CS 880: Quantum Information Processing 9/27/2010

Lecture 10: Eigenvalue Estimation

Instructor: Dieter van Melkebeek Scribe: Dalibor Zelený

Last time we discussed the quantum Fourier transform, and introduced the problem of phase estimation. Today we conclude the discussion of phase estimation, and apply it to the problem of eigenvalue estimation.

1 Phase Estimation

Recall that in the phase estimation problem, we are given a state ψ of the form

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_x e^{2\pi i \omega x} |x\rangle$$

for some real $0 \leq \omega < 1$. Our goal is to determine the approximate value of ω.

In order to find ω, we apply the inverse Fourier transform to the state $|\psi\rangle$ and observe the system. We interpret the observation as an integer z, and output z/N as our approximation of ω. Define Δ to be the smallest real number d (in terms of absolute value) such that $e^{2\pi i(z/N+d)x} = e^{2\pi i \omega x}$, and note that $|\Delta| \leq 1/2$. We define Δ this way to make some facts easier to state, and to make their proofs simpler.

We saw last time that if $\omega = z/N$ for some integer z, this algorithm finds ω exactly. When ω doesn't have the form z/N for any integer z, we can only approximate ω by outputting a value z/N that's close to ω in the sense that $e^{2\pi i \omega x}$ and $e^{2\pi i (z/N) x}$ are close. The best we can hope to find is a z that minimizes $|\Delta|$, i.e., for which $|\Delta| \leq 1/2N$. The reason we cannot do better is that we only have a limited number (namely n) qubits to work with. We showed last time that

$$F^{-1} |\psi\rangle = \sum_z \alpha_z |z\rangle \quad \text{with} \quad \alpha_z = \frac{1}{N} \cdot \frac{1 - e^{2\pi i \Delta N}}{1 - e^{2\pi i \Delta}}. \tag{1}$$

Unlike in the case where ω has the form z/N, we are not guaranteed that we observe z that minimizes $|\Delta|$. We observe a good z with high probability, as shown in the following claims. We prove the first and the third claim. The proof of the second claim is left as an exercise.

Claim 1. $\Pr[\textit{We observe } z \textit{ that minimizes } |\Delta|] \geq 4/\pi^2$.

Claim 2. $\Pr[\textit{We observe } z \textit{ such that } |\Delta| \leq 1/N] \geq 8/\pi^2$.

Claim 3. $\Pr[\textit{We observe } z \textit{ such that } |\Delta| \geq \delta] \leq O(1/\delta N)$.

Proof of Claim 1. When we observe a z that minimizes Δ, we have $|\Delta| \leq 1/2N$. The probability of observing this z is $|\alpha_z|^2$. We give a lower bound on this probability using (1) and a geometric argument.

We get from (1) that

$$|\alpha_z| = \frac{1}{N} \cdot \frac{|1 - e^{2\pi i \Delta N}|}{|1 - e^{2\pi i \Delta}|}. \tag{2}$$

The numerator in (2) is the distance between points a and b in Figure 1 with $b = e^{2\pi i\Delta N} = e^{i\theta}$, where $-\pi \le \theta \le \pi$. Taking the right triangle formed by the points 0, a, and c, we see that $|b - a| = 2\sin(\theta/2)$. Note that for any $\theta \in [-\pi, \pi]$, we have $|\sin(\theta/2)| \ge |\theta/2|/(\pi/2) = |\theta|/\pi$, so $|1 - e^{2\pi i\Delta N}| = 2|\sin(\theta/2)| \ge 2|\theta|/\pi$. Therefore, $|1 - e^{2\pi i\Delta N}| \ge 2 \cdot (2\pi|\Delta|N)/\pi = 4|\Delta|N$. For the denominator, since the arc between two points is longer than the line segment between those two points, we have $|1 - e^{2\pi i\Delta}| \le 2\pi|\Delta|$. Combining the two yields

