Quantum Information Processing and Quantum Computation 13/11/2015

Lecture 9: Quantum Search and Grover's Algorithm

Instructor: Goutam Paul *Scribe: Kaushik Nath*

1 Quantum Search

Given a blackbox access to $f : \{0,1\}^n \to \{0,1\}$ find an $x \in \{0,1\}^n$ s.t., $f(x) = 1$, if it exists, otherwise report that no such x exists. Classically, a deterministic algorithm needs to make $\Theta(N)$ queries to solve the problem in the worst case, where $N = 2^n$.

Grover gave a quantum algorithm that solves this problem with $\Theta\left(\sqrt{N}\right)$ queries and this is known to be the best possible. *Grover*'s algorithm can hence speed up quadratically any algorithm that uses searching as a subroutine.

2 Grover's Algorithm

Define the operator Z_0 as

$$\forall x \in \{0,1\}^n, \quad Z_0|x\rangle = \begin{cases} -|x\rangle & \text{if} \quad x = 0^n \\ |x\rangle & \text{otherwise} \end{cases} \tag{1}$$

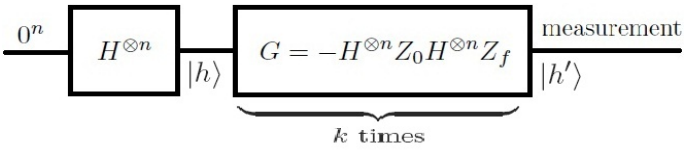

Figure 1: Quantum circuit for *Grover*'s algorithm

It can be easily verified that

$$Z_0 = I_n - 2|0^n\rangle\langle 0^n| \tag{2}$$

where I_n is the $n \times n$ identity matrix. We know that, $f : \{0,1\}^n \to \{0,1\}$, $\exists\ U_f$ s.t, $\forall x \in \{0,1\}^n$, $\forall y \in \{0,1\}$

$$U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle \tag{3}$$

We now derive a special case of equation (3) as given below.

$$\begin{aligned}
U_f|x\rangle(\frac{1}{\sqrt{(2)}}(|0\rangle - |1\rangle)) &= \frac{1}{\sqrt{(2)}}U_f|x\rangle|0\rangle - \frac{1}{\sqrt{(2)}}U_f|x\rangle|1\rangle \\
&= \frac{1}{\sqrt{(2)}}|x\rangle|0 \oplus f(x)\rangle - \frac{1}{\sqrt{(2)}}|x\rangle|1 \oplus f(x)\rangle \\
&= \frac{1}{\sqrt{(2)}}(|x\rangle|f(x)\rangle - |x\rangle|1 \oplus f(x)\rangle) \\
&= \frac{1}{\sqrt{(2)}}(-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle) \\
&= (-1)^{f(x)}|x\rangle\left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right)
\end{aligned}$$

From the above derivation let us define a new operator Z_f as

$$\forall x \in \{0,1\}^n, \quad Z_f|x\rangle = (-1)^{f(x)}|x\rangle \tag{4}$$

Define the sets

$$\begin{aligned}
A &= \{x \in \{0,1\}^n : f(x) = 1\} \\
B &= \{x \in \{0,1\}^n : f(x) = 0\}
\end{aligned}$$

Let $|A| = a$ and $|B| = b$ so that $a + b = 2^n = N$. Now

$$\begin{aligned}
|h\rangle &= \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \\
&= \frac{1}{\sqrt{N}}\left(\sum_{x \in A}|x\rangle + \sum_{x \in B}|x\rangle\right)
\end{aligned}$$

where

$$|A\rangle = \frac{1}{\sqrt{a}}\sum_{x \in A}|x\rangle, \quad |B\rangle = \frac{1}{\sqrt{b}}\sum_{x \in B}|x\rangle$$

Define

$$G = (H^{\otimes n} Z_0 H^{\otimes n})(-Z_f) \tag{5}$$

where $H^{\otimes n} = \underbrace{H \otimes H \otimes \cdots \otimes H}_{n \text{ times}}$. It should be noted that,

$$\begin{aligned}
H^{\otimes n} Z_0 H^{\otimes n} &= H^{\otimes n}(I - 2|0^n\rangle\langle 0^n|)H^{\otimes n} \\
&= H^{\otimes n} I H^{\otimes n} - 2H^{\otimes n}|0^n\rangle\langle 0^n|H^{\otimes n} \\
&= I - 2|h\rangle\langle h|
\end{aligned}$$

