CS691Q Topics on Quantum Computing
Grover's Algorithm

Bo Jiang

September 27, 2017

Given a function $f : \{0,1\}^n \to \{0,1\}$, the goal is to find an x with $f(x) = 1$. Let T_b be the set of inputs with f-value b, i.e. $T_b = \{x \in \{0,1\}^n : f(x) = b\}$ for $b \in \{0,1\}$. Let S be the state space of n qubits, and S_b the subspace spanned by the orthonormal vectors in T_b, i.e.

$$S_b = \mathrm{span}\{|x\rangle : x \in T_b\}, \quad b \in \{0,1\}.$$

Note that $S_0 = S_1^\perp$, and each $|y\rangle \in S$ has a unique decomposition $|y\rangle = |y_0\rangle + |y_1\rangle$ with $|y_b\rangle \in S_b$. Suppose a quantum oracle U_f implements f as follows. For the basis vectors,

$$U_f|x\rangle = \begin{cases} -|x\rangle, & \text{if } x \in T_1; \\ |x\rangle, & \text{if } x \in T_0. \end{cases}$$

Thus the unitary operator U_f takes the following form,

$$U_f = \sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle\langle x| = P_{S_0} - P_{S_1},$$

where $P_{S_b} = \sum_{x\in T_b} |x\rangle\langle x|$ is the projection onto the subspace S_b. Note that U_f is the reflection about the subspace S_0.

Let

$$|\psi_b\rangle = \frac{1}{\sqrt{|T_b|}} \sum_{x\in T_b} |x_b\rangle, \quad b \in \{0,1\}.$$

Note that $|\psi_b\rangle \in S_b$, and $|\psi_0\rangle$ and $|\psi_1\rangle$ form an orthonormal basis of a 2-dimensional subspace W of S. Let

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

where $N = 2^n$ and H is the Hadamard gate. Note that

$$|+^n\rangle = \sqrt{\frac{N-M}{N}}|\psi_0\rangle + \sqrt{\frac{M}{N}}|\psi_1\rangle \in W,$$

where $M = |T_1|$ is the number of valid solutions. Consider the unitary operator

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

For any $|y\rangle \in S$ linearly independent of $|+^n\rangle$,

$$V|y\rangle = 2|+^n\rangle\langle +^n|y\rangle - |y\rangle,$$

or

$$\frac{1}{2}(V|y\rangle + |y\rangle) = \langle +^n|y\rangle|+^n\rangle,$$

so V is the reflection about the line spanned by $|+^n\rangle$ in the 2-dimensional plane spanned by $|y\rangle$ and $|+^n\rangle$.

Note that W is invariant under U_f and V, i.e. $U_f W \subset W$ and $VW \subset W$. Indeed, for any vector $|y\rangle = \alpha|\psi_0\rangle + \beta|\psi_1\rangle \in W$,

$$U_f|y\rangle = \alpha|\psi_0\rangle - \beta|\psi_1\rangle \in W,$$

and

$$V|y\rangle = 2\langle +^n|y\rangle|+^n\rangle \ - |y\rangle \in W.$$

Thus we can restrict ourselves to W.

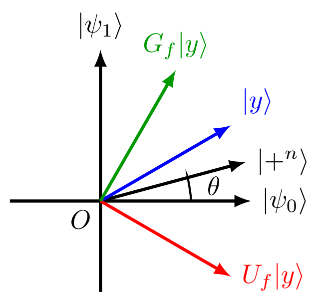

Figure 1: Grover iteration

Let $G_f = VU_f$ and let's see what G_f does to a state $|y\rangle \in W$ (see Figure 1). Use polar coordinates in the plane W and let $\angle|y\rangle$ be the angle of $|y\rangle$ measured from $|\psi_0\rangle$. Recall U_f is the reflection about the subspace S_0, which, when restricted to W, is the reflection about the line $|\psi_0\rangle$. Thus the angle of $U_f|y\rangle$ is $\angle U_f|y\rangle = -\angle|y\rangle$. Similarly, since V is the reflection about $|+^n\rangle$, the angle of $G_f|y\rangle$ satisfies $\angle G_f|y\rangle + \angle U_f|y\rangle = 2\angle|+^n\rangle$. Thus $\angle G_f|y\rangle - \angle|y\rangle = 2\angle|+^n\rangle$ for all $|y\rangle \in W$, which simply means G_f is a rotation by 2θ, where $\theta := \angle|+^n\rangle$. Note that

$$\sin\theta = \langle +^n|\psi_1\rangle = \sqrt{\frac{M}{N}},$$

so

$$\theta = \arcsin\sqrt{\frac{M}{N}}.$$

Starting from the state $|+^n\rangle$, after k iterations, we have $\beta := \angle G_f^k|+^n\rangle = \angle|+^n\rangle + 2k\theta = (2k+1)\theta$, so the resulting state is

$$|\phi\rangle := G_f^k|+^n\rangle = \cos\beta|\psi_0\rangle + \sin\beta|\psi_1\rangle$$

When we measure $|\phi\rangle$ is the standard basis, the probability of getting a valid solution $x \in T_1$ is given by

$$\sum_{x\in T_1} |\langle x|\phi\rangle|^2 = \sum_{x\in T_1} \langle\phi|x\rangle\langle x|\phi\rangle = \langle\phi|P_{S_1}|\phi\rangle = \sin^2\beta.$$

To maximize this probability, we want $\beta \approx \frac{\pi}{2}$, or

$$k \approx \frac{\pi/2}{2\theta} - \frac{1}{2} = \frac{\pi}{4\arcsin\sqrt{\frac{M}{N}}} - \frac{1}{2}.$$

