Grover's Search:

Problem: $f : \{0, 1, \cdots, N-1\} \to \{0, 1\}$

Goal: find an x s.t. $f(x) = 1$.

- $N = 2^n$
- $\exists$ unique x^* s.t. $f(x^*) = 1$

$$f(x) = \begin{cases} 1 & \text{if } x = x^* \\ 0 & \text{o.t.} \end{cases}$$

Quantum Supremacy:

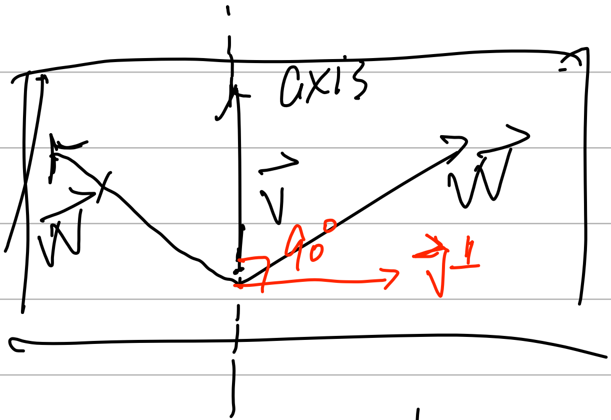
$x \rightarrow \boxed{} \rightarrow f(x)$

$$\begin{cases} f(x_1) = 0 \\ f(x_2) = 0 \\ \vdots \\ f(x^*) = 1 \end{cases}$$

$O(N)$ times of trials.
Best classical algo.

Grover's : $O(\sqrt{N})$ (quantum) queries.

Reflection:



$\perp$: perp

Let $|v\rangle \in \mathbb{C}^N$. R is a reflection across $|v\rangle$

if: ① $R|v\rangle = |v\rangle$

② $\forall\ |w\rangle \perp |v\rangle$, $R|w\rangle = -|w\rangle$

$\perp$ orthogonal

Thm: Forall unit vector $|v\rangle$, the operator

$$R := 2 \cdot |v\rangle\langle v| - \mathbb{I}$$

is a reflection w.r.t. $|v\rangle$

2 Important Reflection Operators:

- Diffusion Operator;
- "minus" version of Phase Oracle.

Diffusion Operator: $|+^n\rangle = \underbrace{|+\rangle|+\rangle\cdots|+\rangle}_{n \text{ of them}}$

$$D := 2\cdot|+^n\rangle\langle+^n| - \mathbb{I}$$

$$|+^n\rangle = H^{\otimes n}\underbrace{|00\cdots0\rangle}_{n \text{ of them}}$$

Phase Oracle: $\boxed{f:\{\ldots\}\longrightarrow\{0,1\} \quad \text{domain} \quad \exists \text{ unique } x^* \text{ s.t. } f(x^*)=1}$

$$PhO_f : |x\rangle := (-1)^{f(x)}|x\rangle := \begin{cases} -|x\rangle & f(x)=1 \\ |x\rangle & f(x)=0 \end{cases}$$

(You can prove) $= \mathbb{I} - 2|x^*\rangle\langle x^*|$

where x^* is s.t. $f(x^*)=1$

$$\underbrace{-PhO_f|x\rangle}_{} = 2|x^*\rangle\langle x^*| - \mathbb{I}$$

$\hookrightarrow$ it is a reflection across $|x^*\rangle$

$\Rightarrow$ PhO_f is a reflection across the state:

$$|bad\rangle := \sqrt{\frac{1}{N-1}}\sum_{x\neq x^*}|x\rangle$$

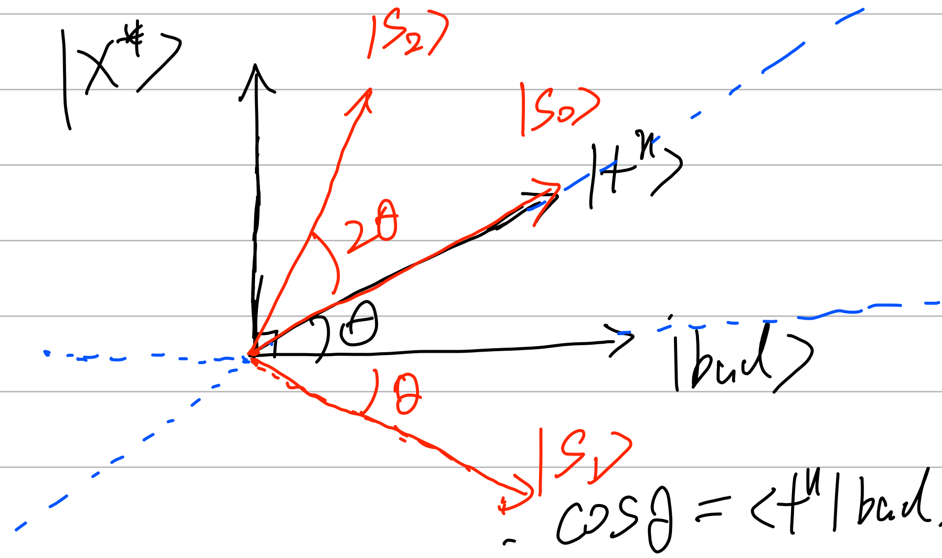
$\Leftrightarrow Ph\,O_f = 2 \cdot |bad\rangle\langle bad| - \mathbb{I}$

