GROVER'S PROBLEM:

INPUT: $f : \{0,1\}^n \rightarrow \{0,1\}$

OUTPUT: $\begin{cases} 1, & \text{if } \exists x \in \{0,1\}^n : f(x) = 1 \\ 0, & \text{otherwise} \end{cases}$

CLASSICALLY: Try all x! $O(2^n)$

GROVER'S ALGORITHM:

$Z_f |x\rangle = (-1)^{f(x)} |x\rangle$

$\{0,1\}^n$

Helper function

$\hookrightarrow$ $f(x)$'s encoder (like U_f)

$Z_0 |x\rangle = \begin{cases} -|x\rangle, & \text{if } x = 0^n \\ |x\rangle, & \text{otherwise} \end{cases}$

$f(0^n) = 1$

$f(x) = 0$, for all other x

GROVER'S ALGORITHM :

$$G = -H^{\otimes n} Z_0 H^{\otimes n} Z_f$$

$x = |0^n\rangle$ (n 10s qubits)

$H^{\otimes n} x$

repeat { apply G to x } $O(\sqrt{2^n})$ times

measure x and output the result

Idea :

$\underbrace{G \dots G}_{\text{known \# times}}(x)$

So, from 2^n to $\sqrt{2^n}$. QUADRATIC SPEEDUP //

$2^n \downarrow$ CLASSICAL

$\sqrt{2^n} \downarrow$ QUANTUM

EXAMPLE:

$n = 2$

$$f : \{0,1\}^2 \rightarrow \{0,1\}$$

$$f(00) = f(01) = f(10) = 0 \quad , f(11) = 1$$

# of iterations = 1 (we know this already)

$$G = -H^{\otimes n} Z_0 H^{\otimes n} Z_f$$

$$H^{\otimes 2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)$$

$$= \frac{1}{2}\Big[(|00\rangle + \underline{|01\rangle} + \underline{|10\rangle} + \underline{|11\rangle}) + (|00\rangle - \underline{|01\rangle} + |10\rangle - \underline{|11\rangle})$$

$$+ (\underline{|00\rangle} + |01\rangle - \underline{|10\rangle} - |11\rangle) - (\underline{|00\rangle} - |01\rangle - |10\rangle + |11\rangle)\Big]$$

$$= 1/2\,(2|00\rangle + 2|01\rangle + 2|10\rangle - 2|11\rangle$$

$$= (|00\rangle + |01\rangle + |10\rangle - |11\rangle)$$

$$G H^{\otimes 2} |00\rangle$$

$$= G\ 1/2\,(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

$$= -H^{\otimes 2} Z_0 H^{\otimes 2} Z_f\ 1/2\,(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

$$= -H^{\otimes 2} Z_0 H^{\otimes 2}\, 1/2\,(|00\rangle + |01\rangle + |10\rangle - |11\rangle)$$

$$= -H^{\otimes 2} Z_0\ 1/2\,(|00\rangle + |01\rangle + |10\rangle - |11\rangle)$$

$$= -H^{\otimes 2}\ 1/2\,(-|00\rangle + |01\rangle + |10\rangle - |11\rangle)$$

$$= -H^{\otimes 2}\ \tfrac{1}{2}\left(-2|00\rangle + \underbrace{\left(|00\rangle + |01\rangle + |10\rangle - |11\rangle\right)}\right)$$

$$= -H^{\otimes 2}\left(-|00\rangle\right. \quad + \quad H^{\otimes 2}\tfrac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle - |11\rangle\right)$$

$$= -\left(\left(-\tfrac{1}{2}|00\rangle - |01\rangle - |10\rangle - |11\rangle\right) + \tfrac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle - |11\rangle\right)\right)$$

$$= -\tfrac{1}{2}\left(-2|11\rangle\right)$$

$$= |11\rangle \quad //$$

GENERIC IDEA:

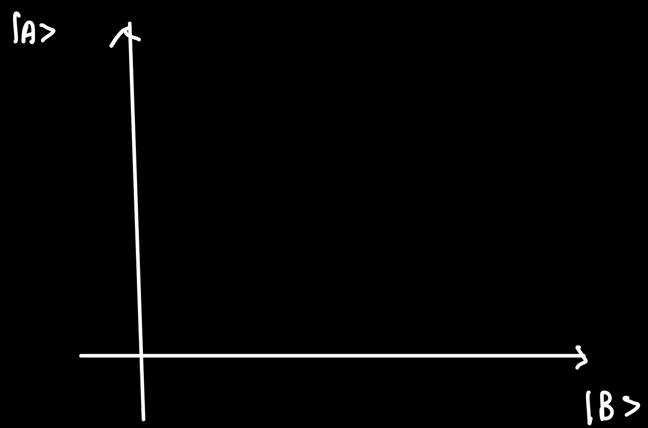
$$A = \{x \in \{0,1\}^n \mid f(x) = 1\} \qquad a = |A|$$

$$B = \{x \in \{0,1\}^n \mid f(x) = 0\} \qquad b = |B|$$

$$N = 2^n = a + b$$

$$|A\rangle = \frac{1}{\sqrt{a}} \sum_{x \in A} |x\rangle \qquad |B\rangle = \frac{1}{\sqrt{b}} \sum_{x \in A} |x\rangle$$

Orthogonal unit vectors



LEMMA :

$$G|A\rangle = \left(1 - \frac{2a}{N}\right)|A\rangle - \frac{2\sqrt{ab}}{N}|B\rangle$$

$$G|B\rangle = \frac{2\sqrt{ab}}{N}|A\rangle - \left(1 - \frac{2b}{N}\right)|B\rangle$$

PROOF:

$$|h\rangle = H^{\otimes n} |0^n\rangle$$

$$= \frac{1}{\sqrt{N}} \sum_x |x\rangle$$

$$|h\rangle = \sqrt{\frac{a}{N}} |A\rangle + \sqrt{\frac{b}{N}} |B\rangle \quad - \text{(1)}$$

$$G = -H^{\otimes n} Z_0 H^{\otimes n} Z_f$$

$$G|A\rangle = -\underbrace{H^{\otimes n} Z_0 H^{\otimes n}} Z_f |A\rangle$$

$$Z_0 = \begin{bmatrix} -1 & & & 0 \\ & 1 & & \\ & & 1 & \\ & 0 & \ddots & \\ & & & 1 \end{bmatrix}$$

$$= I - 2|0^n\rangle\langle 0^n|$$

$$H^{\otimes n} Z_0 H^{\otimes n} = H^{\otimes n} \left(I - 2|0^n\rangle\langle 0^n| \right) H^{\otimes n}$$

$$= I - (2 \cdot |h\rangle\langle h|)$$

$$G|A\rangle = -\left(I - 2\cdot|h\rangle\langle h|\right) Z_f |A\rangle$$

$$= \left(I - 2|h\rangle\langle h|\right) \underbrace{\left(-Z_f\right) |A\rangle}_{\to\ |A\rangle}$$

[as all in $|A\rangle$ are $f(x)=1$]

$$= \left(I - 2|h\rangle\langle h|\right) |A\rangle$$

$$= |A\rangle - 2\langle h|A\rangle . |h\rangle$$

$$|h\rangle = \sqrt{\frac{a}{N}}\,|A\rangle + \sqrt{\frac{b}{N}}\,|B\rangle$$

$\langle h|A\rangle$ = inner product of h, A

$A, B \to$ orthogonal

$\langle A|B\rangle = 0$

$$= \sqrt{\frac{a}{N}}$$

$$G|A\rangle = |A\rangle - 2\sqrt{\frac{a}{N}}\left(\sqrt{\frac{a}{N}}\,|A\rangle + \sqrt{\frac{b}{N}}\,|B\rangle\right)$$

$$= |A\rangle - 2\left(\frac{a}{N}\right)|A\rangle - \frac{2\sqrt{ab}}{N}|B\rangle$$

$$= \left(1 - \frac{2a}{N}\right)|A\rangle - \frac{2\sqrt{ab}}{N}|B\rangle \quad //$$

HENCE PROVED //

$$M = \begin{array}{cc} & \text{FROM} \\ & \begin{array}{cc} |B\rangle & |A\rangle \end{array} \\ \begin{array}{c} |B\rangle \\ \text{TO} \\ |A\rangle \end{array} & \begin{bmatrix} -(1-2b/N) & -2\sqrt{ab}/N \\ 2\sqrt{ab}/N & 1-2a/N \end{bmatrix} \end{array}$$

