# Chapter 9

# Phase Estimation

In this lecture we will describe Kitaev's phase estimation algorithm, and use it to obtain an alternate derivation of a quantum factoring algorithm. We will also use this technique to design quantum circuits for computing the Quantum Fourier Transform modulo an arbitrary positive integer.

## 9.1 Phase Estimation Technique

In this section, we define the phase estimation problem and describe an efficient quantum circuit for it.

**Property .2** *Let $U$ be a $N \times N$ unitary transformation. $U$ has an orthonormal basis of eigenvectors $|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_N\rangle$ with eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_N$, where $\lambda_j = e^{2\pi i \theta_j}$ for some $\theta_j$.*

Proof: $U$, being unitary, maps unit vectors to unit vectors and hence all the eigenvalues have unit magnitude, i.e. they are of the form $e^{2\pi i \theta}$ for some $\theta$. Let $|\psi_j\rangle$ and $|\psi_k\rangle$ be two distinct eigenvectors with distinct eigenvalues $\lambda_j$ and $\lambda_k$. We have that $\lambda_j \langle \psi_j, \psi_k \rangle = \langle \lambda_j \psi_j, \psi_k \rangle = \langle U\psi_j, \psi_k \rangle = \langle \psi_j, U\psi_k \rangle = \langle \psi_j, \lambda \psi_k \rangle = \lambda_k \langle \psi_j, \psi_k \rangle$. Since $\lambda_j \neq \lambda_k$, the inner product $\langle \psi_j, \psi_k \rangle$ is 0, i.e. the eigenvectors $|\psi_j\rangle$ and $|\psi_k\rangle$ are orthonormal. ∎

Given a unitary transformation $U$, and one of its eigenvector $|\psi_j\rangle$, we want to figure out the corresponding eigenvalue $\lambda_j$ (or, equivalently, $\theta_j$). This is the phase estimation problem.

**Definition .3** *For any unitary transformation $U$, let C-U stand for a "controlled U" circuit which conditionally transforms $|\psi\rangle$ to $U|\psi\rangle$ as shown in Figure **??**.*

Assume that we have a circuit which implements the controlled $U$ transformation (We will see later in the course how to construct a circuit that implements a controlled $U$ transformation given a circuit that implements $U$). The phase estimation circuit in Figure **??** can be used to estimate the value of $\theta$.

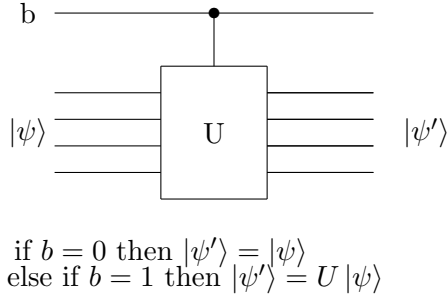The phase estimation circuit performs the following sequence of transformations:

if $b = 0$ then $|\psi'\rangle = |\psi\rangle$
else if $b = 1$ then $|\psi'\rangle = U |\psi\rangle$

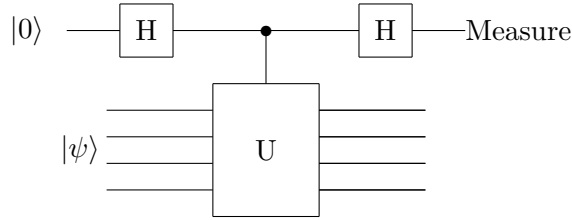Figure 9.1:  Controlled U Circuit



Figure 9.2:  Phase Estimation Circuit

$$
\begin{aligned}
|0\rangle |\psi\rangle \;\; \xrightarrow{H} \quad & \text{s.t. } (|0\rangle + |1\rangle) |\psi\rangle \\
\xrightarrow{C\text{-}U} \quad & \text{s.t. } |0\rangle |\psi\rangle + \text{ s.t. } |1\rangle \lambda |\psi\rangle \\
= \quad & (\text{ s.t. } |0\rangle + \frac{\lambda}{\sqrt{2}} |1\rangle) \otimes |\psi\rangle
\end{aligned}
$$

Note that after the $C$-$U$ transformation, the eigenvector remains unchanged while we have been able to put $\lambda$ into the phase of the first qubit. A Hadamard transform on the first qubit will transform this information into the amplitude which we will be able to measure.