Grover's Algo.

$$\begin{cases} f : \overbrace{\{0,1\}^n}^{Dom} \to \{0,1\} \\ \exists \text{ unique } x^* \quad f(x^*) = 1. \end{cases}$$

$$\begin{cases} - \ |+^n\rangle = \underbrace{|+\rangle \cdots |+\rangle}_{n} = \frac{1}{\sqrt{N}} \sum_{x \in Dom.} |x\rangle \\ - \ |x^*\rangle \\ - \ |bad\rangle = \sqrt{\frac{1}{N-1}} \sum_{x \neq x^*} |x\rangle \end{cases} \quad \begin{bmatrix} -- \ |3\rangle \\ -- \ |1\rangle + |2\rangle + |4\rangle \end{bmatrix}$$

$$\Rightarrow \begin{cases} |+^n\rangle = \sqrt{\frac{N-1}{N}}\, |bad\rangle + \sqrt{\frac{1}{N}}\, |x^*\rangle \\ |bad\rangle \perp |x^*\rangle \ : \ \langle x^* | bad\rangle = 0 \end{cases}$$



$\cos\theta = \langle +^n | bad\rangle = \sqrt{\frac{N-1}{N}}$

↳ $\theta \approx \sqrt{\frac{1}{N}}$ $(N=2^n)$

↑ Taylor expasion.

Algo steps:

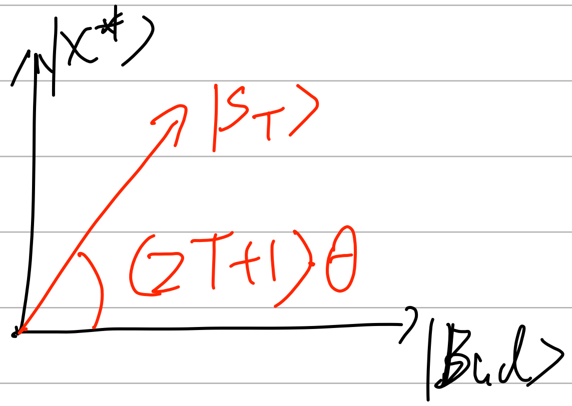
① Prepare $|s_0\rangle := H^n\rangle$

② Alternating Between $(PhO_f$, Diffusion$)$

↳ for T times.

You'll get a state that is

$(2T+1)\theta$ from $|bad\rangle$



We need to set $(2T+1)\cdot\theta = \frac{\pi}{2}$

$$\left.\begin{aligned}\Rightarrow T &= \frac{\pi}{4}\cdot\frac{1}{\theta} - \frac{1}{2} \\ \theta &= O\left(\sqrt{\tfrac{1}{N}}\right)\end{aligned}\right\}$$

$\Rightarrow T = O(\sqrt{N})$

Diffusion Operator can be implemented efficiently once realize :

$$D := 2|+^n\rangle\langle +^n| - I = H^{\otimes n} \Lambda H^{\otimes n}$$

where $\Lambda = \begin{bmatrix} 1 & & & \\ & -1 & & 0 \\ & & \ddots & \\ 0 & & & -1 \end{bmatrix}$

$|0\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$ $|1\rangle = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ \vdots \end{bmatrix}$ $|2\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ \vdots \end{bmatrix}$

$\cdots$ $|N\rangle = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}$

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \cdots + \alpha_N|N\rangle$$

$$\Lambda \cdot |\psi\rangle = \alpha_0|0\rangle - \alpha_1|1\rangle - \alpha_2|2\rangle \cdots - \alpha_n|N\rangle$$

Simon's Algorithm:

Problem: $f : \{0,1\}^n \to \{0,1\}^n$ range.

$\exists$ unique $s \neq 0^n$ s.t.

$[f(x) = f(y) \iff y = x \oplus s]$ bit-wise XOR

[periodic function of period t.
$f(x) = f(x+t) \; \forall x$.

