Grover Search - page 1

Monday, November 19, 2018 8:15 AM

Can Quantum Computers solve NP-complete problems?

NP: A class of decision problems (Yes/No answer)
If the answer on a particular input is Yes, then a solution can be verified in polynomial time.
(Finding a solution to verify may still be hard.)

For example Consider the problem 3SAT
Input: Boolean formula ϕ (in 3 CNF form)
n Boolean input variables $\phi(x_1, x_2, \ldots, x_n)$
$x_i \in \{0, 1\}$
Output: Does ϕ have a satisfying assignment?
Is there a setting $x_i \leftarrow 0/1$
that causes ϕ to evaluate to 1?

This is a Yes/No question.

If ϕ is satisfiable, and someone gives you $x \in \{0,1\}^n$ a Boolean assignment to $x_1, \ldots, x_n$, it can be easily verified that x satisfies ϕ.

Is it possible to solve 3SAT in polynomial time?

Monday, November 19, 2018 8:23 AM

NP- complete problems are the hardest problems in NP.

If there is a poly-time algorithm for any NP- complete problem then there is a poly-time algorithm for every problem in NP.

3SAT is NP - complete.

Important NP- complete problems abound in many areas of operations research, physical sciences, biology, engineering.

It is generally believed that it is impossible to solve any NP- complete problem in polynomial time.

What about Quantum Computers?

Grover Search - page 3

Thursday, November 15, 2018 3:19 PM

Back to the query model where we are given black-box access to a function f in the form of a unitary U_f:

$$U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$$

We are asked to solve some problem with this oracle which usually involves figuring something out about f.

Search problem: f is boolean valued:

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

Want to know if $\exists x$ such that $f(x) = 1$.
(and if so, find x).

Note that any problem in NP can be formulated in this way where f is a classical poly-time computable function.

For example Consider the problem 3SAT
Input: Boolean formula ϕ (in 3 CNF form)
n Boolean input variables $\phi(x_1, x_2, \ldots, x_n)$
$x_i \in \{0,1\}$
Output: Does ϕ have a satisfying assignment?

Thursday, November 15, 2018 3:27 PM

For example Consider the problem 3SAT

Input: Boolean formula ϕ (in 3 CNF form)
n Boolean input variables $\phi(x_1, x_2, \ldots, x_n)$
$x_i \in \{0, 1\}$

Output: Does ϕ have a satisfying assignment?

x would be the assignment of 0/1 values to $x_1, \ldots, x_n$

$f_\phi(x) = 1$ if x satisfies ϕ.

Given ϕ f_ϕ can be computed in poly time.

What kind of speed up can we get with a quantum circuit without knowing anything about f?

For now, assume f a unique solution or no solution.

$$\left| \{x \mid f(x) = 1\} \right| = 0 \text{ or } 1.$$

Let a be the unique solution if it exists.

Thursday, November 15, 2018 3:32 PM

$f(a) = 1$.

Grover's Algorithm

Let $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle$ $\qquad H^{\otimes n}|0\cdots0\rangle = |\psi\rangle$

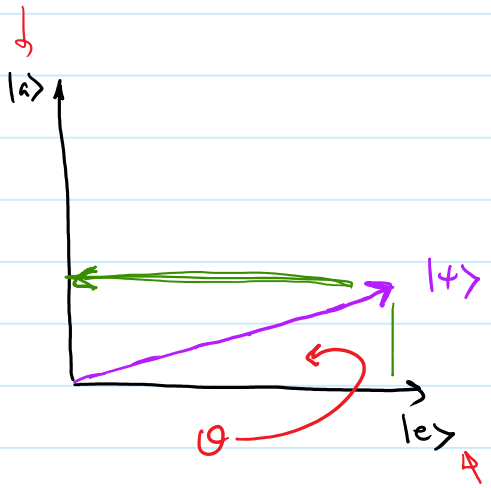
The algorithm will remain in the space spanned by $|a\rangle$ and $|\psi\rangle$.

Note that $|a\rangle$ and $|\psi\rangle$ are not orthogonal. It's better to describe this space with two orthonormal states.

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

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

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



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

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

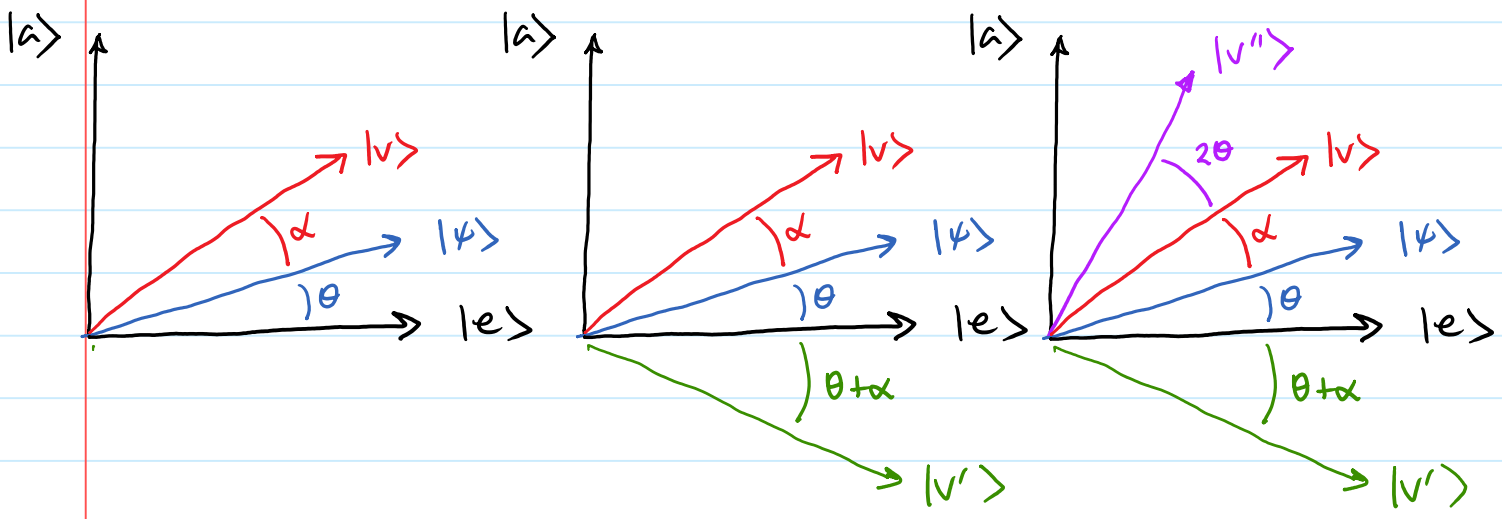
$$\psi = \frac{1}{\sqrt{N}} \sum_x |x\rangle \qquad \theta \approx \frac{1}{\sqrt{N}}.$$