$$
\xrightarrow{H} \quad \frac{1 + \lambda}{\sqrt{2}} |0\rangle + \frac{1 - \lambda}{\sqrt{2}} |1\rangle
$$

Let $P(0)$ and $P(1)$ be the probability of seeing a zero and one respectively on measuring the first qubit. If we write $\lambda = e^{2\pi i\theta}$, we have:

$$
P(0) = \left| \frac{1 + \cos 2\pi\theta + i \sin 2\pi\theta}{\sqrt{2}} \right|^2 = \frac{1 + \cos 2\pi\theta}{2}
$$

$$P(1) = \left| \frac{1 - \cos 2\pi\theta - i \sin 2\pi\theta}{\sqrt{2}} \right|^2 = \frac{1 - \cos 2\pi\theta}{2}$$

There is a bias of $\frac{1}{2}\cos 2\pi\theta$ in the probability of seeing a 0 or 1 upon measurement. Hence, we can hope to estimate $\theta$ by performing the measurement several times. However, to estimate $\cos 2\pi\theta$ within $m$ bits of accuracy, we need to perform $\Omega(2^m)$ measurements. This follows from the fact that estimating the bias of a coin to within $\epsilon$ with probability at least $1 - \delta$ requires $\Theta(\frac{\log(1/\delta)}{\epsilon^2})$ samples.

We will now see how to estimate $\theta$ efficiently. Suppose we can implement the $C_m$-$U$ transformation as defined below.

**Definition .4** *For any unitary transformation $U$, let $C_k$-$U$ stand for a "k-controlled $U$" circuit which implements the transformation $|k\rangle \otimes |\psi\rangle \longrightarrow |k\rangle \otimes U^k |\psi\rangle$ as shown in Figure ??.*
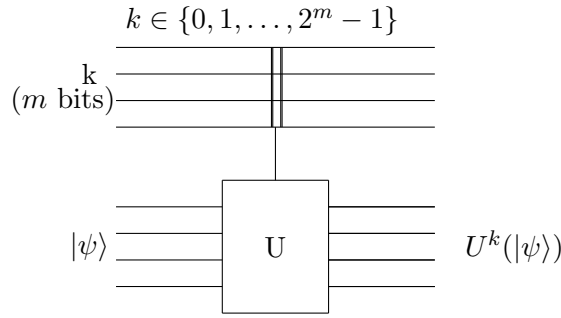


Figure 9.3: m-Controlled U Circuit

Estimating $\theta$ within $m$ bits of accuracy is equivalent to estimating integer $j$, where $\frac{j}{2^m}$ is the closest approximation to $\theta$. Let $M = 2^m$ and $w_M = e^{\frac{2\pi i}{M}}$.
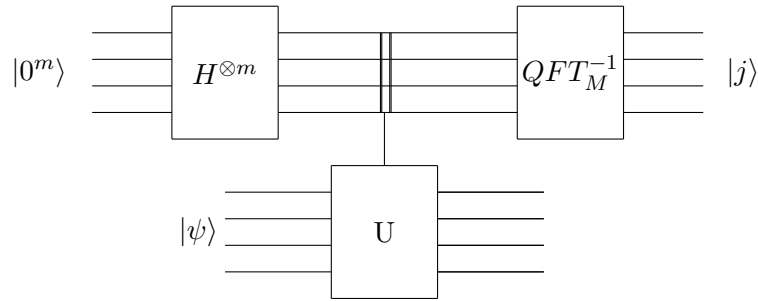


Figure 9.4: Efficient Phase Estimation Circuit

The circuit in Figure **??** performs the following sequence of transformations:

$$|0^m\rangle |\psi\rangle \xrightarrow{H^{\otimes m}} \left( \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} |k\rangle \right) \otimes |\psi\rangle$$

$$\xrightarrow{C_m\text{-}U} \left( \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} \lambda^k |k\rangle \right) \otimes |\psi\rangle$$

$$= \left( \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} \omega_m^{jk} |k\rangle \right) \otimes |\psi\rangle$$

Note that the first register now contains the Fourier Transform mod M of $j$ and if we apply the reverse of the Fourier Transform mod M (note that quantum circuits are reversible), we will get back $j$.

$$\xrightarrow{QFT_M^{-1}} |j\rangle \otimes |\psi\rangle$$

If $\theta = \frac{j}{2^m}$, then clearly the circuit outputs $j$. If $\theta \approx \frac{j}{2^m}$, then the circuit outputs $j$ with high probability (Exercise!).

