Quantum Algorithm

Thursday, May 14, 2020 11:46 AM

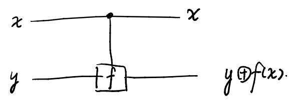
§ 5.3 Quantum algorithms

1. Deutsch - Jozsa algorithm

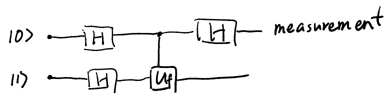
$f: \{0,1\} \longrightarrow \{0,1\}$ Decide whether $f(0) = f(1)$.

Classical: two visit to f. $\boxed{f}$ black box / oracle.

Quantum



$\longleftarrow$ Quantum black box.



Input $|01\rangle$

$$\longrightarrow \frac{1}{2}(|0\rangle+|1\rangle)(|0\rangle-|1\rangle).$$

$$\xrightarrow{C\text{-}U_f} \frac{1}{2}\left[|0\rangle(|0\oplus f(0)\rangle-|1\oplus f(0)\rangle) + |1\rangle(|0\oplus f(1)\rangle-|1\oplus f(1)\rangle)\right]$$

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

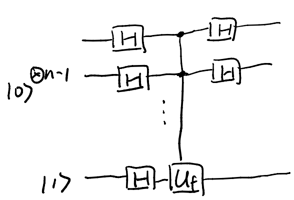
$$= \frac{1}{2}\left(\left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right)(|0\rangle-|1\rangle)\right).$$

$$\xrightarrow{H_1} \frac{1}{2}\left[\left((-1)^{f(0)}+(-1)^{f(1)}\right)|0\rangle + \left((-1)^{f(0)}-(-1)^{f(1)}\right)|1\rangle\right](|0\rangle-|1\rangle).$$

$$\xrightarrow{\text{Measurement}} \text{Prob. in } |0\rangle = \frac{1}{4}\left|(-1)^{f(0)}+(-1)^{f(1)}\right|^2 = \begin{cases} 1 & \text{when } f(0)=f(1) \\ 0 & \text{when } f(0)\neq f(1) \end{cases}$$

Extend to n-bit: $f:\{0,1\}^n \longrightarrow \{0,1\}$

to decide if $f(x)$ $\begin{cases} \text{constant: } f(x)=c \\ \text{balanced: } f(x)=0. \end{cases}$



$$|\psi\rangle \xrightarrow{H^n} \frac{1}{\sqrt{2^{n-1}}}\sum_{x=0}^{2^{n-1}-1} |x\rangle(|0\rangle-|1\rangle)$$

$$\xrightarrow{C\text{-}U_f} \frac{1}{\sqrt{2^{n-1}}}\sum_{x=0}^{2^{n-1}-1} (-1)^{f(x)}|x\rangle(|0\rangle-|1\rangle)$$

$$\xrightarrow{H^{n-1}} \underbrace{\frac{1}{N}\sum_{x,y}(-1)^{f(x)}(-1)^{x\cdot y}}_{c_y}|y\rangle \qquad x\cdot y = x_1y_1\oplus x_2y_2\oplus\cdots\oplus x_ny_n$$

$$\text{Prob} = |c_y|^2$$

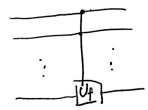
2. Grover Search Algorithm.

structure search (some order for key value) / unstructured search

$$f_w : \{0,1\}^{\otimes n} \longrightarrow \{0,1\}$$

$2^n = N$.

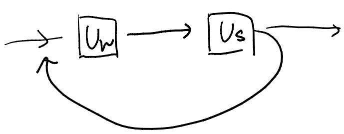
$$|x\rangle|y\rangle \longrightarrow |x\rangle|y \oplus f_w(x)\rangle$$



$$|x\rangle(|0\rangle-|1\rangle) \xrightarrow{U_{f_w}} (-1)^{f_w(x)}|x\rangle(|0\rangle-|1\rangle).$$

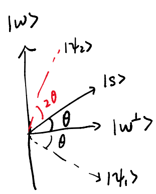
$$U_w|x\rangle = \begin{cases} |x\rangle & \text{if } x \neq w \\ -|x\rangle & \text{if } x = w. \end{cases}$$

$(U_w = I - 2|w\rangle\langle w|) \longleftarrow$ Unitary for Quantum search oracle



$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

$$U_s \overset{def}{=} 2|s\rangle\langle s| - I.$$



2-D subspace spanned by $|w\rangle$, $|s\rangle$.

