Lecture 19

Tuesday, July 25, 2017 2:07 PM

Quantum algorithms

1. Shor's algo: Given N, factor it.

Have BQP algo for Factoring!

2. Simon's algo: Given a polysize classical circuit computing

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

s.t. $\exists\, a \in \{0,1\}^n$, $a \neq 0^n$,

$$\forall x \neq y, \quad f(x) = f(y) \iff x = y \oplus \underset{\substack{\uparrow \\ \text{period}}}{a}$$

x, $x \oplus a$ $\qquad f(x) = f(x \oplus a)$

y, $y \oplus a$ $\qquad f(y) = f(y \oplus a)$

. . . .

Have BQP algo for this!

Have BQP algo for this!

3. Grover's Search algo: Given a polysize classical circuit computing

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

s.t. $\exists$ unique $a \in \{0,1\}^n$: $f(a) = 1$

find this a.

Have quantum $2^{n/2}$-time algo.

Simon's algo:

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

$\exists\ a \in \{0,1\}^n$

$\forall x \neq y, \ [f(x) = f(y) \iff x = y \oplus a]$

1. $|0^n\rangle \xrightarrow{H} \sum_{x \in \{0,1\}^n} |x\rangle$

2. $\sum_{x \in \{0,1\}^n} |x\rangle |0\rangle \longmapsto \underbrace{\sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle}$

$\parallel$

$\sum_{x \in \{0,1\}^n} \left(|x\rangle + |x \oplus a\rangle \right) |f(x)\rangle$

measure

$f(x)$ for uniform random $x \in \{0,1\}^n$

$|x\rangle + |x \oplus a\rangle$

3.

$$\downarrow H$$

$$\sum_{y\in\{0,1\}^n}(-1)^{\langle x,y\rangle}\cdot|y\rangle+\sum_{y\in\{0,1\}^n}(-1)^{\langle x\oplus a,y\rangle}\cdot|y\rangle$$

$x=x_1\ldots x_n\in\{0,1\}^n$

$|x\rangle$

$$H|x\rangle=(|0\rangle+(-1)^{x_1}|1\rangle)$$
$$(|0\rangle+(-1)^{x_2}|1\rangle)$$
$$\vdots$$
$$(|0\rangle+(-1)^{x_n}|1\rangle)$$

$$=\sum_{y\in\{0,1\}^n}(-1)^{\langle x,y\rangle}|y\rangle$$

$$(-1)^{x_1}(-1)^{x_2}\ldots(-1)^{x_n}$$
$$=(-1)^{\sum x_i}$$
$$=(-1)^{\langle x,y\rangle}$$

e.g. $y=1^n$,

$$=(-1)$$

$$\langle x,y\rangle \qquad \sum(\ \ )^{\langle x\oplus a,y\rangle}$$

$$\sum_y (-1)^{\langle x,y\rangle} |y\rangle + \sum_y \underbrace{(-1)^{\langle x\oplus a, y\rangle} \cdot |y\rangle}_{\text{//Exercise}}$$

$$= \sum_y \Big(\underbrace{(-1)^{\langle x,y\rangle} + (-1)^{\langle x,y\rangle} \cdot (-1)^{\langle a,y\rangle}}_{(*)} \Big) \cdot |y\rangle$$

If $\langle a,y\rangle = 1 \mod 2$

then $(*) = 0$

5. Measure

Get classical y s.t. $[\langle a,y\rangle = 0 \mod 2$

uniform random

$$\sum a_i y_i = 0 \mod 2$$

$$y_1 a_1 + y_2 \cdot a_2 + \ldots + y_n \cdot a_n = 0 \ (\mathrm{mod}\ 2)$$

constants

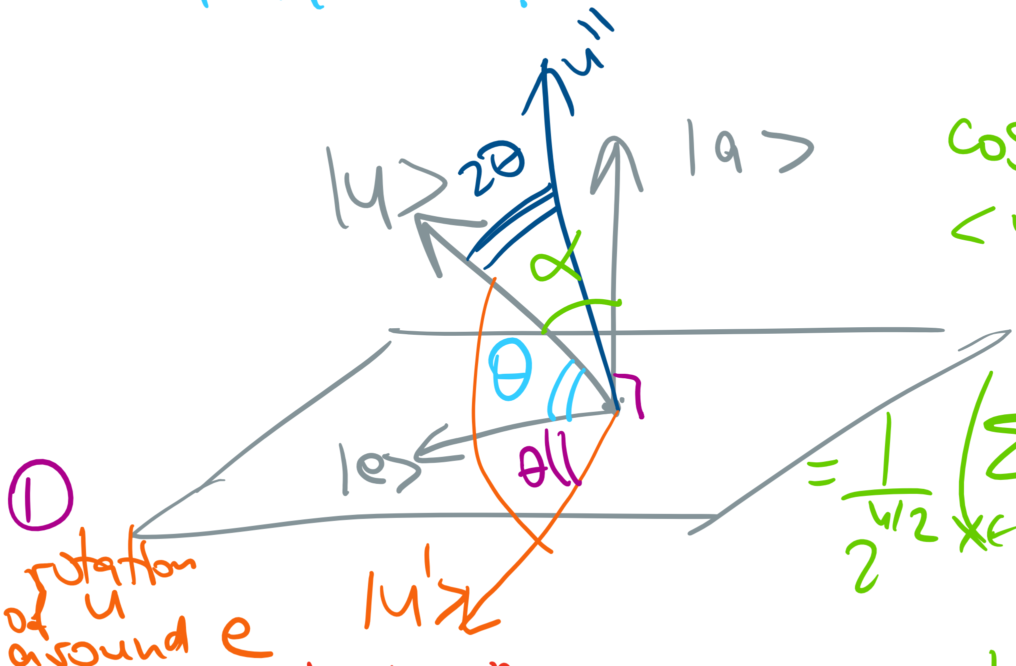
Repeat enough times,
setting t
random eq'ns
for a.
W.h.p., if $t > 2n$,
get $n-1$ lin. indep.
eq'ns in a,
which can solve by Gauss.
Get my a.

