Quantum computation

Lecture 17

Quantum search algorithms

pad

Task: Search space of $N\ (=2^n)$ of N possibilities for a solution to some problem.

Oracle: When consulted, can report whether a particular x is a solution
(black box)

↓

Not easy to find a solution, but easy to check.

$$f(x) = \begin{cases} 0, & \text{if } x \text{ is not a solution} \\ 1, & \text{if } x \text{ is a solution} \end{cases}$$

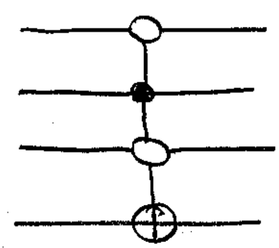
Assume there are M solutions

The oracle evaluates the function f:

$$|x\rangle \otimes |y\rangle \xrightarrow[O]{} |x\rangle \otimes |y \oplus f(x)\rangle$$

controlled bit flip — flip if $f(x) = 1$.

Example:



Classically, $O(N/M)$ oracle calls

Qmally, $O(\sqrt{N/M})$ oracle calls

↓

Quantum parallelism + phase kickback

$$|x\rangle \otimes |-\rangle \xrightarrow[O]{} (-1)^{f(x)} |x\rangle \otimes |-\rangle$$

phase kickback

we can forget this

Quantum algorithm

① Prepare n qubits in state $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle = H^{\otimes n}|0\rangle$

② Oracle: $O = \sum_x (-1)^{f(x)} |x\rangle\langle x| = \underbrace{\sum_{\{x|f(x)=0\}} |x\rangle\langle x|}_{P_0} - \underbrace{\sum_{\{x|f(x)=1\}} |x\rangle\langle x|}_{P_1} = \begin{matrix} 2P_0 - I \\ I - 2P_1 \end{matrix}$.

③ $H^{\otimes n}$

④ Contolled phase that reverses sign of all $|x\rangle$ except $|0\rangle$:

$$|0\rangle\langle 0| - \sum_{x\neq 0} |x\rangle\langle x| = 2|0\rangle\langle 0| - I$$

⑤ $H^{\otimes n}$

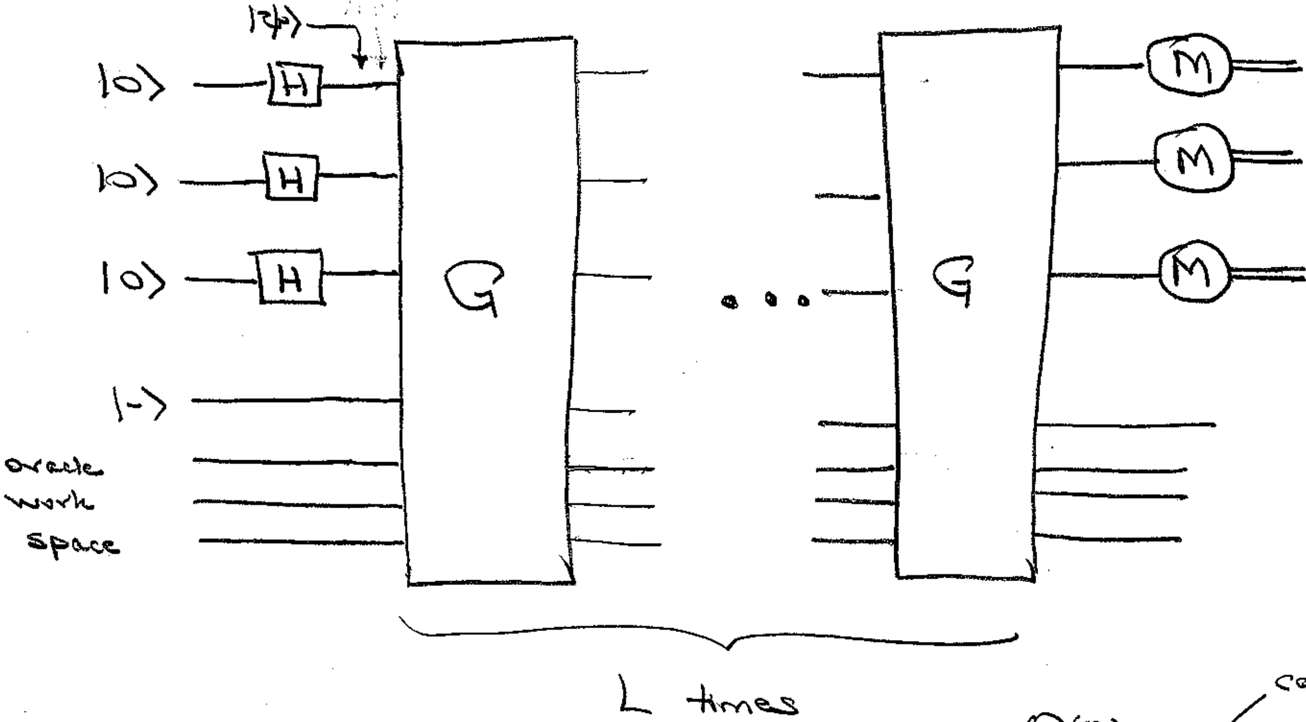
⑥ Repeat ②-⑤ $L = \underbrace{\text{nearest integer}\left(\frac{\pi}{4\sin^{-1}(\sqrt{M/N})} - 1\right)}_{\simeq \frac{\pi}{4}\sqrt{\frac{N}{M}} \text{ for } M \ll N}$ times.

