CS 880: Quantum Information Processing 9/16/10

Lecture 6: Quantum Search

Instructor: Dieter van Melkebeek Scribe: Mark Wellons

In the previous class, we had began to explore Grover's quantum search algorithm. Today, we will illustrate the algorithm and analyze its runtime complexity.

1 Grover's Quantum Search Overview

Grover's algorithm is an excellent example of the potential power of a quantum computer over a classical one, as it can search an unsorted array of elements in $\mathcal{O}(\sqrt{N})$ operations with constant error. A classical computer requires $\Omega(N)$ operations, as it must traverse the entire array in the worst case.

Formally, Grover's algorithm solves the following problem: Given some function $f : \{0,1\}^n \to \{0,1\}$, and possibly the value $t = \left|f^{-1}(1)\right|$. Find any $x \in f^{-1}(1)$.

We begin by entangling all possible inputs so that the state vector looks like

$$|\psi\rangle = \sum \alpha_x |x\rangle \tag{1}$$

where

$$\alpha_x = \frac{1}{\sqrt{2^n}}. \tag{2}$$

For brevity, we will define

$$N \equiv 2^n. \tag{3}$$

If we were to plot the phase of α_x for each $|x\rangle$, it would look as shown in figure 1.

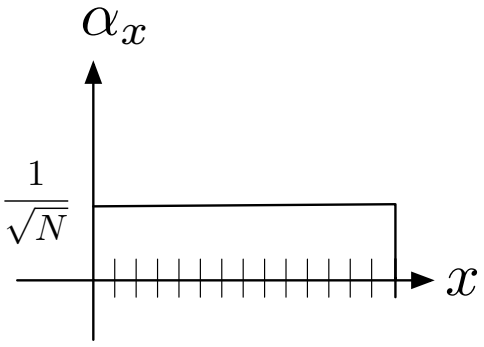


Figure 1: The initial state of the system. Every state is equally likely to be observed if a measurement is taken. We sometimes refer to this state as the *uniform distribution*.

At this point, we introduce a new operator, U_1, which performs a phase kick only on states where $f(x) = 1$ and leaves states where $f(x) = 0$ unchanged. The resulting amplitudes are shown in figure 2. .

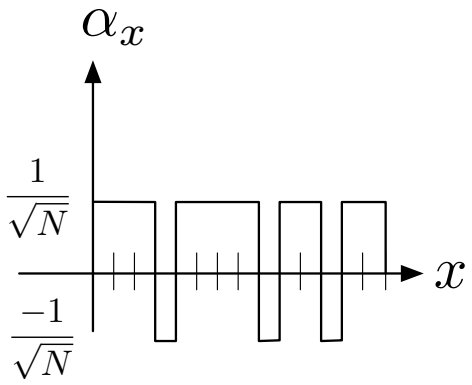


Figure 2: The state of the system after a phase kick on all states where $f(x) = 1$. In this example, there were three states affected, which were reflected across the x-axis.

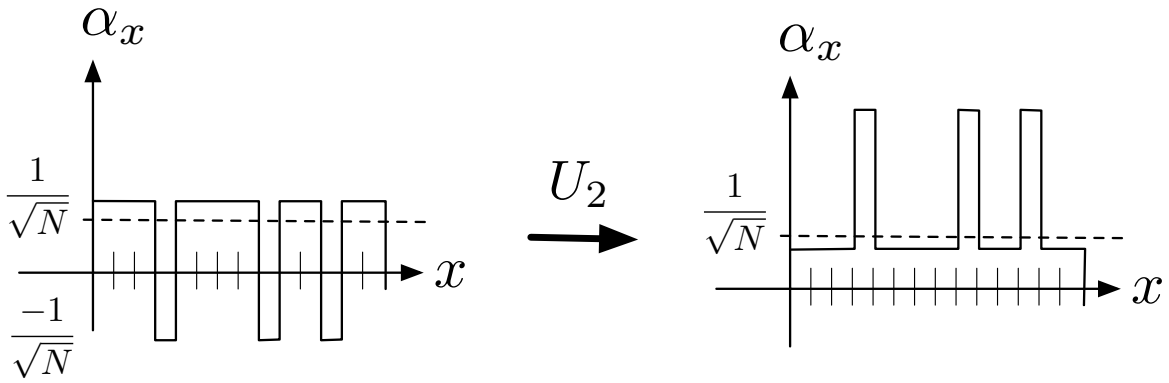


Figure 3: The state of the system after being reflected across the average, which is indicated by a dotted line. Note that the states where $f(x) = 1$ are now much more probable if a measurement is taken.