Now, if the operator G is applied on $|A\rangle$ and $|B\rangle$, we have

$$\begin{aligned}
G|A\rangle &= (I - 2|h\rangle\langle h|)(-Z_f)|A\rangle \\
&= (I - 2|h\rangle\langle h|)|A\rangle \\
&= |A\rangle - 2\sqrt{\frac{a}{N}}|h\rangle \\
&= |A\rangle - 2\sqrt{\frac{a}{N}}\left(\sqrt{\frac{a}{N}}|A\rangle + \sqrt{\frac{b}{N}}|B\rangle\right) \\
&= \left(1 - \frac{2a}{N}\right)|A\rangle - 2\frac{\sqrt{ab}}{N}|B\rangle
\end{aligned}$$

and

$$\begin{aligned}
G|B\rangle &= (I - 2|h\rangle\langle h|)(-Z_f)|B\rangle \\
&= (I - 2|h\rangle\langle h|)(-|B\rangle) \\
&= 2\sqrt{\frac{b}{N}}|h\rangle - |B\rangle \\
&= 2\sqrt{\frac{b}{N}}\left(\sqrt{\frac{a}{N}}|A\rangle + \sqrt{\frac{b}{N}}|B\rangle\right) - |B\rangle \\
&= 2\frac{\sqrt{ab}}{N}|A\rangle - \left(1 - \frac{2b}{N}\right)|B\rangle
\end{aligned}$$

Let us consider that there is a matrix M_G corresponding to the operator G defined as

$$M_G \begin{pmatrix} \alpha|A\rangle \\ \beta|B\rangle \end{pmatrix} = \begin{pmatrix} \alpha G|A\rangle \\ \beta G|B\rangle \end{pmatrix}$$

where

$$\begin{aligned}
M_G &= \begin{pmatrix} 1 - \frac{2a}{N} & -\frac{2\sqrt{ab}}{N} \\ \frac{2\sqrt{ab}}{N} & -\left(1 - \frac{2b}{N}\right) \end{pmatrix} \\
&= \begin{pmatrix} \frac{b-a}{N} & -\frac{2\sqrt{ab}}{N} \\ \frac{2\sqrt{ab}}{N} & \frac{b-a}{N} \end{pmatrix} \\
&= \begin{pmatrix} \sqrt{\frac{b}{N}} & -\sqrt{\frac{a}{N}} \\ \sqrt{\frac{a}{N}} & \sqrt{\frac{b}{N}} \end{pmatrix} \cdot \begin{pmatrix} \sqrt{\frac{b}{N}} & -\sqrt{\frac{a}{N}} \\ \sqrt{\frac{a}{N}} & \sqrt{\frac{b}{N}} \end{pmatrix} \\
&= \begin{pmatrix} \sqrt{\frac{b}{N}} & -\sqrt{\frac{a}{N}} \\ \sqrt{\frac{a}{N}} & \sqrt{\frac{b}{N}} \end{pmatrix}^2
\end{aligned}$$

We know that

$$\left(\sqrt{\frac{a}{N}}\right)^2 + \left(\sqrt{\frac{b}{N}}\right)^2 = 1 \tag{6}$$

If we let

$$\sqrt{\frac{a}{N}} = \sin\theta, \quad \sqrt{\frac{a}{N}} = \cos\theta$$

then

$$M_G = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^2 = R_\theta^2$$

where R_θ is the matrix for rotation by an angle θ in 2-dimension. So, $|h\rangle$ is rotated by an angle of 2θ by a single application of M_G. Hence, just before measurement we get

$$\begin{aligned} |h'\rangle &= |h\rangle \text{ rotated by angle } 2k\theta \\ &= \sin((2k+1)\theta)|A\rangle + \cos((2k+1)\theta)|B\rangle \end{aligned}$$

where k is the number of time steps. So, the search output is equal to the measurement output and the success probability is equal to $\sin^2((2k+1)\theta)$ ($= P_s$ say). We want P_s to be close to 1, i.e., we want $(2k+1)\theta$ close to $\frac{\pi}{2}$, i.e,

$$k = \frac{1}{2}\left(\frac{\pi}{2} - 1\right) = \frac{\pi}{4\theta} - \frac{1}{2} \tag{7}$$

Now, if θ is small enough, i.e., if a is small enough then

$$\sin\theta \approx \theta \Rightarrow \theta = \sqrt{\frac{a}{N}}$$

Hence, from equation (7) we have

$$k \in \Theta\left(\sqrt{N}\right) = \Theta\left(\sqrt{2^n}\right)$$