Grover Search

Note Title 5/1/2012

We have seen a number of different problems in the query model where we are given black-box access to some function f typically in the form of a unitary U_f such that $U_f|x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$.
We are asked to solve some problem with this oracle which is usually to discover something about f.

In the search problem, we assume that f is boolean valued:

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

and we would like to know if $\exists\ a \in \{0,1\}^n$ such that $f(a) = 1$ (and if so, find a).

Note that any problem in the class NP can be formulated in this way where f is a poly-time (classically) computable function. For example in the problem 3-SAT, we want to know whether a boolean formula ϕ in 3-CNF form has a satisfying assignment. In this case the input x to f_ϕ would be a truth assignment to the variables in ϕ. $f_\phi(x) = 1$ iff x satisfies ϕ. Given ϕ, $f_\phi(x)$ is clearly in P.
We are asking here what kind of speed-up we can get by using a quantum circuit without using any specific knowledge about f.

We will assume for now that f has a unique solution or no solution:

$$|\{a \mid f(a) = 1\}| \leq 1.$$

Let a be this unique solution (if it exists).

Let $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle$

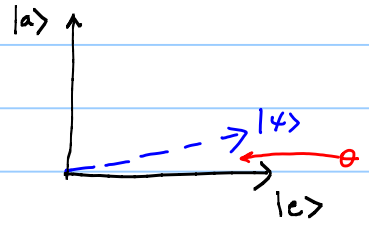
The algorithm will remain in the 2-dimensional subspace spanned by $|a\rangle$ and $|\psi\rangle$: $\alpha|a\rangle + \beta|\psi\rangle$.

It's better to define this space by two orthogonal states.

$$|e\rangle = |\psi\rangle - \underbrace{\langle a|\psi\rangle}_{1/\sqrt{N}} |a\rangle = \frac{1}{\sqrt{N}} \sum_{x \neq a} |x\rangle$$

$|e\rangle$ is orthogonal to $|a\rangle$ but not quite normalized:

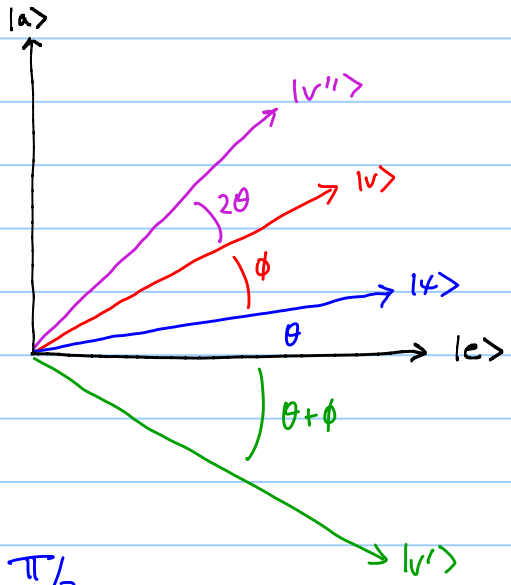
$$|e\rangle \leftarrow \frac{1}{\sqrt{N-1}} \sum_{x \neq a} |x\rangle$$



$$|\psi\rangle = \sqrt{\tfrac{N-1}{N}}\,|e\rangle + \tfrac{1}{\sqrt{N}}\,|a\rangle$$

In a general step, we start in some state $|v\rangle$

1. Rotate around $|e\rangle$ by π (result $|v'\rangle$)
2. Rotate around $|\psi\rangle$ by π (result $|v''\rangle$)



$|v''\rangle$ is now 2θ closer to $|a\rangle$.

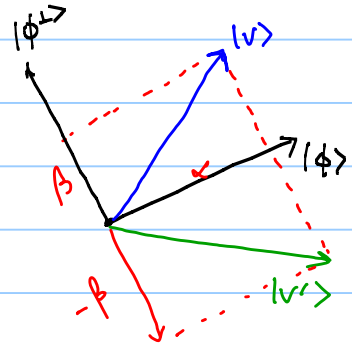
What is θ?

$$\langle\psi|e\rangle = \cos\theta$$

$$\tfrac{1}{\sqrt{N}} = \langle\psi|a\rangle = \sin\theta \sim \theta$$

Repeat c times: $\theta + 2c\theta \approx \pi/2$.

How to implement these rotations?