We also another operator, U_2, which reflects each amplitude across the average value of α_x, as shown in figure 3.

We now repeatably apply U_1 and U_2 until the amplitudes of the desired states vastly exceeds the amplitudes of the other states. We then take a measurement, and with high probability will get some state x such that $f(x) = 1$. Which particular x we get will be uniformly random among the valid states.

2 Unitary Property of U_1 and U_2

We omit the proof that U_1 is unitary as it is simply a phase kick, which was shown to be unitary in a previous lecture.

To show U_2 is unitary, we first show it is linear. To understand how U_2 might be implemented, we note that reflecting around the average is equivalent to subtracting the average, reflecting across

the x-axis, and then adding the average back. In formal notation, we can describe U_2 as

$$U_2 \equiv -\left(|\psi\rangle - AVG(\alpha_x)\sum|x\rangle\right) + AVG(\alpha_x)\sum|x\rangle \tag{4}$$

where

$$AVG(\alpha_x) \equiv \frac{1}{N}\sum \alpha_x. \tag{5}$$

This is clearly linear in a_x, as $AVG(\alpha_x)$ is simply a linear combination of the a_x's and all of the operators are linear.

We finish this proof by showing that all the eigenvalues of U_2 are magnitude 1, a condition required of unitary matrices. First consider what happens when we apply U_2 to the initial state shown in figure 1. Nothing will happen, as the reflection across the average transforms this state to itself. Thus, the uniform distribution is an eigenvector and the eigenvalue is 1.

Now consider the case shown in figure 4. On the left, we have a system where the average is zero, and after applying U_2, we have the system mirrored across the x-axis. Thus this state is another eigenvector and the eigenvalue is -1. In fact, all the eigenvectors orthogonal to the uniform distribution will be states that U_2 simply reflects across the x-axis. Therefore, all eigenvalues are either 1 or -1, as we can consider U_2 to be a reflection across the $\sum_x |x\rangle$axis.

