^{\otimes n}|0\cdots0\rangle\langle 0\cdots1|H^{\otimes n} - H^{\otimes n}\cdot H^{\otimes n}$$

$$= 2|s\rangle\langle s| - I.$$

"Analysis"

Theorem 7.1.21.

$n \in \mathbb{N}$. $N = 2^n$. $f: \{0,1\}^n \to \{0,1\}$. $M = |f^{-1}(1)| > 0$.

return a $\vec{x} \in \{0,1\}^n$. s.t. $f(\vec{x}) = 1$. with probability $\underbrace{\sin^2((2k+1)\theta)}_{> \sin^2\theta = \frac{M}{N}}$.

k times $G = k(U_f) + k \cdot \underbrace{O(n)}_{O(\log N)}$

Proof: $(2k+1)\theta \leq \frac{\pi}{2}$.

$$\Rightarrow \quad k \leq \frac{\pi}{4\theta} - \frac{1}{2}$$

$$\Rightarrow \quad k = \left\lfloor \frac{\pi}{4\theta} - \frac{1}{2} \right\rfloor.$$