Grover's Search

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

$\exists$ unique $a \in \{0,1\}^n$, $f(a) = 1$.

Find a.



$\cos\alpha = \langle u | a \rangle$

$= \frac{1}{2^{n/2}} \left(\sum_{x \in \{0,1\}^n} |x\rangle \right)$.

$|a\rangle$

$|u\rangle = H|0^n\rangle$

$|e\rangle = |u\rangle - |a\rangle$

$\theta = \frac{\pi}{2} - \alpha$

$\alpha = \frac{\pi}{2} - \theta \Rightarrow \cos\alpha = \cos\left(\frac{\pi}{2} - \theta\right)$

$\frac{1}{2^{n/2}} = \boxed{\sin\theta}$

$\sin\theta \approx \theta$ for "small" θ

$\boxed{\theta \approx \frac{1}{2^{n/2}}}$

Run time $\to O\left(\frac{1}{\theta}\right)$

$= O(2^{n/2})$.

② Reflect u' around u $\Big\} = O(2^{n/2})$.

Reflection of w around e:

$$w = \underbrace{\left(\sum_{x \neq a} w_x \cdot |x\rangle \right)}_{=e} + w_a \cdot |a\rangle$$

$\big\downarrow$ reflection around e

$$w' = \left(\sum_{x \neq a} w_x \cdot |x\rangle \right) - w_a \cdot |a\rangle$$

Quantum Magic:

$$\left(\sum w_x \cdot |x\rangle |0\rangle \right) + w_a \cdot |a\rangle \cdot |1\rangle$$

$$\underbrace{\left(\sum_{x \neq a} w_x \cdot |x\rangle \underline{\underline{|0\rangle}}\right) + w_a \cdot |a\rangle \cdot \underline{\underline{|1\rangle}}}$$

$\Downarrow$ Z-operation to last qubit

$$Z: \begin{array}{l} |0\rangle \to |0\rangle \\ |1\rangle \to -|1\rangle \end{array}$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\sum_{x \neq a} w_x \cdot |x\rangle |0\rangle - w_a \cdot |a\rangle \cdot |1\rangle$$

"uncompute of"

$$\sum_{x \neq a} w_x \cdot |x\rangle \cancel{|0\rangle} - w_a \cdot |a\rangle \cdot \cancel{|0\rangle}$$

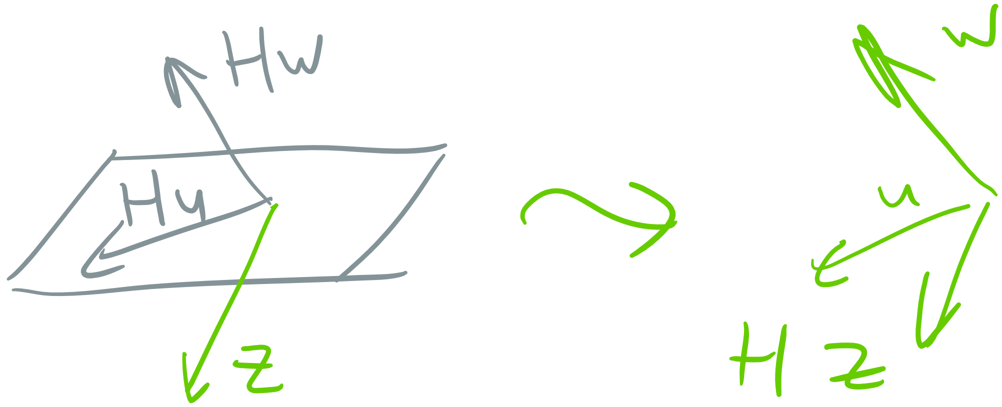
Reflection of w around u:

Hw around $Hu = |0^n\rangle$

$(H \cdot H \cdot |0^n\rangle = |0^n\rangle)$

$g(0^n) = 1$

$g(x) = 0 \quad \forall x \neq 0^n$



Unitary matrices

(1) $\langle Hv, Hw \rangle = \langle v, w \rangle$

(2) $\langle Hv, Hv \rangle = \langle v, v \rangle$