$\langle s|w\rangle = \sin\theta$, $\langle s|w^\perp\rangle = \cos\theta$

U_w: A reflection along $|w^\perp\rangle$ axis.

$|s\rangle \to |\psi_1\rangle$

U_s: A reflection along $|s\rangle$ axis

$|\psi_1\rangle \to |\psi_2\rangle$

$U_s U_w$: rotation from $\underset{\uparrow \text{initial}}{\underline{|s\rangle}}$ to $|w\rangle$ by 2θ.

Remark: 1) $H^{\otimes n}(2|s\rangle\langle s| - I)H^{\otimes n} = 2|0\rangle\langle 0| - I = \begin{cases} 1 & |x\rangle = 0 \\ -1 & \text{otherwise} \end{cases}$

- U_s : Toffoli

2) Grover Search is optimal.

$$T \geq \frac{\pi}{4}\sqrt{N}(1-\varepsilon)$$

After T rotations,

$$\Rightarrow \angle(|w^\perp\rangle, |\psi_T\rangle) = (2T+1)\theta$$

$$(2T+1)\theta = \frac{\pi}{2} \text{ iff } |\psi_T\rangle = |w\rangle$$

$$T \sim \frac{\pi}{4\theta} = \frac{\pi}{4}\sqrt{N} = O(\sqrt{n})$$ speed up !

3. Quantum Simulation

Simulate k-local Hamiltonian.

$$H = \underset{\uparrow}{\sum_{i\mu}} X_{i\mu}\sigma_{i\mu} + \underset{\uparrow}{\sum_{ij\mu\nu}} X_{i\mu}X_{j\nu}\sigma_{i\mu}\sigma_{j\nu} + \dots$$

$$H = \sum_{i\mu} x_{i\mu}\sigma_{i\mu} + \sum_{ij\mu\nu} x_{i\mu} x_{j\nu}\sigma_{i\mu}\sigma_{j\nu} + \ldots$$

$\uparrow$ 1-local $\qquad\qquad$ $\uparrow$ 2-body interaction

$(\mu, \nu = 1, x, y, z)$.

Theorem: a Quantum Computer can efficiently simulate k-local Hamiltonian

Proof. Trotter decomposition.

$\mathcal{H}_A, \mathcal{H}_B \Rightarrow$ realize $\alpha H_A + \beta H_B + i\gamma [H_A, H_B] \Rightarrow \cdots$

$\hookrightarrow$ Lie Algebra spanned by $H_A, \mathcal{H}_B$.

Cost $\sim \binom{n}{k} \sim n^k$

$\sim \log\left(\frac{1}{\varepsilon}\right)$. ($\varepsilon$ error).

§ 5.4. Quantum Algorithm II.

1. QFT.

FFT: $f(x) \longrightarrow g(y) \overset{\text{def}}{=} \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{2\pi i x y/N} f(x) \qquad O(N \log N)$

QFT: $\sum_x f(x)|x\rangle \longrightarrow \sum_y g(y)|y\rangle$

$$= \sum_y \left(\frac{1}{\sqrt{N}} \sum_x f(x) e^{i2\pi x y/N}\right)|y\rangle$$

$$\Rightarrow \quad |x\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{i2\pi x y/N}|y\rangle.$$

$|x\rangle \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} (-1)^{x\cdot y}|y\rangle. \qquad$ QFT in $\mathbb{Z}_2^{\otimes n}$.

Let $x = x_{n-1} \cdot 2^{n-1} + x_{n-2} 2^{n-2} + \ldots + x_0 = (x_{n-1} x_{n-2} \cdots x_0)_2$.