We know

$$|h\rangle = \sqrt{\frac{a}{N}}\,|A\rangle + \sqrt{\frac{b}{N}}\,|B\rangle \quad \text{[FROM 1]}$$

as $\frac{a}{N} + \frac{b}{N} = 1$

we can assume $\sqrt{\frac{a}{N}} = \sin\theta$

$$\sqrt{\frac{b}{N}} = \cos\theta$$

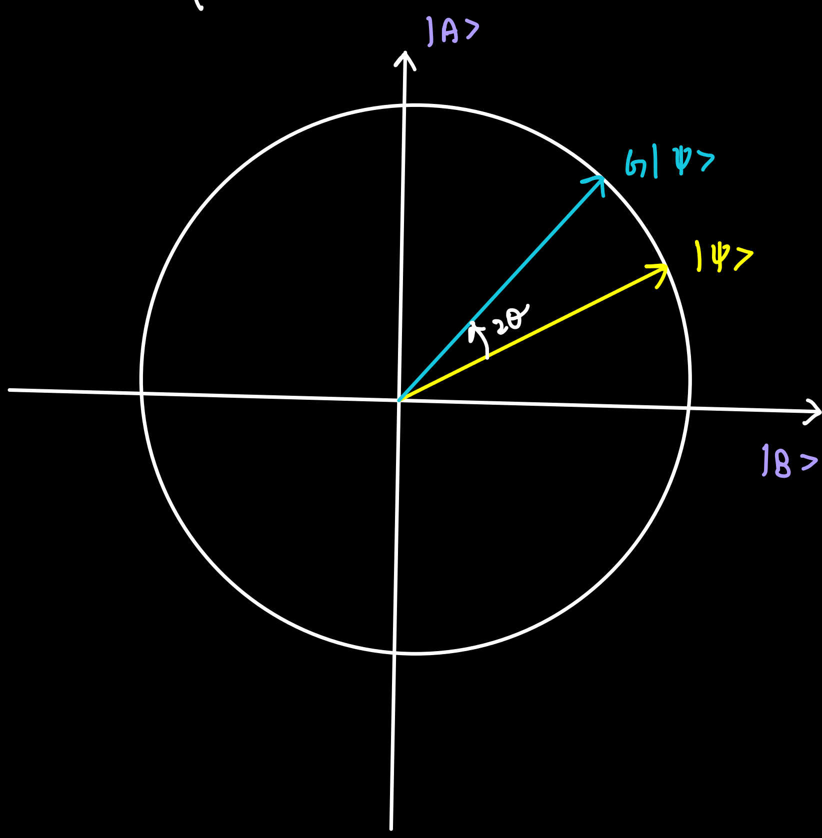
$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

