

Grover's Algorithm

Search.

Given N items, 1 "marked"

look at k of them

prob = k/N of finding it.

Quantum: "look" at $\sim \sqrt{N}$

e.g. Database

$$\text{or } p = m^2 + n^2 \quad 44 + 1$$

$$\sim \sqrt{p/2}, \quad \sqrt{p}$$

$$f(x) = \begin{cases} 0 & x \neq a \\ 1 & x = a \end{cases} \leftarrow \text{marked item}$$

$$U_f |x\rangle_n |y\rangle_1 = |x\rangle |y \oplus f(x)\rangle_1 \quad N=2^n$$

"phase
kickback"

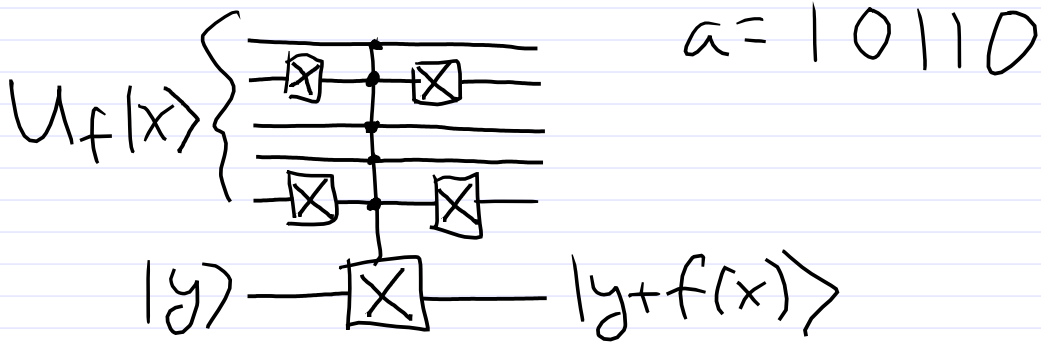
$$\begin{array}{ccc} |x\rangle & \text{---} & |x\rangle \\ |1\rangle & \text{---} \boxed{H} & (-1)^{f(x)} H |1\rangle \end{array} \quad \left[U_f \right]$$

$$U_f (|x\rangle \otimes H|1\rangle) = (-1)^{f(x)} (|x\rangle \otimes H|1\rangle)$$

$$V(x) |x\rangle_n = (-1)^{f(x)} |x\rangle_n = \begin{cases} |x\rangle & x \neq a \\ -|a\rangle & x = a \end{cases}$$

$$V |\psi\rangle = |\psi\rangle - 2|a\rangle \langle a|\psi\rangle$$

$$V_f = \underline{1} - 2|a\rangle \langle a| \quad \text{embodies } f$$



$$|\varphi\rangle = H^{\otimes n} |0\rangle = \frac{1}{\sqrt{2^n}} \sum_{0 \leq x < 2^n} |x\rangle$$

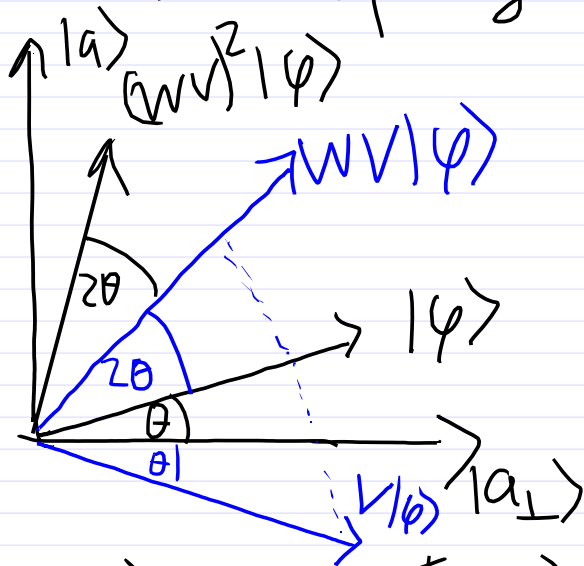
also need

$$W = 2|\varphi\rangle\langle\varphi| - 1$$

inverts states orthogonal to $|\varphi\rangle$

$$V = \underline{1} - 2|a\rangle\langle a|$$

work in 2d space generated by $|a\rangle, |\psi\rangle$



$$\langle a | \psi \rangle = \cos(\pi/2 - \theta) = \sin \theta = \frac{1}{2^{n/2}} \\ \approx \theta \approx \frac{1}{\sqrt{N}}$$

WV is a rotation (by what angle?)
by 2θ

$$\text{(or } V = \begin{pmatrix} 1 & \\ & -1 \end{pmatrix} \quad W = R_\theta V R_{-\theta} \quad R_\theta = \begin{pmatrix} c & -s \\ s & c \end{pmatrix} \\ WV = R_\theta V R_{-\theta} V = R_{2\theta} \text{)}$$