⑦ Measure in computational basis.

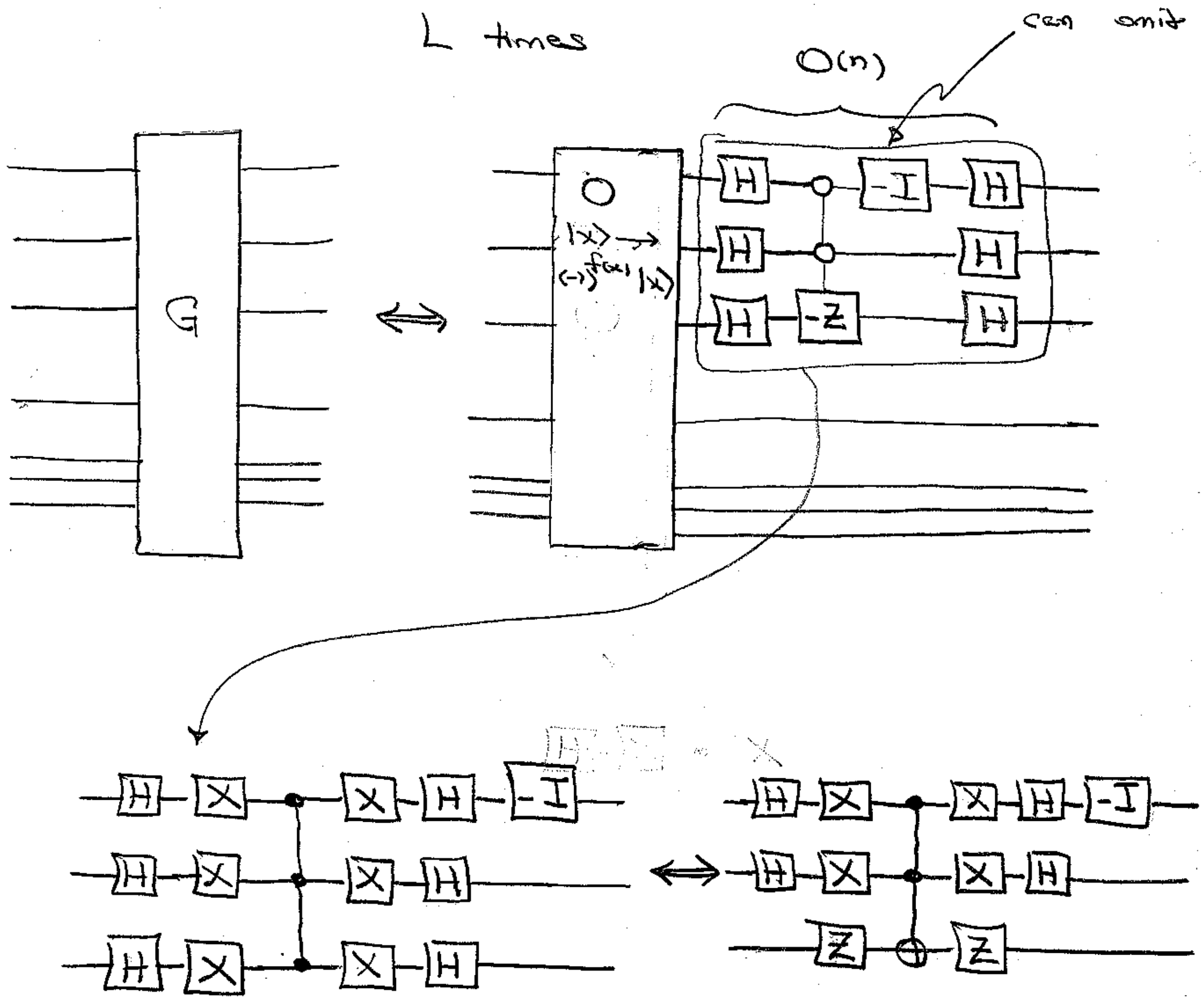
$$H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} = 2|\psi\rangle\langle\psi| - I = P_\psi - P_\psi^\perp$$