Sunday, November 18, 2018 1:36 PM

In a general step, we start with 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?

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

$$\cos\theta = \langle\psi|e\rangle$$
$$\sin\theta = \langle\psi|a\rangle = \frac{1}{\sqrt{N}}.$$

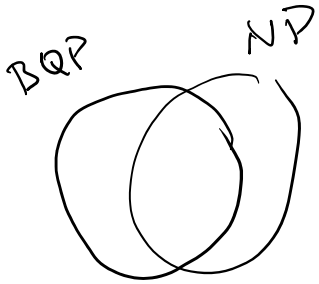
For small θ, $\sin\theta \sim \theta \Rightarrow \theta \sim \frac{1}{\sqrt{N}}$.

Repeat c times so that $\theta + 2c\theta \approx \frac{\pi}{2}$.

Grover Search - page 7

Sunday, November 18, 2018 1:36 PM

$N = 2^n$.



Repeat c times so that $\theta + 2c\theta \approx \frac{\pi}{2}$.

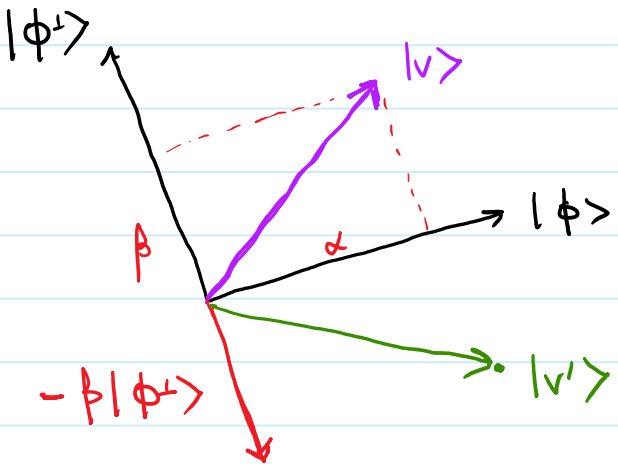
$$\frac{1}{\sqrt{N}} + \frac{2c}{\sqrt{N}} \approx \frac{\pi}{2}. \qquad c \approx \sqrt{N}\,\frac{\pi}{4} - \frac{1}{2}$$

How to implement these rotations:

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

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

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



Rotation around $|e\rangle$ be π.

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

Sunday, November 18, 2018 7:00 PM

Rotation around $|e\rangle$ be 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 the extra qubit is $|-\rangle$:

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

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

$I = |0\rangle\langle 0| + |1\rangle\langle 1|$
$|+\rangle\langle +| + |-\rangle\langle -|$

Sunday, November 18, 2018 7:05 PM

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

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

$(2|\psi\rangle\langle\psi| - I) =$

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

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

Check: $(|\psi\rangle\langle\psi| - |\psi^\perp\rangle\langle\psi^\perp|)[\alpha|\psi\rangle + \beta|\psi^\perp\rangle]$

$= \alpha|\psi\rangle - \beta|\psi^\perp\rangle$

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

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

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

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

$2H^{\otimes n}|0\cdots 0\rangle\langle 0\cdots 0|\cdot H^{\otimes n} - H^{\otimes n}\cdot I\cdot H^{\otimes n}$

$H^{\otimes n}(|0\rangle\langle 0| - |1\rangle\langle 1|)H^{\otimes n} = 2|+^n\rangle\langle +^n| - I.$

2 $H^{\otimes n}|0\rangle\langle 0|\cdot H^{\otimes n} - H^{\otimes n}\cdot I\cdot H^{\otimes n}$

$A|0\cdots0\rangle = |0\cdots0\rangle$
$A|x\rangle = -x.$
$x \neq 0.$

Sunday, November 18, 2018 7:17 PM

$$H^{\otimes n}\left(2|0\cdots0\rangle\langle 0\cdots0| - I\right)H^{\otimes n} = 2|\psi\rangle\langle\psi| - I.$$

Controlled phase shift
Apply phase shift of (-1) to every state except $|0\cdots0\rangle$.

Grover's Algorithm Recap:

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

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

① Rotate about $|e\rangle$ by π
apply U_f to $|\psi\rangle|-\rangle$

② Rotate about $|\psi\rangle$ by π
$H^{\otimes n}$, controlled phase shift, $H^{\otimes n}$
$\times(-1)$ to every state
except $|0\cdots0\rangle$.

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

Final state $= |v\rangle$ Probability of measuring a is $|\langle v|a\rangle|^2$. $\sim 1 - 1/N$.