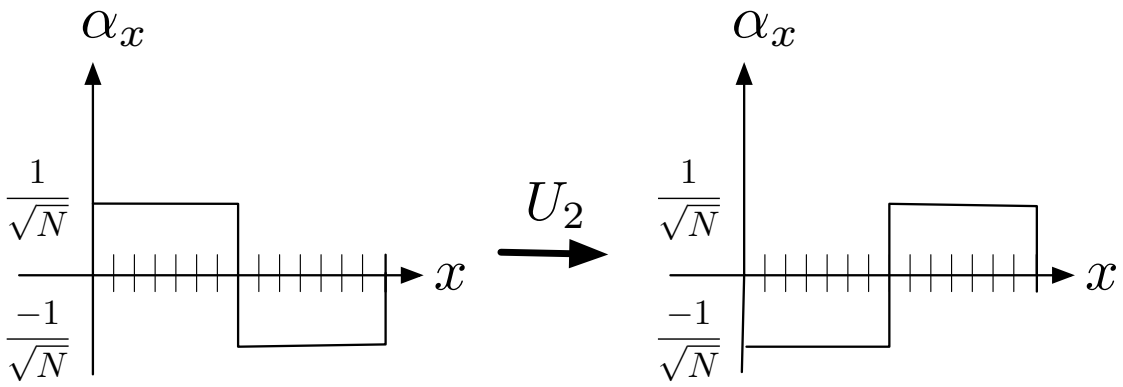
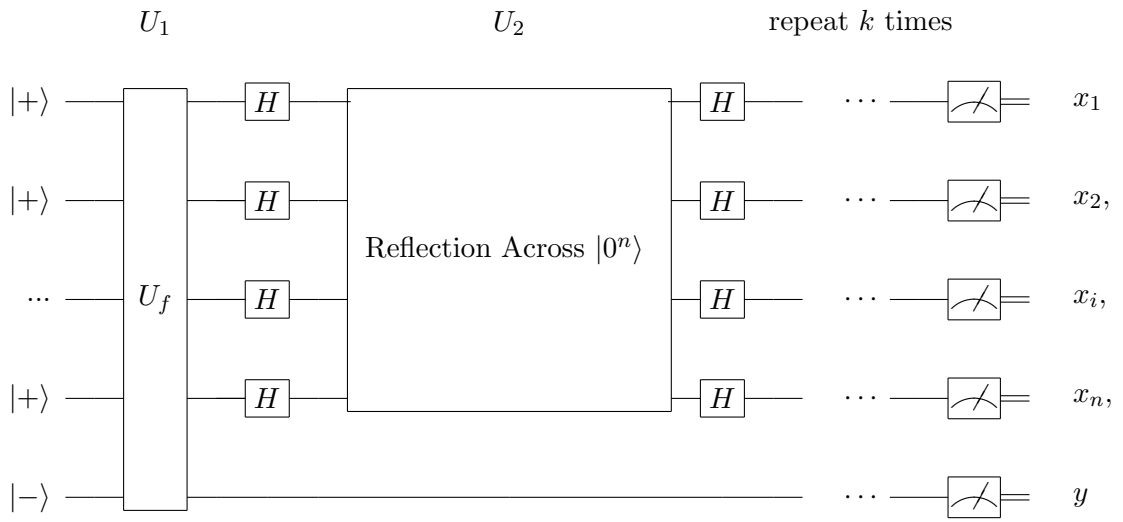


Figure 4: The state of the system before applying U_2 is on the left, and the system afterwards is on the right. As the average is zero, the system is merely reflected across the x-axis.

3 Quantum Circuit

Now we would like to construct the quantum circuit that implements Grover's algorithm. We naturally start with the uniform superposition. Since U_1 is simply a phase kick, it can be implemented by adding an additional $|-\rangle$ qubit as described in previous lectures. To implement U_2, recall that U_2 is reflection along a axis. If this axis was a basis axis, this reflection would be easy to realize. Unfortunately, it is instead some basis determined by the uniform superposition. However, we can change basis via Hadamard gates, which will shift us to the basis state corresponding to the all-zeros vector. Now we simply reflect across this basis state, and then change back to the uniform superposition, and we have implemented U_2. We can repeat U as many times as desired. The full

circuit is shown below.



There are alternatives ways to implement U, but this is adequate for our purposes.

4 Algorithm Complexity

4.1 For a known t

We now seek to determine the optimal value of k, where k is the number of applications of U. Consider that the amplitude α_x of $|x\rangle$ at any point in time depends only whether $f(x) = 0$ or $f(x) = 1$. Since $\alpha_x^{(i)}$ only depends on $f(x)$, we can describe the system state after i iterations of U as

$$\left|\psi^{(i)}\right\rangle = \beta_i \frac{1}{\sqrt{N-t}} \sum_{x:f(x)=0} |x\rangle + \gamma_i \frac{1}{\sqrt{t}} \sum_{x:f(x)=1} |x\rangle\,, \tag{6}$$

where β_i and γ_i are constants and are constrained by

$$\beta_i^2 + \gamma_i^2 = 1. \tag{7}$$

It follows that

$$\begin{aligned} \beta_0 &= \sqrt{\frac{N-t}{N}}, \\ \gamma_0 &= \sqrt{\frac{t}{N}}. \end{aligned}$$