②-⑤: Grover iterate $G = (P_\psi - P_\psi^\perp)\underbrace{(P_0 - P_1)}_{O}$

Circuit: $n=3$



$|\psi\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|-\rangle$
H
H
H
G
G
M
M
M
oracle work space
L times



can omit
O(n)
G
O
$|x\rangle \rightarrow (-1)^{f(x)}|x\rangle$
H
-I
-Z
X
Z

What's happening?

Consider 2-d subspace spanned by

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_{\{x | f(x)=0\}} |x\rangle \quad \text{and} \quad |\beta\rangle = \frac{1}{\sqrt{M}} \sum_{\{x|f(x)=1\}} |x\rangle$$

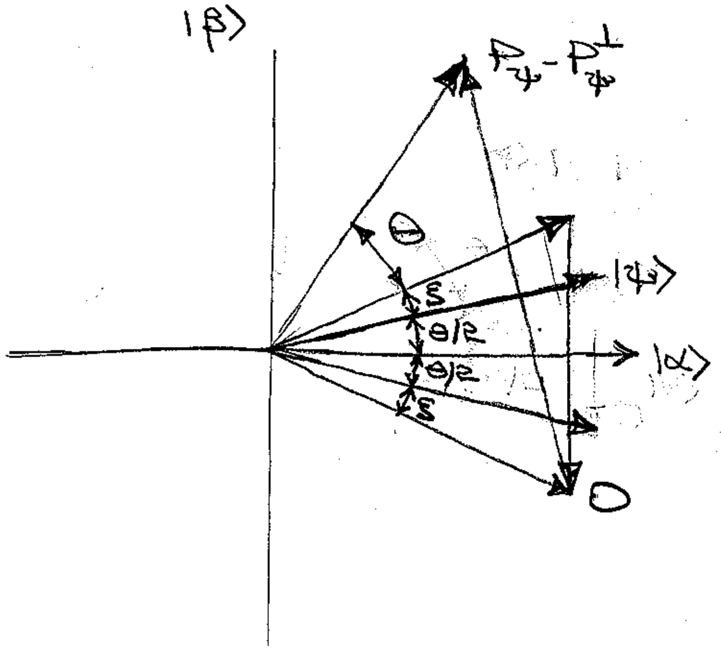
① $|\psi\rangle = \sqrt{\frac{N-M}{N}}\,|\alpha\rangle + \sqrt{\frac{M}{N}}\,|\beta\rangle$

② $O\big(a|\alpha\rangle + b|\beta\rangle\big) = (P_0 - P_1)\big(a|\alpha\rangle + b|\beta\rangle\big) = a|\alpha\rangle - b|\beta\rangle$

③ $\big(P_\psi - P_\psi^\perp\big)\big(a|\psi\rangle + b|\phi\rangle\big) = a|\psi\rangle - b|\phi\rangle$

reflection through $|\alpha\rangle$

reflection through $|\psi\rangle$



$$\cos(\theta/2) = \langle\alpha|\psi\rangle = \sqrt{\frac{N-M}{N}} = \sqrt{1-\frac{M}{N}}$$

$$\sin(\theta/2) = \sqrt{M/N}$$

$M/N \ll 1: \quad \theta \simeq 2\sqrt{M/N}$

$M = N/2: \quad \theta = \pi/2$

$M=1,\ N=4$
$\sin^2(\theta/2) = \frac{1}{4},\quad \cos\theta = \frac{1}{2},\quad \theta = 60°$
1 iteration gets it exactly right.