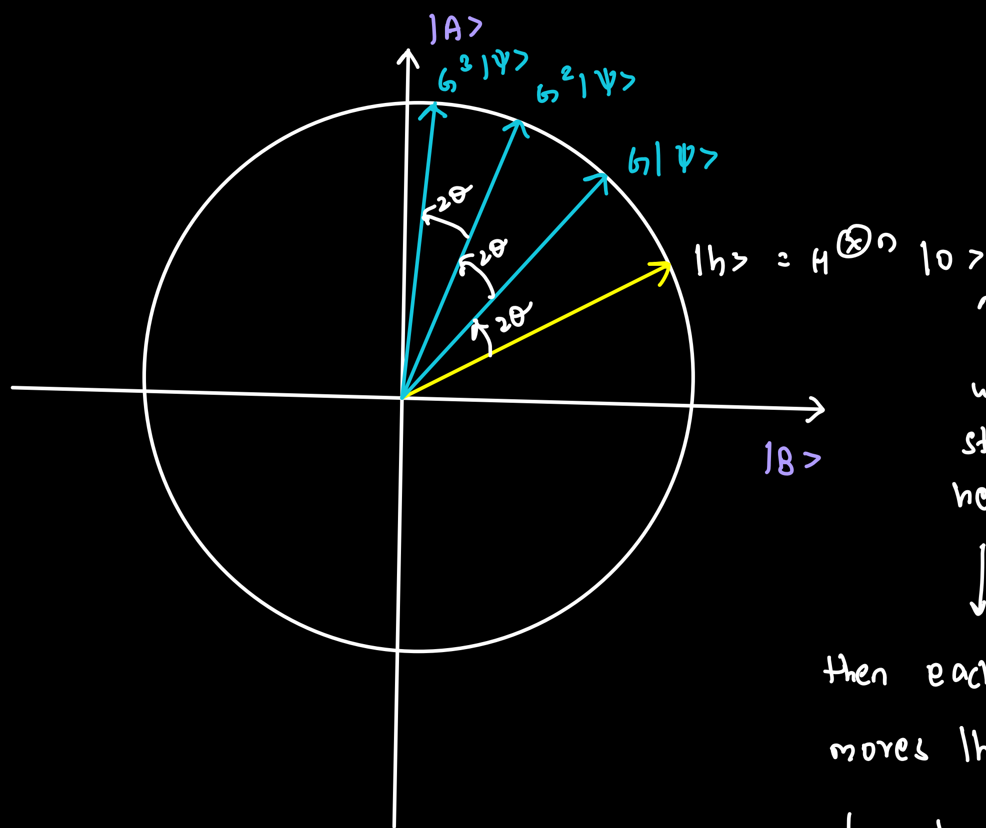
$$R_\theta^2 = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^2$$

$$= \begin{pmatrix} \sqrt{b/N} & -\sqrt{a/N} \\ \sqrt{a/N} & \sqrt{b/N} \end{pmatrix}^2$$

$$= \begin{pmatrix} \sqrt{b/N} & -\sqrt{a/N} \\ \sqrt{a/N} & \sqrt{b/N} \end{pmatrix} \begin{pmatrix} \sqrt{b/N} & -\sqrt{a/N} \\ \sqrt{a/N} & \sqrt{b/N} \end{pmatrix}$$

$$= \begin{pmatrix} (b-a)/N & -2\sqrt{ab}/N \\ 2\sqrt{ab}/N & (b-a)/N \end{pmatrix} = M$$





we start here

then each G moves $|h\rangle$ towards $|A\rangle$.

(rotate 2θ)

May not overlap with $|A\rangle$. We might only go as close as possible.

HOW MANY TIMES TO CALL G?

$$|h\rangle = \cos\theta\,|B\rangle + \sin\theta\,|A\rangle$$

Iterate k times :

$$\cos\left((2k+1)\theta\right)|B\rangle + \underbrace{\sin\left((2k+1)\theta\right)}\,|A\rangle$$

we want this to be as close to 1 as possible.

$$\sin((2k+1)\theta) \approx 1$$

$$(2k+1)\theta \approx \pi/2$$

$$2k+1 \approx \pi/2\theta$$

$$k \approx \pi/4\theta - 1/2$$

Case:

Assume $a = 1$

$$\sin\theta : \sqrt{a/N}$$

$$\cos\theta : \sqrt{b/N}$$

$$\sin\theta = \sqrt{a/N} = 1/\sqrt{N}$$

if N is very large, $1/\sqrt{N}$ is very small

$$\sin\theta \approx \theta$$

$$\theta \approx 1/\sqrt{N}$$

$$k = \frac{\pi}{4\theta} - \frac{1}{2} = \frac{\pi\sqrt{N}}{4} - \frac{1}{2}$$ //

so in our example

$N = 4$

$\pi/2 - 1/2 = (3.14 - 1)/2$

$= 2.14/2$

$= 1.07 \approx 1$ //

$$\theta \approx \sqrt{\frac{1}{N}}, \quad k \approx \frac{\pi\sqrt{N}}{4} - 1/2$$

$$|\sin((2k+1)\theta)|^2$$

$$= \left|\sin\left(\left(2\left(\frac{\pi\sqrt{N}}{4} - \frac{1}{2}\right) + 1\right)\sqrt{\frac{1}{N}}\right)\right|^2$$

$$= \left|\sin\left(\left(\frac{\pi}{2}\sqrt{N}\right)\left(\frac{1}{\sqrt{N}}\right)\right)\right|^2$$

$$= |\sin \pi/2|^2$$

$= 1$ //