We can thus describe the system as a two-dimensional system with parameters β and γ, where (β, γ) lie on the unit circle, as shown in figure 5. Here we plot β on the B axis and γ on the C axis. This unit circle allows us to generate a new variable θ, which is the angle between the B-axis and the point (β,γ) as measured from the origin. We can describe the initial value of θ as

$$\sin(\theta_0) = \sqrt{\frac{t}{N}}. \tag{8}$$

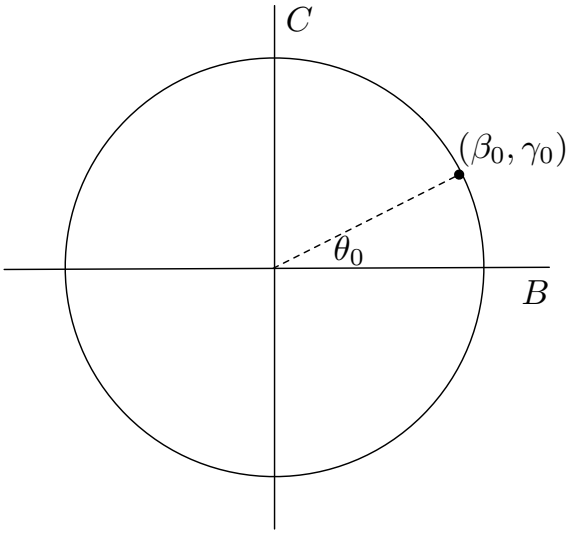


Figure 5: β and γ can be mapped to the unit circle, with β on the B axis and γ on the C axis.

Given some point (β,γ) on this unit circle, what will the effect of the U_1 and U_2 operators be on this point? Since U_1 is a phase kick, it transforms (β,γ) by

$$(\beta, \gamma) \rightarrow (\beta, -\gamma) \tag{9}$$

which is simply a reflection across the B-axis. U_2 reflects the point across the line defined by the origin and the point (β_0,γ_0). Taken together, these two reflections form a rotation of $2\theta_0$. That is, every application of U rotates the point $2\theta_0$ counterclockwise. It follows that after i iterations,

$$\begin{aligned} \theta_i &= (2i+1)\theta_0, \\ \beta_i &= \cos(\theta_i), \\ \gamma_i &= \sin(\theta_i). \end{aligned}$$

From looking at the unit circle, it should be clear that the best time to make a measurement is when (β,γ) is on or very close to the C-axis, as that is when the amplitudes of the valid states is highest. It follows that the ideal value of k would satisfy

$$(2k+1)\theta_0 = \frac{\pi}{2} \tag{10}$$

which leads to

$$k = \frac{1}{2}\left(\frac{\pi}{2\theta_0} - 1\right). \tag{11}$$

This may not be an integer, so we simply choose the closest integer value. We now claim that if we choose a k such that

$$k = \left\lceil \frac{1}{2}\left(\frac{\pi}{2\theta_0} - 1\right) \right\rfloor \tag{12}$$

then

$$\text{Prob}\left[\text{observe } x \in f^{-1}(1)\right] \geq \frac{1}{2}. \tag{13}$$

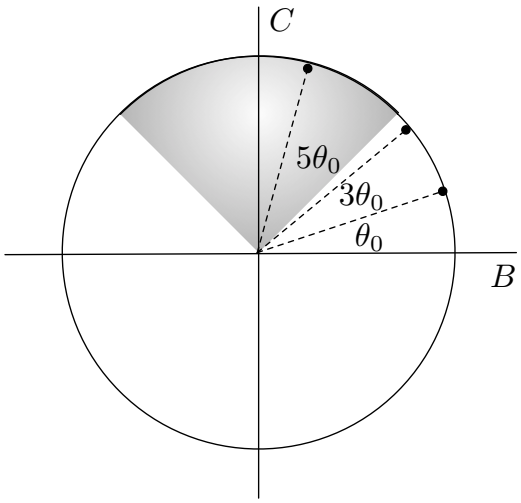


Figure 6: Here is an example where we have applied U three times, which brings us into the shaded part the of unit circle. Each application of U rotates us by $2\theta_0$, and there is no value of $\theta_0 < \pi/2$ that will allow us to completely jump over the shaded area when applying U. Measurements taken in the shaded region have probability $\geq 1/2$ of observing a valid state.