## 9.2   Kitaev's Factoring Algorithm

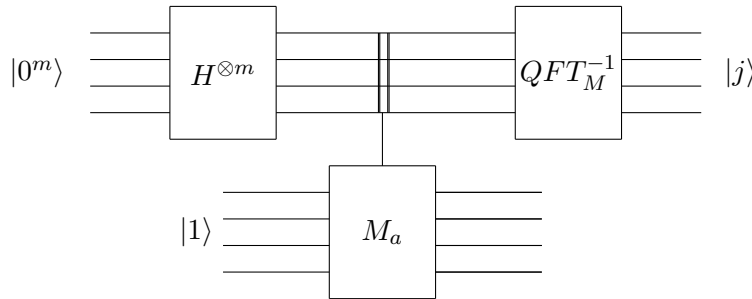In this section, we will see how to use the phase estimation circuit to factor a number.



Figure 9.5: Order Finding Circuit (Kitaev's)

Recall that the problem of factoring reduces to the problem of order finding. To factor $N$, it is sufficient to pick a random number $a$ and compute the minimum positive $r$ such that $a^r \equiv 1$ mod $N$. With reasonable probability, $r$ is even and $a^{r/2} \not\equiv \pm$ mod $N$ and hence $N \mid a^r - 1$, i.e. $N \mid (a^{r/2} + 1)(a^{r/2} - 1)$. Since $N$ does not divide $a^{r/2} \pm 1$, it must be the case that a part of it divides $a^{r/2} + 1$ and hence $gcd(N, a^{r/2} + 1)$ is a non-trivial factor of $N$.

We now reduce the problem of order finding to the phase estimation problem. Consider the unitary transformation $M_a : |x\rangle \rightarrow |xa \bmod N\rangle$. Its eigenvectors are $|\psi_k\rangle = \frac{1}{\sqrt{r}} \left( |1\rangle + \omega^{-k} |a\rangle + \ldots + \omega^{-k(r-1)} |a^{r-1}\rangle \right),$

where $\omega = e^{2\pi i/r}$:

$$
\begin{aligned}
M_a \left|\psi_k\right\rangle &= \frac{1}{\sqrt{r}} \left( \left|a\right\rangle + \omega^{-k}\left|a^2\right\rangle + \ldots + \omega^{-k(r-1)}\left|a^r\right\rangle \right) \\
&= \omega^k \frac{1}{\sqrt{r}} \left( \left|1\right\rangle + \omega^{-k}\left|a\right\rangle + \ldots + \omega^{-k(r-1)}\left|a^{r-1}\right\rangle \right) \\
&= \omega^k \left|\psi_k\right\rangle
\end{aligned}
$$

It follows that $\left|\psi_k\right\rangle$ is an eigenvector of $M_a$ with eigenvalue $\omega^k$. Hence, if we can implement the $C_m$-$M_a$ transformation and construct the eigenvector $\psi_k$ for some suitable $k$, we can use the phase estimation circuit to obtain an approximation to the eigenvalue $w^k$ and therefore reconstruct $r$ as follows: $w^k = e^{2\pi i\theta}$ for $\theta = k/r$. Recall that phase estimation reconstructs $\theta \approx \frac{j}{2^m}$ where $j$ is the output of the phase estimation procedure carried out to $m$ bits of precision. Thus with high probability $\frac{j}{2^m}$ is a very close approximation to $\frac{k}{r}$. Assuming that $k$ is relatively prime to $r$ (which we will ensure with high probability) we can estimate $r$ using the method of continued fractions if we choose $M \approx N^2$.

Lets look carefully at the $C_m$-$M_a$ transformation. It transforms $\left|k\right\rangle\left|x\right\rangle \rightarrow \left|xa^k \bmod N\right\rangle$. But this is precisely the transformation that does modular exponentiation. There exists a classical circuit that performs this transformation in $O(|x|^2|k|)$ time, and thus we can construct a quantum circuit that implements the $C_m$-$M_a$ transformation.