$$|\alpha_z| \ge \frac{1}{N} \cdot \frac{4|\Delta|N}{2\pi|\Delta|} = \frac{2}{\pi},$$

so $|\alpha_z|^2 \ge 4/\pi^2$ as we wanted. □

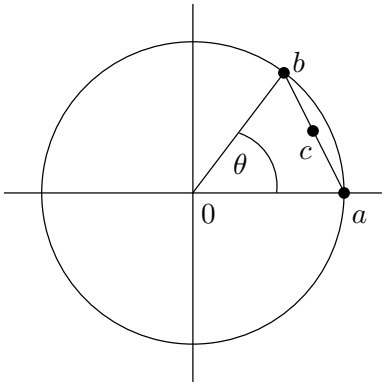

Figure 1: A geometric aid for the proof of Claims 1 and 3. The circle has radius 1, and we have $a = 1$ and $b = e^{i\theta}$. The point c is in the middle of the line segment from a to b.

Exercise 1. *Prove Claim 2.*

Proof of Claim 3. We need an upper bound for $|\alpha_z|$ now. First note that the numerator in (2) is at most 2 because it's the distance between two points on a unit circle. Since $|\Delta| \le 1/2$, we have $|1 - e^{2\pi i\Delta}| = 2|\sin(\pi\Delta)| \ge 2(\pi|\Delta|)/(\pi/2) = 4|\Delta|$, so $|\alpha_z| \le 2/|\Delta|N$, and

$$|\alpha_z|^2 \le (2/\Delta N)^2. \tag{3}$$

We need to sum (3) over all z that cause a large value of Δ. The smallest $|\Delta|$ can be in order to count towards that sum is δ. Since we output integers, the next possible values of $|\Delta|$ are $\delta + 1/N$, $\delta + 2/N$, and so on. Each of those values occurs for two values of z (once in an overestimate and once in an underestimate). The smallest value of $|\Delta|N$ is then δN, and the other possible values

are $\delta N + k$ for positive integers k.

$$\begin{aligned}
\Pr[\text{We observe } z \text{ such that } |\Delta| \geq \delta] &\leq 2 \sum_{k=0}^{\infty} \left(\frac{2}{N\delta + k} \right)^2 \\
&\leq 2 \int_{x=0}^{\infty} \left(\frac{2}{N\delta + x} \right)^2 dx \\
&\leq 2 \int_{x=N\delta}^{\infty} \left(\frac{2}{x} \right)^2 dx \\
&\leq O\left(\frac{1}{N\delta} \right).
\end{aligned}$$

□

2 Eigenvalue Estimation

In eigenvalue estimation, we are given a unitary operator U acting on m qubits and an eigenvector $|\varphi\rangle$ of U. Since $|\varphi\rangle$ is an eigenvector of U, it follows that

$$U |\varphi\rangle = e^{2\pi i \omega} |\varphi\rangle \quad \text{for some } \omega \in [0, 1). \tag{4}$$

Our goal is to estimate the eigenvalue corresponding to $|\varphi\rangle$, which really means we just need a good estimate of ω in (4). As we will see soon, we can use phase estimation to find ω.

Before we can find ω, we need to create a superposition that admits the use of phase estimation, namely something that looks like a Fourier transform. We do so using an idea similar to phase kickback—we inject the eigenvalue into the amplitude.

We apply a controlled U operator to construct the necessary superposition. The new operator, CU, has the following behavior on an eigenvector $|\varphi\rangle$:

$$\begin{aligned}
(CU) |0\rangle |\varphi\rangle &= |0\rangle |\varphi\rangle \\
(CU) |1\rangle |\varphi\rangle &= |1\rangle U |\varphi\rangle = e^{2\pi i \omega} |1\rangle |\varphi\rangle
\end{aligned}$$

Then if we apply CU to the superposition $|+\rangle |\varphi\rangle$, we get

$$(CU) |+\rangle |\varphi\rangle = \frac{|0\rangle + e^{2\pi i \omega} |1\rangle}{\sqrt{2}} |\varphi\rangle .$$