In general, to rotate state $|v\rangle$ around $|\phi\rangle$

express: $|v\rangle = \alpha|\phi\rangle + \beta|\phi^\perp\rangle$

$|v'\rangle = \alpha|\phi\rangle - \beta|\phi^\perp\rangle$

perp in 2D plane

Rotation around $|e\rangle$ by π: $|v\rangle = \alpha|e\rangle + \beta|a\rangle$

$|v'\rangle = \alpha|e\rangle - \beta|a\rangle$

$$|v\rangle = \sum_x \alpha_x |x\rangle \longrightarrow |v'\rangle = \sum_x \alpha_x (-1)^{f(x)} |x\rangle$$

this is -1 only when $f(x) = 1$ which is when $x = a$.

We have done this operation before. It is a call to U_f when extra qubit is $|-\rangle$:

$$\sum_x \alpha_x |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \longrightarrow \sum_x \alpha_x |x\rangle \left[\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \oplus f(x)\right]$$

$$\left[(-1)^{f(x)} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right]$$

Rotation about $|4\rangle$ by π: $|V\rangle = \alpha|4\rangle + \beta|4^\perp\rangle$

$|V'\rangle = \alpha|4\rangle - \beta|4^\perp\rangle$

$$(2|4\rangle\langle 4| - I) = (2|4\rangle\langle 4| - \underbrace{(|4\rangle\langle 4| + |4^\perp\rangle\langle 4^\perp|)}_{I})$$

$$= |4\rangle\langle 4| - |4^\perp\rangle\langle 4^\perp|$$

$$(|4\rangle\langle 4| - |4^\perp\rangle\langle 4^\perp|)[\alpha|4\rangle + \beta|4^\perp\rangle] = \alpha|4\rangle - \beta|4^\perp\rangle$$

$H^{\otimes n}|0\rangle = |4\rangle$ $\qquad$ $|4\rangle\langle 4| = H^{\otimes n}|0\rangle\langle 0|(H^{\otimes n})^\dagger$

$= H^{\otimes n}|0\rangle\langle 0|H^{\otimes n}$ $\qquad$ $H^\dagger = H$

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

controlled phase shift (everything except 0).
Compute OR of all the qubits and phase shift if this is 1.

Grover's Algorithm Recap:

$|0\rangle^n \xrightarrow{H^{\otimes n}} |+\rangle$

Repeat $\Theta(\sqrt{N})$ times:

(1) Rotate about $|e\rangle$ by π
apply U_f to $|+\rangle|-\rangle$

(2) Rotate about $|+\rangle$ by π
$H^{\otimes n}$, Controlled phase shift, $H^{\otimes n}$
(everything except $|0\rangle$)

Measure (outcome a). Check $f(a) = 1$.

Alternative View of Grover Search
(from Umesh's notes 2007 - Lecture 11)

Rotation about $|+\rangle$ can be seen as "inversion about the mean".
Consider vector $(\alpha_1 \ldots \alpha_N)$ where $\mu = \frac{1}{N}\sum_j \alpha_j$
Inversion about the mean is takes α_j to $2\mu - \alpha_j$.

This is exactly what $H^{\otimes n}\left(I - 2|0\rangle\langle 0|\right)H^{\otimes n}$ does

$$H^{\otimes n}\begin{bmatrix}-1 & & \\ & 1 & \\ & & \ddots \\ & & & 1\end{bmatrix}H^{\otimes n} = H^{\otimes n}\left[\begin{pmatrix}-2 & & \\ & 0 & \\ & & \ddots \\ & & & 0\end{pmatrix} + I\right]H^{\otimes n}$$

$$= H^{\otimes n}\begin{bmatrix}-2 & & \\ & 0 & \\ & & \ddots \\ & & & 0\end{bmatrix}H^{\otimes n} + I = \begin{bmatrix}-2/N & \cdots & -2/N \\ \vdots & & \vdots \\ -2/N & \cdots & -2/N\end{bmatrix} + I$$