It is not obvious how to obtain an eigenvector $\left|\psi_k\right\rangle$ for some $k$, but it is easy to obtain the uniform superposition of the eigenvectors $\left|\psi_0\right\rangle, \left|\psi_1\right\rangle \ldots \left|\psi_{r-1}\right\rangle$. Note that $\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \left|\psi_k\right\rangle = \left|1\right\rangle$. Hence, if we use $\left|1\right\rangle$ as the second input to the phase estimation circuit, then we will be able to measure a random eigenvalue $w^k$, where $k$ is chosen u.a.r. from the set $\{0, \ldots, r-1\}$. Note that $k = 0$ is completely useless for our purposes. But $k$ will be relatively prime to $r$ with reasonable probability.

With these observations, it is easy to see that the circuit in Figure ?? outputs $\left|j\right\rangle$ with high probability, where $\frac{j}{2^m}$ is the closest approximation to $\frac{k}{r}$ for some random $k$. Note that with reasonable probability, $k$ is relatively prime to $r$ and if that be the case, then we can estimate $r$ using the method of continued fractions if we choose $M \approx N^2$.

Though the thinking and the analysis behind the Kitaev's and Shor's order-finding algorithm are different, it is interesting to note that the two circuits are almost identical. Figure ?? describes the Shor's circuit with $QFT_Q$ transformation replaced by $H^{\otimes q}$ since both act in an identical manner on $\left|0^q\right\rangle$. The quantities $q$, $Q$ and $x$ in the Shor's algorithm correspond to $m$, $M$ and $a$ in the Kitaev's algorithm. Also, note that raising $a$ to some power is same as performing controlled multiplication.

## 9.3   QFT mod Q

In this section, we will present Kitaev's quantum circuit for computing Fourier Transform over an arbitrary positive integer $Q$, not necessarily a power of 2. Let $m$ be such that $2^{m-1} < Q \leq 2^m$ and let $M = 2^m$.
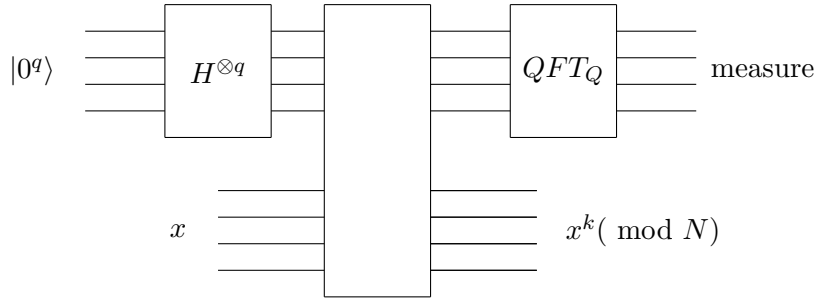
Figure 9.6: Order Finding Circuit (Shor's)

Recall that the Fourier Transform mod $Q$ sends

$$|a \bmod Q\rangle \longrightarrow \frac{1}{\sqrt{Q}} \sum_{b=0}^{Q-1} \omega^{ab} |b\rangle \stackrel{\text{let}}{=} |\chi_a\rangle$$

where $\omega = e^{2\pi i/Q}$. Note that $\{|\chi_a\rangle \mid a = 0, 1, \ldots, Q-1\}$ forms an orthonormal basis, so we may regard the Fourier Transform as a change of basis.

Consider the following sequence of transformations, which computes something close to the Fourier Transform mod $Q$:

$$|a\rangle |0\rangle \longrightarrow |a\rangle \otimes \frac{1}{\sqrt{Q}} \sum_{b=0}^{Q-1} |b\rangle \longrightarrow |a\rangle \otimes \frac{1}{\sqrt{Q}} \sum_{b=0}^{Q-1} \omega^{ab} |b\rangle = |a\rangle \otimes |\chi_a\rangle$$

We can implement the circuit that sends $|0\rangle \longrightarrow \frac{1}{\sqrt{Q}} \sum_{b=0}^{Q-1} |b\rangle$ efficiently in the following two ways:

1. Perform the following sequence of transformations.

$$|0\rangle^m \otimes |0\rangle \xrightarrow{H^{\otimes m}} \frac{1}{M} \sum_{x=0}^{2^m-1} |x\rangle |0\rangle \xrightarrow{x \geq Q} \frac{1}{M} \sum_{x=0}^{2^m-1} |x\rangle |x \geq Q\rangle$$

   Note that since we can efficiently decide whether or not $x \geq Q$ classically, we can also do so quantum mechanically. Now take measurement on the second register. If the result is a 0, the first register contains a uniform superposition over $|0\rangle, \ldots, |Q-1\rangle$. If not, we repeat the experiment. At each trial, we succeed with probability $Q/M > 2^{m-1}/2^m = 1/2$.