Recall that our goal is to get something that looks like a Fourier transform. To that end, construct $|y_j\rangle$ as follows:

$$|y_j\rangle |\psi\rangle = (CU)^{2^j} |+\rangle |\psi\rangle = \frac{|0\rangle + e^{2\pi i 2^j \omega} |1\rangle}{\sqrt{2}} |\psi\rangle ,$$

so we have

$$|y\rangle |\psi\rangle = \left(\bigotimes_{j=1}^{n} \frac{|0\rangle + e^{2\pi i 2^j \omega} |1\rangle}{\sqrt{2}} \right) |\psi\rangle = \frac{1}{\sqrt{N}} \sum_x e^{2\pi i \omega x} |x\rangle |\psi\rangle . \tag{5}$$

Figure 2 shows the circuit that produces the superposition (5). We construct it as a concatenation of CU gates raised to powers of to from 1 to 2^{n-1}, each controlled by a different qubit in the

$|+\rangle$ state. After that, the n control qubits are in the right superposition for phase estimation, so we apply the inverse Fourier transform to them, make an observation, and get an approximation of ω like we did in phase estimation. Note that the three claims we stated for phase estimation carry over to this setting.

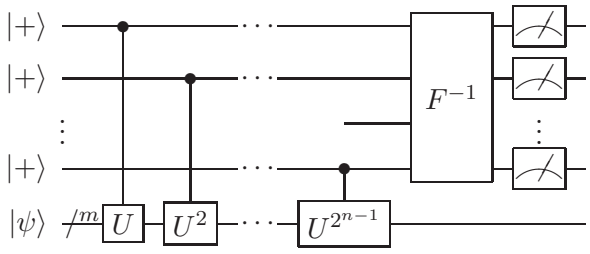

Figure 2: The Eigenvalue Estimation Circuit

We make a few remarks about the circuit in Figure 2. First, this is efficient only if we can construct higher powers of the controlled U gates efficiently. For example, if we only have oracle access to U, we are out of luck and need k consecutive applications of the CU gate to get $(CU)^k$. But even that may be sufficient in some applications, as we will see in the next section.

Second, when we apply eigenvalue estimation, we aren't always going to have access to an eigenvector $|\varphi\rangle$, so let's see what happens when we use some general state $|\psi\rangle$ instead. We can write this state as a linear combination $\sum_j \alpha_j |\varphi_j\rangle$ of eigenvectors of U. After we apply the inverse Fourier transform in Figure 2, the state is $\sum_j \alpha_j |\widetilde{\omega_j}\rangle |\varphi_j\rangle$. With probability $|\alpha_j|^2$, we observe a good approximation of ω_j. Thus, we get an estimation of some eigenvalue out of the algorithm. Whether this is useful or not depends on the application. In the next section we will see some applications where this is useful information.

3 Applications of Eigenvalue Estimation

Eigenvalue estimation has many applications. We list a few here.

- An implementation of Grover's algorithm
- Approximating the Fourier transform over $\mathbb{Z}_N$ for N other than powers of 2
- Solving well-conditioned sparse systems of linear equations
- Order finding and integer factorization
- Computing discrete logarithms

We describe the first application today. We will discuss the other applications in the coming lectures.

3.1 Grover's Algorithm

Recall that in Grover's algorithm, we are given oracle access to $f : \{0,1\}^m \to \{0,1\}$ and our goal is to find an input x such that $f(x) = 1$. During the analysis, we noted that all positive inputs (those where $f(x) = 1$) had the same amplitude, and also that all negative inputs (those where $f(x) = 0$) had the same amplitude. Let t be the number of positive inputs. We defined superpositions $|B\rangle = \frac{1}{\sqrt{M-t}} \sum_{f(x)=0} |x\rangle$ and $|C\rangle = \frac{1}{\sqrt{t}} \sum_{f(x)=1} |x\rangle$ representing all the negative and all the positive inputs, respectively, and viewed the state as a superposition of $|B\rangle$ and $|C\rangle$. The goal of the algorithm was to increase the amplitude of the positive inputs and decrease the amplitude of the negative inputs. We achieved that by describing an operator G and applying it the right number of times. For the analysis, we viewed the B component of our state on the horizontal axis, the C component on the vertical axis, and the state itself as a point on the unit circle. In fact, looking at Figure 1, the state would be at point b and would have an angle of θ with the positive B axis. Applying G had the effect of rotating the state counterclockwise by 2θ.