$$\begin{pmatrix}\text{optimal \#}\\ \text{of iterations}\end{pmatrix} = \begin{matrix}\text{nearest}\\ \text{integer}\end{matrix}\left(\frac{\pi}{2\theta} - 1\right) \xrightarrow[M/N \ll 1]{} \frac{\pi}{4}\sqrt{\frac{N}{M}}$$

$\frac{\theta}{2} + L\theta$ as near to $\pi/2$ as possible; always $\theta/2$ or closer

$$\begin{pmatrix}\text{probability of}\\ \text{getting a solution}\end{pmatrix} = \sin^2\left(\frac{\theta}{2} + L\theta\right) \geq \cos^2(\theta/2) \xrightarrow[M/N \ll 1]{} 1 - \frac{M}{N}$$

$$= 1 - \frac{M}{N}$$

Counting the solutions:

Eigenvectors and eigenvalues of G in 2-d subspace

$$G \frac{1}{\sqrt{2}}(|\alpha\rangle \pm i|\beta\rangle) = e^{\mp i\theta} \frac{1}{\sqrt{2}}(|\alpha\rangle \pm i|\beta\rangle)$$

Run the phase estimation algorithm on G using $|\psi\rangle$ as input. Get θ or $-\theta$ as output, and thus determine M.

<u>Optimality</u>. Why not $N^{1/4}$ or even an exponential improvement over classical searching? It turns out that $\sqrt{N}$ is the best that can be done. Here's the argument.

Let's assume $M=1$ (one solution). Start with arbitrary state $|\psi\rangle$. By alternative application of the oracle O_x and any unitaries we want, we get to the state

$$|\psi_k^x\rangle = U_k O_x U_{k-1} O_x \cdots U_1 O_x |\psi\rangle$$

after k iterations. For the search to succeed for arbitrary x, we need $|\langle x|\psi_k^x\rangle|^2 = \begin{pmatrix}\text{success} \\ \text{probability}\end{pmatrix} \geq \frac{1}{2}$ for all x. This means that the states $|\psi_k^x\rangle$ must diverge from one another as k increases. What we will show is, first, that the states $|\psi_k^x\rangle$

must diverge from

$$|\psi_k\rangle = U_k U_{k-1} \cdots U_1 |\psi\rangle = \begin{pmatrix}\text{state with no} \\ \text{oracle calls}\end{pmatrix}$$

and, second, that sufficient divergence can be achieved only for $k \gtrsim \sqrt{N}$. We do the former in two steps

① $$\|\psi_k^x - x\|^2 = 2 - 2\,\mathrm{Re}\big(\underbrace{\langle x|\psi_k^x\rangle}_{\text{choose real and positive}}\big) = 2 - 2\langle x|\psi_k^x\rangle \le 2\left(1 - \frac{1}{\sqrt{2}}\right)$$

expresses required closeness of $|\psi_k^x\rangle$ to $|x\rangle$

$$E_k = \frac{1}{N}\sum_x \|\psi_k^x - x\|^2 \le 2 - \sqrt{2}$$

② $$F_k = \frac{1}{N}\sum_x \|x - \phi\|^2 = 2 - \frac{2}{N}\sum_x \mathrm{Re}(\langle x|\phi\rangle)$$

$$\ge 2 - \frac{2}{N}\underbrace{\sum_x |\langle x|\phi\rangle|}_{\le \sqrt{N}}$$

$$F_k \ge 2\left(1 - \frac{1}{\sqrt{N}}\right)$$

expresses fact that no vector can be close to all members of an orthonormal basis.