We know this as k must bring us with the top quarter of the unit circle, as shown in figure 6. The advantage of being in the shaded area is that, in terms of absolute value, the amplitudes of the valid states exceed the amplitudes of the invalid states, thus giving us an probability $\geq 1/2$ when taking a measurement.

We can now show that

$$k = \mathcal{O}\left(\sqrt{\frac{N}{t}}\right) \tag{14}$$

for small values of t. Using the small angle approximation we can rewrite equation 8 as

$$\theta_0 \approx \sqrt{\frac{t}{N}}. \tag{15}$$

Which can be substituted into equation (12), giving us equation (14).

4.2 For an unknown t

If t is unknown, there are several things we can try. For now, let us assume that t is positive.

4.2.1 First Attempt

We can try $k = 1$, and then double k with each step until the first success. This algorithm will have some iteration i^* where Prob[success] $\geq 1/2$. This is clearly true, as if we double k every step, then there is no way we can skip the top quarter of the unit circle.

How many times do we use U in the algorithm? As each iteration doubles the number of times U is applied, this is simply the sum of a geometric series. So number of applications of U until iteration i^* is still $\mathcal{O}\left(\sqrt{\frac{N}{t}}\right)$.

However, this algorithm does not quite work, as i^* is only guaranteed to have probability of success $\geq 1/2$. So it is very possible that we will reach i^*, fail the measurement, and then move past i^*. If we move past i^*, the amplitudes of the valid states begin *decreasing*, thus lowering the probability of measuring a valid state. In other words, the problem with this algorithm is we do not know when to stop if we do not get a success.

4.2.2 Second Attempt

In our first attempt, the amplitudes of the valid states were improving until we reached i^*, at which point they declined. In our second attempt, we correct for that by trying to maintain our position in the desirable region. We do that by setting $l = 1$ and doubling l in each iteration, and each time, we pick a k uniformly from random from the set $\{1, 2, 3, ..., l\}$. This has the advantage that if we overstep i^*, there is still a probability of at least $1/2$ that we will pick a point in the good region. It follows that the we expect to overstep i^* by only one iteration.

In any case, the expected number of applications of U is

$$\langle \text{number of } U \rangle = \langle \text{number of } U \text{ up to } i^* \rangle + \langle \text{number of } U \text{ after } i^* \rangle \tag{16}$$

We showed in the first attempt that

$$\langle \text{number of } U \text{ up to } i^* \rangle = \mathcal{O}\left(\sqrt{\frac{N}{t}}\right), \tag{17}$$

which just leaves the us to solve the right term in equation (16). Since the number of applications of U doubles every step, we can express this term as

$$\langle \text{number of } U \text{ after } i^* \rangle \leq \sum_{i>i^*} 2^i \left(\frac{3}{4}\right)^{i-i^*} \tag{18}$$

The $3/4$ arrises from that fact each U has a probability of $1/2$ of being in the good region and points in the good region have $1/2$ probability of being a success. However, this series diverges, as the ratio in our geometric series is greater than 1. This can easily fixed by not doubling between each iteration. Instead, we chose some other factor $\lambda < 4/3$, and now the series converges as shown.

$$\begin{aligned}
\langle \text{number of } U \text{ after } i^* \rangle &\leq \sum_{i>i^*} \lambda^i \left(\frac{3}{4}\right)^{i-i^*}, \\
&\leq \lambda^{i^*} \sum_{i>i^*} \lambda^{i-i^*} \left(\frac{3}{4}\right)^{i-i^*}, \\
&\leq \lambda^{i^*} \sum_{i>0} \lambda^i \left(\frac{3}{4}\right)^{i}.
\end{aligned}$$

What's inside the summation converges, as it is a simple geometric series. We also know λ^{i^*} from equation (17). As we now know both of the terms on the right side of equation (16), it follows that Grover's algorithm runs in $\mathcal{O}\left(\sqrt{\frac{N}{t}}\right)$.