Exercise 2. *The eigenvalues of G and their corresponding eigenvectors are*

$$\lambda_+ = e^{2i\theta}, \qquad |\varphi_+\rangle = \frac{1}{\sqrt{2}} |B\rangle + \frac{i}{\sqrt{2}} |C\rangle$$
$$\lambda_- = e^{-2i\theta}, \qquad |\varphi_-\rangle = \frac{i}{\sqrt{2}} |B\rangle + \frac{1}{\sqrt{2}} |C\rangle$$

Using the eigenvectors from Exercise 2 above, we can write the state as $|\psi\rangle = \alpha_+ |\varphi_+\rangle + \alpha_- |\varphi_-\rangle$. We apply the eigenvalue estimation algorithm to $|+\rangle^{\otimes n} |\psi\rangle$ to get

$$\alpha_+ \left|\widetilde{2\theta}\right\rangle |\varphi_+\rangle + \alpha_- \left|\widetilde{-2\theta}\right\rangle |\varphi_-\rangle \tag{6}$$

Therefore, we observe a good estimate γ that is within δ of either 2θ or -2θ with probabilities $|\alpha_+|^2$ and $|\alpha_-|^2$, respectively (modulo a loss of a tiny constant factor depending on δ coming from Claim 3). Finally, we approximate the number of positive inputs t by $\tilde{t} = M \cdot \sin^2(\gamma/2)$, which is the same regardless of which of the two angles γ was approximating.

The actual size of the set of positive inputs is t, and we would like to bound the difference $|t - \tilde{t}|$.

$$\begin{aligned}
|t - \tilde{t}| &= M |\sin^2\theta - \sin^2(\gamma/2)| \\
&\leq M \cdot \left(2\sin\theta + \frac{\delta}{2}\right)\frac{\delta}{2} && (7) \\
&\leq \delta\sqrt{tM} + M\frac{\delta^2}{4} && (8) \\
&= O(\sqrt{t}) \quad \left(\text{ for } \delta = \frac{1}{\sqrt{M}}\right) && (9)
\end{aligned}$$

We get (7) by factoring the line above and using the fact that the sine is Lipschitz continuous with the Lipschitz constant less than 1. We get (8) by definition of t. If we pick δ as in (9), we get an estimate of t within an additive factor of $\sqrt{t}$, which is a very good approximation. We need $\sqrt{M}$ applications of G (and thus $\sqrt{M}$ queries to f) to get this accuracy. Then to run Grover's algorithm, we can approximate t with $\tilde{t}$, and then apply G $\tilde{t}$ times to do the search, and make an observation. To do the approximation, we initialize $|\psi\rangle$ in Figure 2 with $|+\rangle^{\otimes m}$, and use the controlled version of G in place of CU.

4 Next Time

Now suppose we observe the bottom m wires in the circuit from Figure 2 instead of the top n wires. The state has the form $\alpha_+ \left|\widetilde{2\theta}\right\rangle |\varphi_+\rangle + \alpha_- \left|\widetilde{-2\theta}\right\rangle |\varphi_-\rangle$, and the two components of the state are almost orthogonal, so they do not interfere with each other too much. Now both $|\varphi_+\rangle$ and $|\varphi_-\rangle$ cause an observation of a positive example with probability 1/2 because they are both uniform superpositions of positive and negative inputs. Then we might as well not use the inverse Fourier transform on the top wires because it has no effect when performing Grover's algorithm. We make this intuition more formal in the next lecture.