Apply $(WV)^l$ $\theta \approx \frac{1}{2^{n/2}}$

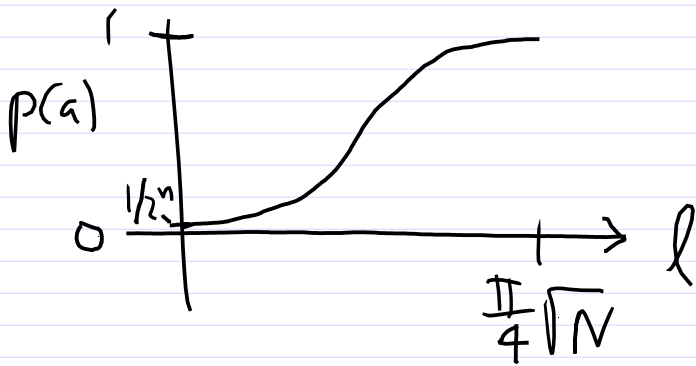
with $(2l+1)\frac{1}{2^{n/2}} = \frac{\pi}{2}$

gives close as possible to $|a\rangle$

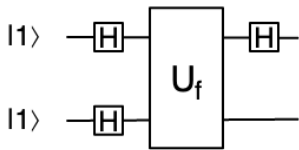
$$l \approx \frac{\pi}{4} 2^{n/2} = \frac{\pi}{4} \sqrt{N}$$

$$p(a) = |\langle a | (WV)^l | \varphi \rangle|^2$$

$$= \sin^2(2l+1)\theta = \sin^2\left(\frac{2l+1}{2^{n/2}}\right)$$



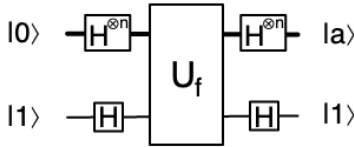
1.



$|1\rangle \quad f(0)=f(1)$
 $|0\rangle \quad f(0)\neq f(1)$

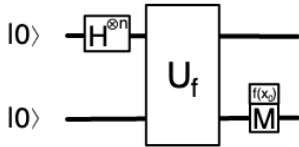
Deutsch '92 (p.44), factor of 2 speedup to determine whether or not 1bit \rightarrow 1bit function $f(x)$ is constant

2.



Bernstein-Vazirani '93 (p.52), $f(x) = a \cdot x \equiv \oplus_i a_i x_i$, factor of n speedup to determine a

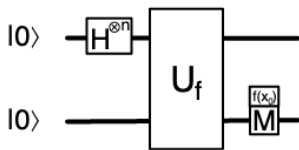
3.



$$\frac{1}{2^{1/2}} (|x_0\rangle + |x_0 \oplus a\rangle) \xrightarrow{\text{H}^{\otimes n}} \text{M}$$

Simon '94 (p.56), $f(x) = f(x \oplus a)$, measured y has $a \cdot y = 0$ (equivalently $\sum_i a_i y_i = 0 \pmod{2}$), exponential speedup ($2^{n/2} \rightarrow O(n)$) to determine a

4.

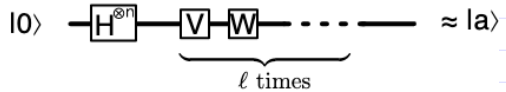
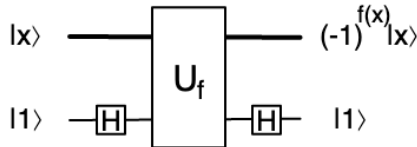


$$\frac{1}{m^{1/2}} \sum_{k=0}^{m-1} |x_0 + kr\rangle \xrightarrow{\text{U}_{\text{FT}}} \text{M}$$

Shor '94 (p.70), $f(x) = f(x + r)$, resulting y is measured with probability $p(y) = \frac{1}{2^{nm}} \left| \sum_{k=0}^{m-1} e^{2\pi i k r y / 2^n} \right|^2$, gives $|y - 2^n/r| < 1/2$ with $p > .4$, sufficient to determine

period r via partial fraction expansion, exponential speedup ($n2^n, \exp(n^{1/3}) \rightarrow O(n^3)$).
 (Note: replaces $\mathbf{H}^{\otimes n} |x\rangle = \frac{1}{2^{n/2}} \sum_{0 \leq y < 2^n} e^{i\pi x \cdot y} |y\rangle$ with $\mathbf{U}_{\text{FT}} |x\rangle = \frac{1}{2^{n/2}} \sum_{0 \leq y < 2^n} e^{2\pi i x y / 2^n} |y\rangle$.)
 Practical application is $f(x) \equiv b^x \pmod{N}$, where $b \equiv a^c \pmod{N}$ is an encrypted message, from which d' , satisfying $cd' \equiv 1 \pmod{r}$, can be calculated, and d' recovers unencrypted message $a \equiv b^{d'} \pmod{N}$ (in contrast to using d , with $cd = 1 \pmod{(p-1)(q-1)}$, where $N = pq$ and r divides $(p-1)(q-1) = |G_{pq}|$).