Note that it is *not* true that doing more work (i.e. larger k) is always better, since we may overshoot. When $M \ll N$, $\arcsin\sqrt{\frac{M}{N}} \approx \sqrt{\frac{M}{N}}$, we obtain

$$k \approx \frac{\pi}{4}\sqrt{\frac{N}{M}}.$$

In general, if we know M, we can set

$$k = \left\lfloor \frac{\pi}{4\arcsin\sqrt{\frac{M}{N}}} \right\rfloor \leq \frac{\pi}{4}\sqrt{\frac{N}{M}},$$

where $\lfloor x \rfloor$ is the largest integer no greater than x. Then

$$\left|\beta - \frac{\pi}{2}\right| \leq \min\left\{\theta, \frac{\pi}{4}\right\}.$$

Indeed, if $\theta \in [\frac{\pi}{4}, \frac{\pi}{2}]$, then $k = 0$ and $\beta = \theta$, so $|\beta - \frac{\pi}{2}| \leq \frac{\pi}{4} \leq \theta$. If $\theta \in (0, \frac{\pi}{4}]$, then using $-1 < \lfloor x \rfloor \leq 0$, we obtain $|\beta - \frac{\pi}{2}| \leq \theta \leq \frac{\pi}{4}$. Therefore, the probability of getting a valid solution is

$$\sin^2\beta = \cos^2\left(\beta - \frac{\pi}{2}\right) \geq \max\left\{\cos^2\theta, \cos^2\frac{\pi}{4}\right\} = \max\left\{1 - \frac{M}{N}, \frac{1}{2}\right\} \geq \frac{1}{2}.$$

Repeating the algorithm $\lceil \log_2 \frac{1}{\epsilon} \rceil$ times, we find a solution with probability at least $1 - \epsilon$ if there is one. The number of queries is at most

$$\frac{\pi}{4}\sqrt{\frac{N}{M}}\lceil \log_2 \frac{1}{\epsilon} \rceil.$$

The algorithm is summarized in Algorithm 1.

Algorithm 1 Grover's algorithm with known M

Require: f, M, ϵ

$k \leftarrow \left\lfloor \frac{\pi}{4\arcsin\sqrt{\frac{M}{N}}} \right\rfloor$
for $j = 1, 2, \ldots, \lceil \log_2 \frac{1}{\epsilon} \rceil$ **do**
  $|\phi\rangle \leftarrow H^{\otimes n}|0^n\rangle$
  for $\ell = 1, 2, \ldots, k$ **do**
    $|\phi\rangle \leftarrow G_f|\phi\rangle$ ▷ Grover iteration
  end for
  $x \leftarrow$ measurement result of $|\phi\rangle$ in standard basis
  if $f(x) = 1$ **then**
    return x
  end if
end for

If M is unknown, we run Grover's algorithm with $k = 0, 1, 2, 2^2, \ldots, 2^J$ iterations, where $J = \lfloor \log_2 \sqrt{N} \rfloor$.

If $M \geq N/2$, Grover's algorithm with $k = 0$ finds a solution with probability at least $\frac{1}{2}$. If $1 \leq M < N/2$, let

$$m = \left\lfloor \log_2 \frac{\pi}{4\theta} \right\rfloor .$$

Note that $N^{-1/2} \leq \theta < \frac{\pi}{4}$, so $0 \leq m \leq J$. Grover's algorithm with 2^m iterations finds a solution with probability

$$\sin^2\left[(2^{m+1}+1)\theta\right] \geq \sin^2\left(\frac{\pi}{4}+\theta\right) = \frac{1}{2}\left[1-\cos\left(\frac{\pi}{2}+2\theta\right)\right] = \frac{1}{2}[1+\sin(2\theta)] \geq \frac{1}{2}.$$

Therefore, the above algorithm always finds a solution with probability at least $\frac{1}{2}$ if there is one. The total number of queries is at most

$$\sum_{0\leq j\leq J} 2^j = 2^{J+1} - 1 \leq 2\sqrt{N}.$$

If we run Grover's algorithm for $\lceil \log_2 \frac{1}{\epsilon} \rceil$ times for each k before moving onto the next and terminate whenever a solution is found, then with probability at least $1-\epsilon$, the algorithm finds a solution with the number of queries being at most

$$\lceil \log_2 \frac{1}{\epsilon} \rceil \sum_{0\leq j\leq m} 2^j \leq 2^{m+1} \lceil \log_2 \frac{1}{\epsilon} \rceil \leq \frac{\pi}{2\theta} \lceil \log_2 \frac{1}{\epsilon} \rceil \leq \frac{\pi}{2}\sqrt{\frac{N}{M}} \lceil \log_2 \frac{1}{\epsilon} \rceil.$$

In the worst case where $M = 0$, we have to go through all the iterations, and the number of queries is at most

$$\lceil \log_2 \frac{1}{\epsilon} \rceil \sum_{0\leq j\leq J} 2^j \leq 2\sqrt{N} \lceil \log_2 \frac{1}{\epsilon} \rceil.$$

The algorithm is summarized in Algorithm 2.

Algorithm 2 Grover's algorithm with unknown M

Require: f, ϵ

for $k = 0, 1, 2, 2^2 \ldots, 2^{\lfloor \log_2 \sqrt{N} \rfloor}$ **do**
  for $j = 1, 2, \ldots, \lceil \log_2 \frac{1}{\epsilon} \rceil$ **do**
    $|\phi\rangle \leftarrow H^{\otimes n}|0^n\rangle$
    for $\ell = 1, 2, \ldots, k$ **do**
      $|\phi\rangle \leftarrow G_f|\phi\rangle$ ▷ Grover iteration
    end for
    $x \leftarrow$ measurement result of $|\phi\rangle$ in standard basis
    if $f(x) = 1$ **then**
      return x
    end if
  end for
end for