# Grover's algorithm (ch. 6)

Search space N ($N = 2^n$), no structure

index 0 ... N−1

$f(x) = 0$ for most x

$f(x) = 1$ for a subset x → "marked" elem.
↳ size M that we look for

Oracle

class. need $O(N)$ queries

QM need $\sqrt{N}$ queries

↳ $|x\rangle|q\rangle \xrightarrow{O} |x\rangle|q \oplus f(x)\rangle$
↳ 1 bit

Observe: $|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \xrightarrow{O} (-1)^{f(x)}|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$

OR: $|x\rangle \xrightarrow{O} (-1)^{f(x)}|x\rangle$

Algorithm:

1. $|0\rangle^{\otimes n}$ $\qquad \overbrace{|0\rangle\ldots|0\rangle}^{n}$
2. $H^{\otimes n} \to \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle \to$ call it $|\psi\rangle$
3. repeat $\sim\sqrt{\frac{N}{M}}$ times
   - (a) call Oracle
   - (b) $H^{\otimes n}$
   - (c) cond. phase flip : $|0\rangle \to |0\rangle$, $|x\rangle \to -|x\rangle \quad \forall x \neq 0$ $\qquad \begin{bmatrix} 1 & & & \\ & -1 & & \\ & & \ddots & \\ & & & -1 \end{bmatrix}$
   - (d) $H^{\otimes n}$
4. measure

Note: if don't know $M$, can determine it using q. counting algorithm, in $O(\sqrt{N})$

How does it work?

(c) $\begin{bmatrix} 1 & & & \\ & -1 & & \\ & & \ddots & \\ & & & -1 \end{bmatrix} = 2|0\rangle\langle 0| - I$

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

$$|\psi\rangle\langle\psi| = \frac{1}{N}\begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}$$

$$|\psi\rangle\langle\psi| \sum \alpha_k |k\rangle = \frac{1}{N}\begin{bmatrix} 1 & 1 & \cdots & 1 \\ & & & \\ & & & \end{bmatrix}\begin{bmatrix} \alpha_0 \\ \vdots \\ \alpha_{N-1} \end{bmatrix} = \begin{bmatrix} \langle\alpha\rangle \\ \vdots \\ \langle\alpha\rangle \end{bmatrix}$$

$$\left(2|\psi\rangle\langle\psi| - I\right) \sum \alpha_k |k\rangle = 2\begin{bmatrix} \langle\alpha\rangle \\ \vdots \\ \langle\alpha\rangle \end{bmatrix} - \begin{bmatrix} \alpha_0 \\ \\ \alpha_{N-1} \end{bmatrix}$$

each elem. $2\langle\alpha\rangle - \alpha_k = \langle\alpha\rangle - \left(\alpha_k - \langle\alpha\rangle\right)$

INVERSION ABOUT AVERAGE

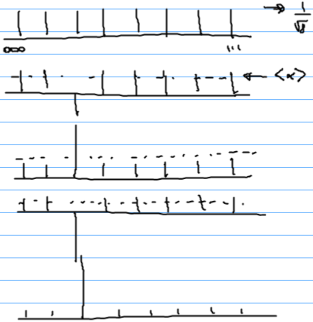
2

3a

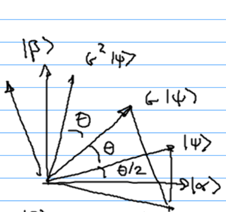
3b-d

3e

3b-d



# Optimal # iterations?




$$|\alpha\rangle \equiv \frac{1}{\sqrt{N-M}} \sum_x{}'' |x\rangle \longrightarrow x \text{ } \underline{\text{not}} \text{ sols.}$$

$$|\beta\rangle \equiv \frac{1}{\sqrt{M}} \sum_x{}' |x\rangle \longrightarrow x \text{ ARE sols.}$$

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

- oracle: $a|\alpha\rangle + b|\beta\rangle \to a|\alpha\rangle - b|\beta\rangle \to$ refl. about $|\alpha\rangle$
- $2|\psi\rangle\langle\psi| - I$: refl. about $|\psi\rangle$

→ rotation $G$

$$|\psi\rangle = \cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle$$

$$G|\psi\rangle = \cos\frac{3\theta}{2}|\alpha\rangle + \sin\frac{3\theta}{2}|\beta\rangle$$

$$G^k|\psi\rangle = \cos\left(\frac{2k+1}{2}\theta\right)|\alpha\rangle + \sin\left(\frac{2k+1}{2}\theta\right)|\beta\rangle$$

Optimum $k$: $\frac{\theta}{2} + k\theta \approx \frac{\pi}{2} \to k \approx \left(\frac{\pi}{\theta} - 1\right)\frac{1}{2} < \frac{\pi}{2\theta}$

if $M \ll N$: $\theta$ small, $\frac{\theta}{2} \sim \sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}$

$$k < \frac{\pi}{4}\sqrt{\frac{N}{M}}$$

NOTE: Grover's algorithm is optimal!

Applicability

① phone book of size $N$

name $\rightarrow$ #     binary search (efficient)

# $\rightarrow$ name     takes $O(N)$

q. alg $\rightarrow \sqrt{N}$ look ups

$\rightarrow$ not useful appl.

② $f$ can be efficiently evaluated

$f^{-1}$ cannot

NP-complete problems

SAT: $x_1 x_2 \bar{x}_3 + x_3 x_7 + x_2 x_4 + \cdots = 1$

$\exists\ x_i$ ? s.t.

No