5.



Grover '96 (p.90), $f(x) = 1$ only for (m) marked value(s) $x = a$, uses "phase kickback" to express \mathbf{U}_f in terms of $\mathbf{V} = \mathbf{1} - 2|a\rangle\langle a|$, and $\mathbf{W} = 2|\phi\rangle\langle\phi| - \mathbf{1} = \mathbf{H}^{\otimes n} (2|0\rangle\langle 0| - \mathbf{1}) \mathbf{H}^{\otimes n}$ is easily constructed. Applying $\ell \approx \frac{\pi}{4} \frac{2^{n/2}}{\sqrt{m}}$ times gives probability $p(a) \approx 1 - O(m/2^n)$, for square-root speedup ($2^n/m \rightarrow \sqrt{2^n/m}$).

m marked states

$$f(x) = \begin{cases} 1 & x \in Y \\ 0 & x \notin Y \end{cases}$$

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

$Y =$ set of marked states

$$|Y| = m$$

$$|\varphi\rangle = \frac{1}{\sqrt{2^n}} \sum_{0 \leq x < 2^n} |x\rangle = \cos\theta |no\rangle + \sin\theta |yes\rangle$$

$$|yes\rangle = \frac{1}{\sqrt{m}} \sum_{x | f(x)=1} |x\rangle$$

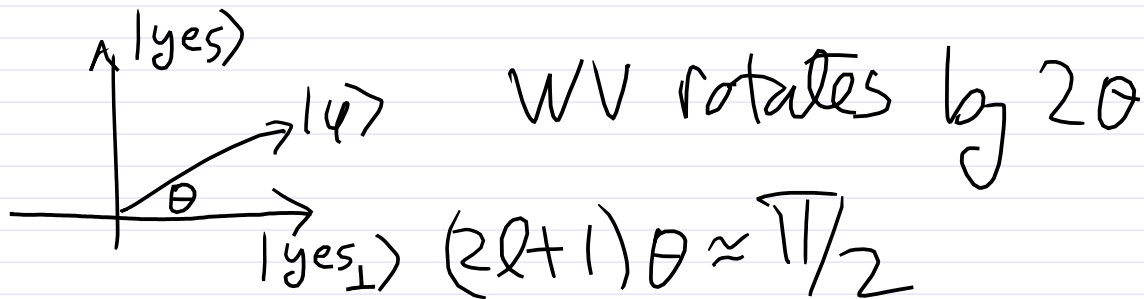
$$|no\rangle = \frac{1}{\sqrt{2^n - m}} \sum_{x | f(x)=0} |x\rangle$$

$$\sin\theta = \langle yes | \varphi \rangle = \sqrt{\frac{m}{2^n}}$$

$$\cos\theta = \langle no | \varphi \rangle = \sqrt{1 - \frac{m}{2^n}}$$

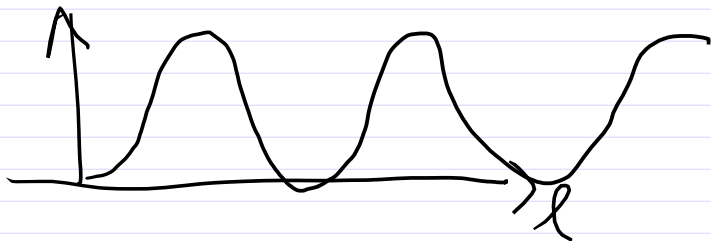
$$V = | -2 | \text{yes} \rangle \langle \text{yes} |$$

$$W = 2 | \varphi \rangle \langle \varphi | - 1$$



$$\theta \approx \sqrt{\frac{m}{2^n}} = \sqrt{\frac{m}{N}}$$

$$l \approx \frac{\pi}{4} \sqrt{\frac{N}{m}}$$



$\langle \text{yes} | (WV)^n | \varphi \rangle$ is periodic

$\approx \sin 2l\theta$ in $l \pm \pi/\theta$

so period = $\frac{\pi 2^{n/2}}{\sqrt{m}}$.

Run QFT to get period, gives m
then Grover $\frac{\pi}{4} \sqrt{N/m}$ times

A special case: $m=1$ $n=2$ ($N=4$)

$$\sin \theta = \langle a | \varphi \rangle = \frac{1}{2^{n/2}} = 1/2 \quad \theta = \pi/6$$



WV rotates by $\pi/3$
single WV exactly $|a\rangle$

Q.M.: $\frac{1}{4} \cdot 1 + \frac{3}{4} \frac{1}{3} 2 + \frac{1}{2} 3$
| classically expect $= 2^{1/4}$