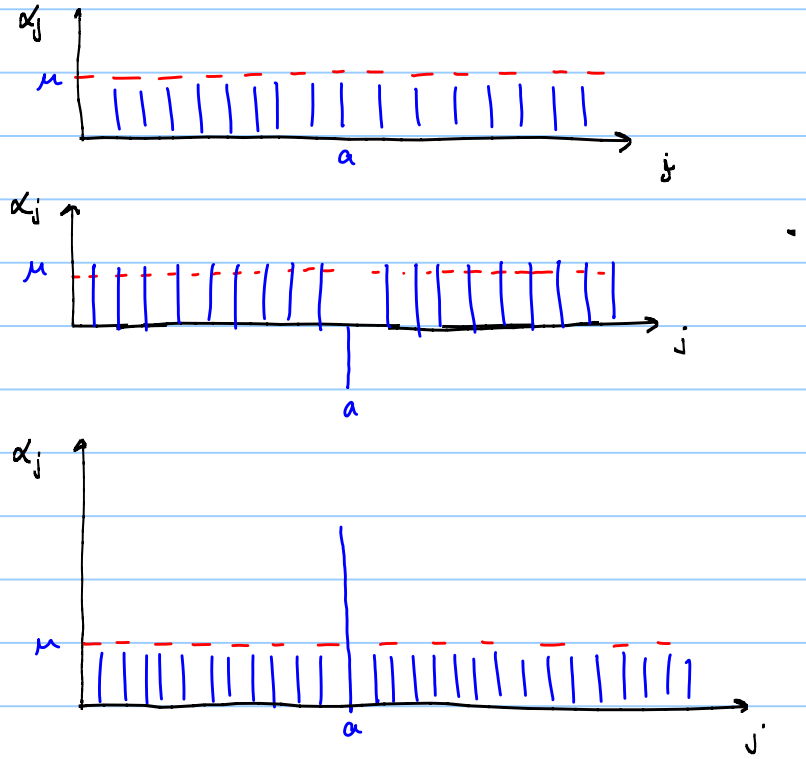
$$= \begin{bmatrix}-2/N+1 & & -2/N \\ & \ddots & \\ -2/N & & -2/N+1\end{bmatrix}$$

$H^{\otimes n} = \frac{1}{\sqrt{N}}\begin{bmatrix}1 & 1 & \cdots & 1 \\ 1 & & & \\ \vdots & & \pm 1 & \\ 1 & & & \end{bmatrix}$ First row + col of $H^{\otimes n}$ is $1/\sqrt{N}$

Grover starts in $|\psi\rangle = \frac{1}{\sqrt{N}}\sum_x |x\rangle$

Invert phase of a
Invert about mean
} α_a increases by $\frac{2}{\sqrt{N}}$

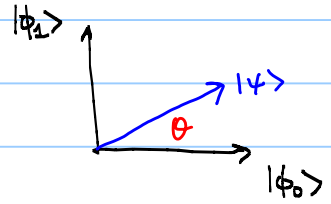
Repeat $O(\sqrt{N})$ times.



What if $\left|\{a \mid f(a)=1\}\right| = M > 1$?

$$|\phi_1\rangle = \frac{1}{\sqrt{M}} \sum_{\substack{x: \\ f(x)=1}} |x\rangle \qquad |\phi_0\rangle = \frac{1}{\sqrt{N-M}} \sum_{\substack{x: \\ f(x)=0}} |x\rangle$$

$$|\psi\rangle = \sqrt{\frac{N-M}{N}}\,|\phi_0\rangle + \sqrt{\frac{M}{N}}\,|\phi_1\rangle$$



$$\sin\theta = \sqrt{\frac{M}{N}}$$

If we know M, can select # iterations c s.t. $(2c+1)\theta \approx \frac{\pi}{2}$

If $M \ll N$ $\quad \theta \approx \sqrt{M/N}$ $\quad$ # iterations $O\left(\sqrt{N/M}\right)$.

Error: Since we advance by 2θ in each iteration, we can select the number of iterations so that we are within θ of the target $|a\rangle$.
The probability that we measure something in $|a\rangle$ is $\cos^2\theta$. The probability of error is $\sin^2\theta$.

$\sin^2\theta = M/N$.

So if we want this to be $1/4$ (for example), we want $\sin\theta \leq 1/2$
this is satisfied for $\theta \leq 1/2$.
So assume $M \leq N/2$.
(if $M > N/2$ can just sample randomly to get a solution).

Applications of unstructured search:

- → Approximate Counting
- → Random Generation.
- → Find minimum
- → $O(N^{1/3})$ for collisions

We will discuss approximate counting because it is useful for the case where M is unknown.