2. If we pick a number u.a.r. in the range 0 to $Q-1$, the most significant bit of the number is 0 with probability $2^{m-1}/Q$. We can therefore set the first bit of our output to be the

superposition:

$$\sqrt{\frac{2^{m-1}}{Q}}\,|0\rangle + \sqrt{1 - \frac{2^{m-1}}{Q}}\,|1\rangle$$

If the first bit is 0, then the remaining $m-1$ bits may be chosen randomly and independently, which correspond to the output of $H^{\otimes m-1}$ on $|0^{m-1}\rangle$. If the first bit is 1, we need to pick the remaining $m-1$ bits to correspond to a uniformly chosen random number between 0 and $Q - 2^{m-1}$, which we can do recursively.

The second transformation $|a\rangle\,|b\rangle \to \omega^{ab}\,|a\rangle\,|b\rangle$ can be made using the controlled phase shift circuit.

This gives us an efficient quantum circuit for $|a\rangle\,|0\rangle \to |a\rangle\,|\chi_a\rangle$, but what we really want is a circuit for $|a\rangle \to |\chi_a\rangle$. In particular, for application to factoring, we need a circuit that "forgets" the input $a$ in order to have interference in the superposition over $|\chi_a\rangle$.

What we would like is a quantum circuit that transforms $|a\rangle\,|\chi_a\rangle \to |0\rangle\,|\chi_a\rangle$. If we could find a unitary transformation $U$ with eigenvector $|\chi_a\rangle$ and eigenvalue $e^{2\pi i a/Q}$, then we could use phase estimation to implement the transformation $|0\rangle\,|\chi_a\rangle \to |a\rangle\,|\chi_a\rangle$. By reversing the quantum circuit for phase estimation (which we could do since quantum circuits are reversible), we have an efficient quantum circuit for

$$|a\rangle\,|0\rangle \to |a\rangle\,|\chi_a\rangle \to |0\rangle\,|\chi_a\rangle$$

which is what we need. Note that the phase estimation circuit with $m$ bits of precision outputs $j$ such that $\frac{j}{2^m} \approx \frac{a}{Q}$. So if we take $2^m >> Q^2$, we can use continued fractions to reconstruct $a$ as required above.

To see that the required $U$ exists, consider $U : |x\rangle \to |x - 1 \bmod Q\rangle$. Then,

$$U(\chi_a) = U\left(\sum_{b=0}^{Q-1} \omega^{ab}\,|b\rangle\right) = \sum_{b=0}^{Q-1} \omega^{ab}\,|b-1\rangle = \omega^a \sum_{b=1}^{Q} \omega^{a(b-1)}\,|b-1\rangle = \omega^a \chi_a.$$

In addition, note that $U^k$ can be efficiently computed with a classical circuit, and can therefore be both efficiently and reversibly computed with a quantum circuit. The overall circuit to compute $QFT$ mod $Q$ is shown in Figure ?? (The circuit should be read from right to left).
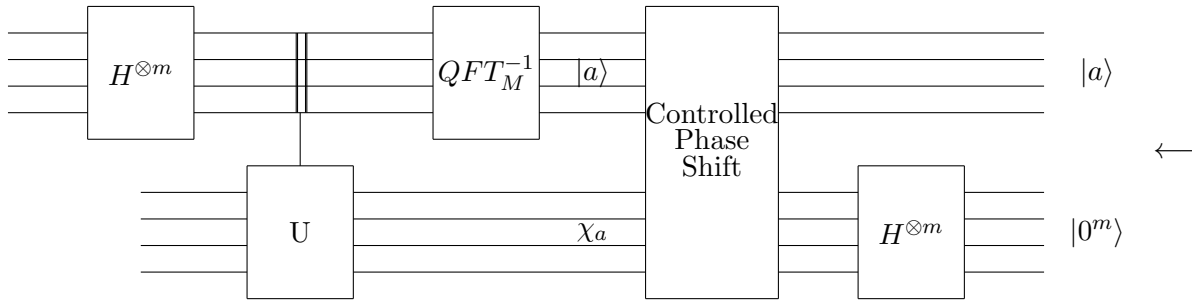
Figure 9.7: Using Reverse Phase Estimation Circuit to do QFT mod Q for arbitrary Q