CSE 190 / Math 152 - Introduction to Quantum Computing May 28th, 2024

Lecture 15 - Phase Estimation Exercise

Question

Let U be a single-qubit unitary with (unknown) eigenstates $|\psi_+\rangle$ and $|\psi_-\rangle$ with eigenvalues $+1$ and -1, respectively:

$$U|\psi_+\rangle = \quad |\psi_+\rangle$$
$$U|\psi_-\rangle = -|\psi_-\rangle$$

Suppose we can apply controlled-U, but otherwise cannot see the exact matrix representation of U. Design a quantum algorithm which generates an eigenstate of U at random (not necessarily uniformly at random).

Approach

This problem looks similar to the setup of phase estimation, so let's first recall that setting:

Phase Estimation

Setup: Unitary U with eigenstate $|\psi\rangle$ with eigenvalue $e^{2\pi i\theta}$

Input: Unitary $\Lambda_m(U)$ such that

$$\Lambda_m(U)(|k\rangle \otimes |\varphi\rangle) = |k\rangle \otimes U^k |\varphi\rangle$$

for all states $|\varphi\rangle$ and all integers $k \in \{1, 2, \ldots, 2^m - 1\}$ written in binary using m bits.

Output: Approximation $\tilde{\theta}$ of θ with high probability:

$$|\tilde{\theta} - \theta| \leq \frac{1}{2^{m+1}}$$

As a special case, when $\theta = j/2^m$ for some integer $j \in \{0, \ldots, 2^m - 1\}$, the phase estimation circuit outputs j with certainty (hence, can determine eigenvalue exactly).

We need to massage the input of the question to fit the setting of phase estimation.

Claim 1. *Controlled-U is the same operation as $\Lambda_m(U)$ for $m = 1$.*

Proof. Notice that when $m = 1$, we can only use 1 bit to represent the integer k in the definition of $\Lambda_m(U)$. Therefore, there are only two cases to consider $k = 0$ and $k = 1$, which are (conveniently) the same written in binary:

$$\Lambda_1(U)(|0\rangle \otimes |\varphi\rangle) = |0\rangle \otimes |\varphi\rangle$$
$$\Lambda_1(U)(|1\rangle \otimes |\varphi\rangle) = |1\rangle \otimes U|\varphi\rangle$$

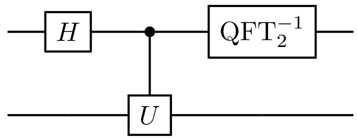
In other words, when $k = 0$, we do nothing, and when $k = 1$ we apply U. This is the exact definition of controlled-U. □

Now let's turn to the representation of the eigenvalues $+1$ and -1 as numbers on the complex unit circle, i.e., $e^{2\pi i\theta}$ for some value of θ. It will turn out that we can represent these numbers with a θ which is exactly $j/2$ for some integer j, so phase estimation is exact.

Claim 2. *$e^{2\pi i(j/2)}$ is 1 when $j = 0$ and -1 when $j = 1$.*

Proof. Follows from the fact that $e^0 = 1$ and $e^{i\pi} = -1$. $\square$

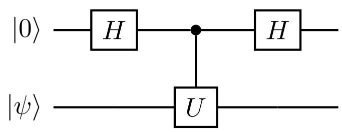
We are ready to apply the phase estimation circuit Q, which looks like the following in the case of $m = 1$:



By the input/output behavior of phase estimation, we have that

$$Q|0\rangle|\psi_+\rangle = |0\rangle|\psi_+\rangle \quad (1)$$
$$Q|0\rangle|\psi_-\rangle = |1\rangle|\psi_-\rangle \quad (2)$$

In other words, when we apply the phase estimation algorithm the first qubit flags whether or not the state of the second register is the $+1$ eigenstate or the -1 eigenstate. It will be useful to be able to do these kinds of calculations using the properties of phase estimation, but for such a simple setting, we can verify these equations explicitly. The key to do so is to recall that QFT_2 is just single-qubit Hadamard, which implies that QFT_2^{-1} is also Hadamard. That is, the circuit for the equations above becomes



where $|\psi\rangle$ is one of $|\psi_+\rangle$ or $|\psi_-\rangle$. For $|\psi_+\rangle$, we get

$$|0\rangle|\psi_+\rangle \xrightarrow{H\otimes I} \frac{|0\rangle|\psi_+\rangle + |1\rangle|\psi_+\rangle}{\sqrt{2}} \xrightarrow{C\text{-}U} \frac{|0\rangle|\psi_+\rangle + |1\rangle U|\psi_+\rangle}{\sqrt{2}} = \frac{|0\rangle|\psi_+\rangle + |1\rangle|\psi_+\rangle}{\sqrt{2}} = |+\rangle|\psi_+\rangle \xrightarrow{H\otimes I} |0\rangle|\psi_+\rangle$$

and for $|\psi_-\rangle$, we get

$$|0\rangle|\psi_-\rangle \xrightarrow{H\otimes I} \frac{|0\rangle|\psi_-\rangle + |1\rangle|\psi_-\rangle}{\sqrt{2}} \xrightarrow{C\text{-}U} \frac{|0\rangle|\psi_-\rangle + |1\rangle U|\psi_-\rangle}{\sqrt{2}} = \frac{|0\rangle|\psi_-\rangle - |1\rangle|\psi_-\rangle}{\sqrt{2}} = |-\rangle|\psi_-\rangle \xrightarrow{H\otimes I} |1\rangle|\psi_-\rangle$$

As expected, these calculations agree with equations (1) and (2) above.

These calculations were done assuming we had access to an eigenstate of U. Clearly, however, we can't use that information since that's what we were supposed to generate in the first place. The trick will be to use the fact that $|\psi_+\rangle$ and $|\psi_-\rangle$ form a basis:

Fact 3. *Let U be an m-qubit unitary with distinct eigenvalues. U has exactly 2^m orthonormal eigenstates $|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_{2^m}\rangle$. Therefore, these eigenstates form a basis for all m-qubit states.*

Using the fact, we can take any state, say $|0\rangle$ and write it in the eigenstate basis:

$$|0\rangle = \alpha|\psi_+\rangle + \beta|\psi_-\rangle$$

where α, β are complex amplitudes. It's worth emphasizing that because we don't know the eigenstates, we also don't know the amplitudes α and β, but that will be okay to solve the problem. Now, when we apply the phase estimation circuit Q using $|0\rangle$ in the usual place of the eigenstate, we get

$$Q|0\rangle|0\rangle = Q|0\rangle(\alpha|\psi_+\rangle + \beta|\psi_-\rangle) = \alpha Q|0\rangle|\psi_+\rangle + \beta Q|0\rangle|\psi_-\rangle = \alpha|0\rangle|\psi_+\rangle + \beta|1\rangle|\psi_-\rangle$$

where in the last line we are once again using equations (1) and (2). To complete the problem, simply measure the first register. We get outcome 0 with probability $|\alpha|^2$ and outcome 1 with probability $|\beta|^2$. Importantly, when we measure 0, the eigenstate $|\psi_+\rangle$ is in the second register, and when we measure 1, the eigenstate $|\psi_-\rangle$ is in the second register. In other words, we have prepared eigenstate $|\psi_+\rangle$ with probability $|\alpha|^2$ and the eigenstate $|\psi_-\rangle$ with probability $|\beta|^2$. To generate, each state uniformly at random we could have started with a random state $|\varphi\rangle$ (from something called the Haar measure) instead of the state $|0\rangle$.