We apply ① and ② to the desired measure of divergence, $D_k \equiv \frac{1}{N}\sum_x \|\psi_k^x - \psi_k\|^2$. To do so, We will twice use 2 applications of the Schwarz inequality.

$$\|a+b\|^2 = \|a\|^2 + \|b\|^2 + 2\,\mathrm{Re}\langle a|b\rangle$$

$$\begin{matrix}\le\\ \ge\end{matrix}\ \|a\|^2 + \|b\|^2 \pm 2\underbrace{|\langle a|b\rangle|}_{\le \|a\|\,\|b\| \quad \text{Schwarz inequality}}$$

$$\|a+b\|^2 \begin{matrix}\le\\ \ge\end{matrix} \|a\|^2 + \|b\|^2 \pm 2\|a\|\,\|b\| = \left(\|a\| \pm \|b\|\right)^2$$

$$\sum_x \|a_x + b_x\|^2 \begin{matrix}\le\\ \ge\end{matrix} \underbrace{\sum_x \|a\|^2}_{\equiv A^2} + \underbrace{\sum_x \|b_x\|^2}_{\equiv B^2} \pm 2\underbrace{\sum_x \|a_x\|\,\|b_x\|}_{\le \left(\sum_x \|a_x\|^2\right)^{1/2}\left(\sum_x \|b_x\|^2\right)^{1/2}}$$

$$\begin{matrix}\le\\ \ge\end{matrix}\ A^2 + B^2 \pm 2AB = (A \pm B)^2$$

Let's apply this to D_k

$$D_k = \frac{1}{N}\sum_x \|\psi_k^x - \psi_k\|^2$$

$$= \frac{1}{N}\sum_x \|\psi_k^x - x + x - \psi_k\|^2$$

$$\ge E_k + F_k - 2\sqrt{E_k F_k}$$

$$= \left(\sqrt{F_k} - \sqrt{E_k}\right)^2$$

Plugging in our bounds on E_k and F_k, we get

$$D_k \ge \left[\sqrt{2}\left(1-\frac{1}{\sqrt{N}}\right)^{1/2} - \sqrt{2}\left(1-\frac{1}{\sqrt{2}}\right)^{1/2}\right]^2$$

$$= 2\left(\sqrt{1-1/\sqrt{N}} - \sqrt{1-1/\sqrt{2}}\right)^2$$

$$\equiv C_N^2 \qquad C_N \xrightarrow[N\to\infty]{} \sqrt{2}\left(1-\sqrt{1-1/\sqrt{2}}\right) = 0.649$$

This inequality expresses the necessary average divergence of the set ψ_k^x from ψ_k required for the search algorithm to work. We now show that D_k can grow no faster than $4k^2/N$. We proceed by induction. $D_{k=0} = 0$, so the property holds for $k=0$. Assume $D_k \le 4k^2/N$. Then

$$D_{k+1} = \frac{1}{N}\sum_x \underbrace{\| U_{k+1} O_x \psi_k^x - U_{k+1}\psi_k \|^2}_{= \| O_x \psi_k^x - \psi_k \|^2}$$

$$O_x = I - 2|x\rangle\langle x|$$

$$(O_x - I)\psi_k = -2|x\rangle\langle x|\psi_k\rangle$$

$$= \frac{1}{N}\sum_x \| O_x(\psi_k^x - \psi_k) + (O_x - I)\psi_k \|^2$$

$$\le \frac{1}{N}\sum_x \|O_x(\psi_k^x - \psi_k)\|^2 + \frac{1}{N}\sum_x \|(O_x - I)\psi_k\|^2$$

$$+ \frac{1}{N}2\left(\quad\right)^{1/2}\left(\quad\right)^{1/2}$$

$$\sum_x \|(\psi_k^x - \psi_k)\|^2 = N D_k \qquad 4\sum_x |\langle x|\psi_k\rangle|^2 = 4$$

$$\Longrightarrow D_{k+1} \le D_k + \frac{4}{N} + \frac{2}{N}\sqrt{ND_k}\ 2$$

$$= \left(\sqrt{D_k} + \frac{2}{\sqrt{N}}\right)^2$$

Inductive hypothesis $\longrightarrow$

$$\le \left(\frac{2k}{\sqrt{N}} + \frac{2}{\sqrt{N}}\right)^2$$

$$= \frac{4(k+1)^2}{N}$$

So we end up with

$$\frac{4k^2}{N} \ge D_k \ge C_N^2 \Longrightarrow k \ge \frac{C_N}{2}\sqrt{N} \xrightarrow[N\to\infty]{} 0.324\sqrt{N}$$