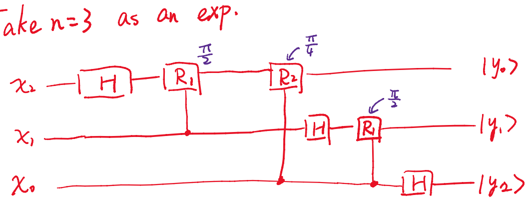
$y = (y_{n-1} y_{n-2} \cdots y_0)_2$, $\qquad$ float: $(.x_0) = \frac{x_0}{2} \quad (.x_1 x_0) = \frac{x_1}{2} + \frac{x_0}{4}$

Fraction part: $\frac{xy}{N} = \frac{xy}{2^n} = y_{n-1}(.x_0) + y_{n-2}(.x_1 x_0) + \ldots + y_0(.x_{n-1} x_{n-2} \cdots x_0)$.

$$|x\rangle \xrightarrow{\text{QFT}} \frac{1}{\sqrt{2^n}} \sum_{y_0, y_1 \cdots y_{n-1}} e^{i2\pi xy/N} |y_{n-1} y_{n-2} \cdots y_0\rangle$$

$$= \frac{1}{\sqrt{2^n}} \underbrace{\left(|0\rangle + e^{i2\pi(.x_0)}|1\rangle\right)}_{y_{n-1}} + \underbrace{\left(|0\rangle + e^{i2\pi(.x_1 x_0)}|1\rangle\right)}_{y_{n-2}} \cdots\cdots \underbrace{\left(|0\rangle + e^{i2\pi(.x_{n-1} x_{n-2} \cdots x_0)}|1\rangle\right)}_{y_0}$$

Take $n=3$ as an exp.



$R_d = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2^d}} \end{pmatrix}$

Total Cost of Q.F.T :

n Hadamard gate. $0+1+\dots+n-1 = \frac{n(n-1)}{2}$ C-Rd gates.

Cost $\sim \frac{n^2}{2}$. poly.

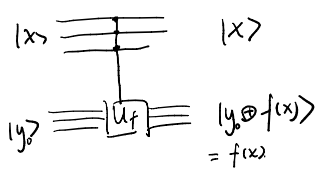
F.F.T cost $N\log N \sim 2^N \cdot n$

exponential speed up!

2. Efficient Period finding with Q.F.T.

Task: $f:\{0,1\}^n \to \{0,1\}^m$. has an unknown period.

$f(x) = f(x+mr) \Rightarrow$ find $\underline{r}$.



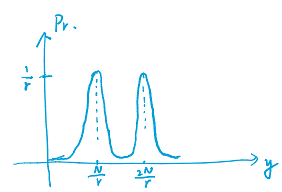
Input $H^{\otimes n}|x\rangle \to \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$

U_f $|\psi_0\rangle = \frac{1}{\sqrt{N}}\sum_x |x\rangle|f(x)\rangle$.

$y_0 = |f(x_0)\rangle$

$$|\psi_x\rangle = \frac{1}{\sqrt{A}}\sum_{j=0}^{A-1}|x_0+jr\rangle \qquad A = \frac{N}{r}$$

$$\xrightarrow{Q.F.T} |\psi_x'\rangle = \frac{1}{\sqrt{NA}}\sum_{y=0}^{N-1} e^{i2\pi x_0 y/N}\sum_{j=0}^{A-1} e^{i2\pi jry/N}|y\rangle$$



Measure in basis $|y\rangle$.

$$\Pr\{y\} = \frac{1}{NA}\left|\sum_{j=0}^{A-1} e^{\frac{2\pi i jry}{N}}\right|^2$$

$\to$ strongly peaked if $\frac{ry}{N} \sim$ integer.

3. Reduction of Factorization to period Finding

$\underline{N}$.

Step: 1) Randomly Choose integer $a < N$.

Suppose $(a, N) = 1$. (easy to find)

2) Construct function $U_f \Leftarrow n^3$.

$f(x) \equiv a^x \pmod N$.

Find period of $f(x)$.

3) Suppose period is r. $\Rightarrow a^r \equiv 1 \pmod N$.

if factorizable

Prob $\geq \frac{1}{2}$ r is even, $(a^{r/2}-1)(a^{r/2}+1) \equiv 0 \pmod N$.

Prob $\geq \frac{1}{2}$ r is even, $(a^{r/2}-1)(a^{r/2}+1) \equiv 0 \pmod N$.

$N \nmid$ one of $a^{\frac{r}{2}}+1$, $a^{r/2}-1$

$\gcd(N, a^{r/2}+1)$ is a factor of N

4. Generalization

1) Q.F.T. $\Leftrightarrow$ Quantum phase estimation.

efficiently solve $\begin{cases} \text{eigenvalues of big matrix} \\ \text{linear equations} \end{cases}$

$$|\psi\rangle = \sum_{i=0}^{2^n-1} a_i |i\rangle$$

2) Generalization of Period-finding

Generalized to any Abelian hidden subgroup.