Goal: Given oracle access to f, figure out "s".

Quantum Supremacy:

- Best classical (randomized) algo. needs $\Theta(\sqrt{2^n})$ classical queries to achieve a constant winning probability. $\varepsilon \in [0, 1]$
- Simon's algo. uses $O(n)$ quantum queries.

- Classical complexity $= \theta(\sqrt{2^n})$

both $\underline{O(\sqrt{2^n})}$ and $\Omega(\sqrt{2^n})$

(upper) (lower)

- $\underline{\text{Upper Bound:}}$ $O(\sqrt{2^n})$ $f\ \{0,1\}^n \to \{0,1\}^n$

$$\begin{matrix} x_1 & x_2 & \cdots & x_q \\ \downarrow & \downarrow & & \downarrow \\ f(x_1) & f(x_2) & \cdots & f(x_q) \end{matrix}$$

collision : $f(x_i) = f(x_j) \Rightarrow x_i \oplus x_j = s$

23 students,

w.p. 50% at least 2 students share the same birth day

n students,

$$\Pr[\text{None of them share same Birthday}] = \frac{365(365-1)\cdots(365-n+1)}{365^n}$$

If "d" days, "n" students.

$$\Pr[\text{at least two share the same birthday}] \approx 1 - e^{\frac{n(n-1)}{2d}}$$

$$\approx 1 - \left(\frac{d-1}{d}\right)^{\frac{n(n-1)}{2}}$$

By setting $n = \sqrt{d}$, you get

$$\Pr[\text{collision happens}] \approx 0.5$$

Classical lower bound $\Omega(\sqrt{2^n})$

(due to Richard Cleve)

Events:

- A_K: the K-th query leads to ~~the~~ 1st collision.
- B_K: no collision has been found in the first $(K-1)$ queries.
- C_K: the K-th query leads to a collision

Pr[Collision appears within the first m queries]

$$= \Pr\left[\bigcup_{k=1}^{m} A_k\right]$$

① Try to bound $\Pr[A_k]$ $\forall k$.

$$\Pr[A_k] = \Pr[B_k \wedge C_k] \le \Pr[C_k \mid B_k]$$

$$\begin{array}{ccccc} x_1 & x_2 & \cdots & x_{k-1} & x_k \\ \downarrow & \downarrow & & \downarrow & \downarrow \\ f(x_1) & \cdots & & f(x_{k-1}) & f(x_k) \end{array}$$

How many possible values for s? $\rightarrow$ $(2^n - 1)$

"s" $\in \{0,1\}^n \setminus \{0^n\}$

"No collision so far" eliminates $\binom{n-1}{2}$ possible bad values for "s"

$$\Pr[C_k \mid B_k] = \Pr\left[\begin{array}{l} \text{Collision w/ } f(x_1) \ \vee \\ \text{Collision w/ } f(x_2) \ \vee \\ \quad \vdots \\ \text{Collision w/ } f(x_{k-1}) \end{array} \;\middle|\; B_k\right]$$

$$\leq \underbrace{(k-1)}_{\downarrow} \cdot \underbrace{\Pr[\text{collision w/ } f(x_i) \mid B_k]}$$

$$\leq \overbrace{(k-1)} \cdot \frac{1}{(2^n-1)-\binom{k-1}{2}}$$

$$\leq \frac{2k}{2^{n+1}-k^2}$$

$\Rightarrow$

$$\boxed{\text{Claim: } \Pr[C_k \mid B_k] \leq \frac{2k}{2^{n+1}-k^2} \ (\forall k)}$$

$$\Pr\left[\begin{array}{l}\text{Collision appears within}\\ \text{the first } m \text{ queries}\end{array}\right] = \Pr\left[\biguplus_{k=1}^{m} A_k\right]$$

$$\leq \sum_{k=1}^{m} \Pr[A_k] \quad \text{(union bound)}$$

$$\leq \sum_{k=1}^{m} \Pr[C_k \mid B_k]$$

$$\leq \sum_{k=1}^{m} \frac{2k}{2^{n+1}-k^2} \quad \text{(by the claim above)}$$

$$\leq \sum_{k=1}^{m} \frac{2m}{2^{n+1}-m^2} = \frac{2m^2}{2^{n+1}-m^2}$$

If you want to win w/ prob. $3/4$

set $\frac{2m^2}{2^{n+1}-m^2} \geq \frac{3}{4}$

$$\Rightarrow m \geq \sqrt{\frac{6}{11} \cdot 2^n}$$

$$\Rightarrow m = \Omega\left(\sqrt{2^n}\right)$$

Simon's Algorithm

① Prepare $|0^{2n}\rangle$. Compute

$$(H^n \otimes \mathbb{I}) \cdot |0^{2n}\rangle = \left(\frac{1}{\sqrt{2^n}} \sum_x |x\rangle\right) \cdot |0^n\rangle$$

② Apple the standard oracle:

$$U_f \cdot \left(\frac{1}{\sqrt{2^n}} \sum_x |x\rangle\right) \cdot |0^n\rangle = \frac{1}{\sqrt{2^n}} \sum_x \underbrace{|x\rangle}_{\text{reg } 1} \underbrace{|f(x)\rangle}_{\text{reg } 2}$$

③ Measure reg 2:

$$\frac{1}{\sqrt{2}} \left(|x_1\rangle + |x_2\rangle\right) | y \rangle$$, where

$f(x_1) = f(x_2) = y$

$$\left[\begin{array}{l} 00 \to 1 \\ 01 \nearrow \\ 10 \to 2 \\ 11 \nearrow \end{array}\right. \qquad \begin{array}{l} |00\rangle|1\rangle + \\ |01\rangle|1\rangle \\ |10\rangle|2\rangle \\ |11\rangle|2\rangle \end{array}$$

$\Rightarrow$ state s.t. $\frac{1}{\sqrt{2}}\left(|x\rangle + |x \oplus s\rangle\right)|f(x)\rangle$

④ $H^{\otimes n}$ again:

$$H^{\otimes n} \cdot \frac{(|x\rangle + |x \oplus s\rangle)}{\sqrt{2}}$$

(by $H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_y (-1)^{\langle x,y\rangle} |y\rangle$)

$$\frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2^n}} \sum_z (-1)^{\langle x,z\rangle} |z\rangle + \frac{1}{\sqrt{2^n}} \sum_z (-1)^{\langle x \oplus s, z\rangle} |z\rangle\right]$$

$$= \frac{1}{\sqrt{2^{n+1}}} \cdot \sum_z \left[(-1)^{\langle x,z\rangle} + (-1)^{\langle x \oplus s, z\rangle}\right] \cdot \underbrace{|z\rangle}_{\text{reg } 2}$$

⑤ We measure reg 2.

w.p. $\left(\frac{[\ldots\ldots]}{\sqrt{2^{n+1}}}\right)^2$, observe z.

$\Rightarrow$ If observe z, ~~then~~ then:

$$(-1)^{\langle x, z\rangle} + (-1)^{\langle x\oplus s, z\rangle} \neq 0$$

$$\Rightarrow \langle x, z\rangle = \langle x\oplus s, z\rangle$$

$$\Rightarrow \langle x, z\rangle \oplus \langle x\oplus s, z\rangle = 0$$

$$\Rightarrow \langle x\oplus x\oplus s, z\rangle = 0$$

$$\Rightarrow \langle s, z\rangle = 0$$

$$\Rightarrow \begin{cases} s = s_1 \cdots s_n \\ z = z_1 \cdots z_n \end{cases}$$

$$\Rightarrow \boxed{s_1\cdot z_1 + s_2 z_2 + \cdots s_n\cdot z_n = 0 \pmod 2}$$

Repeating Step ① - ③ for n times:

$$\begin{cases} s_1\cdot z_1^{(1)} + s_2\cdot z_2^{(1)} + \cdots + s_n z_n^{(1)} = 0 \pmod 2 \\ s_1\cdot z_1^{(2)} + s_2\cdot z_2^{(2)} + \cdots + s_n\cdot z_n^{(2)} = 0 \pmod 2 \\ \vdots \\ s_1\cdot z_1^{(n)} + s_2\cdot z_2^{(n)} + \cdots + s_n\cdot z_n^{(n)} = 0 \pmod 2 \end{cases}$$

$$\Leftrightarrow \begin{cases} \langle s, z^{(1)} \rangle = 0 \\ \langle s, z^{(2)} \rangle = 0 \\ \quad \vdots \\ \langle s, z^{(n)} \rangle = 0 \end{cases}$$

$\boxed{z^{(1)} = z^{(2)}}$

$\times$ w.h.p.

By union bound:

$\begin{cases} \text{Each pair collide w.p. } \frac{1}{2^{n/4}} \\ \text{There are } \binom{n}{2} \approx n^2 \text{ pairs.} \end{cases}$

$$\Rightarrow \Pr[\text{NO collision}] \leq n^2 \cdot \frac{1}{2^{n/4}}$$

$$\approx O\left(\sqrt{\frac{1}{2n}}\right)$$