CS 599 P1: Introduction to Quantum Computation — Boston University, Fall 2025
Instructor: Alexander Poremba — **Scribe:** Yiding Zhang

LECTURE # 11: QUANTUM PHASE ESTIMATION

In this lecture, we will encounter the *Quantum Phase Estimation* (QPE) algorithm: this is a fundamental algorithmic primitive which is used to determine the eigenvalues (or "phases") associated with the eigenvectors of a unitary operator. QPE shows up as an important subroutine in many powerful quantum algorithms, such as Shor's factoring algorithm or in the context of quantum simulation, where one wishes to to estimate the energy of a quantum mechanical system efficiently.

1 Background: Linear Algebra

In this section, we review some basic notions from linear algebra that will be used later. We first recall the definitions of *eigenvalues* and *eigenvectors*.

Definition 1.1 (Eigenvalues and eigenvectors)**.** *Let $M \in \mathbb{C}^{N\times N}$ be a matrix and $|\psi\rangle \in \mathbb{C}^N$ be a vector. We say $|\psi\rangle$ is an* eigenvector *of M with* eigenvalue $\lambda \in \mathbb{C}$ *if it holds that*

$$M|\psi\rangle = \lambda|\psi\rangle\,.$$

Example: Eigenvalues and eigenvectors of the Pauli operators.

Below, we recall the eigenvectors and eigenvalues of the Pauli operators Z and X:

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|, \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = |+\rangle\langle +| - |-\rangle\langle -|.$$

Operator	Eigenvector(s)	Eigenvalue(s)
Z	$Z\|0\rangle = +\|0\rangle$	$\lambda_0 = +1$
	$Z\|1\rangle = -\|1\rangle$	$\lambda_1 = -1$
X	$X\|+\rangle = +\|+\rangle$	$\lambda_+ = +1$
	$X\|-\rangle = -\|-\rangle$	$\lambda_- = -1$

The definitions of eigenvalues and eigenvectors lead to the following question:

Question: *When can a matrix be diagonalized via an orthonormal basis of its eigenvectors?*

To answer this question, we introduce the notion of *normal matrices*.

Definition 1.2 (Normal matrices)**.** *Let $M \in \mathbb{C}^{N\times N}$ be a matrix. We say that M is* normal *if*

$$MM^\dagger = M^\dagger M$$

Here are some special cases of normal matrices.

- **Unitary matrices**. A unitary matrix $U \in \mathbb{C}^{N\times N}$ satisfies $UU^\dagger = U^\dagger U = I$.
- **Hermitian matrices**. A Hermitian matrix $H \in \mathbb{C}^{N\times N}$ satisfies $H^\dagger = H$.

The following well-known spectral theorem from linear algebra tells us that any normal matrix can be diagonalized via an orthonormal basis of its eigenvectors.

Theorem (Spectral theorem)

Let $M \in \mathbb{C}^{N\times N}$ be any normal matrix. Then, there exists a set of complex numbers $\{\lambda_i\}_{i=0}^{N-1}$ and a set of normalized and orthogonal N-dimensional vectors $\{|\psi_i\rangle\}_{i=0}^{N-1}$, as well as a

- change of basis $U \in \mathbb{C}^{N\times N}$ with
$$U = \sum_{i=0}^{N-1} |\psi_i\rangle\langle e_i|$$
- and a diagonal matrix $D = \mathsf{diag}(\lambda_0, \lambda_1, \ldots, \lambda_{N-1})$ with
$$D = \sum_{i=0}^{N-1} \lambda_i \, |e_i\rangle\langle e_i|$$

such that the matrix M admits a decomposition

$$M = UDU^\dagger = \sum_{i=0}^{N-1} \lambda_i \, U \, |e_i\rangle\langle e_i| \, U^\dagger = \sum_{i=0}^{N-1} \lambda_i \, |\psi_i\rangle\langle\psi_i| \,,$$

where $\{\lambda_i\}_{i=0}^{N-1}$ are the eigenvalues of M and $\{|\psi_i\rangle\}_{i=0}^{N-1}$ are the eigenvectors of M which form an orthonormal basis of $\mathbb{C}^N$.

Now that we reviewed the spectral theorem, it is useful to re-visit the Pauli X and Z matrices from before. The Pauli Z and X operators are *normal* and admit the following spectral decompositions:

Operator	Change of basis U	Diagonal D
Z	$U = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$D = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
X	$U = H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$	$D = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

We can represent each of the matrices as a diagonal matrix conjugated by a unitary change of basis:

$$Z = I \cdot \mathsf{diag}(1, -1) \cdot I, \qquad X = H \cdot \mathsf{diag}(1, -1) \cdot H.$$

Another illustrative example is the spectral theorem for *unitary matrices*. For any unitary $U \in \mathbb{C}^{N\times N}$ (which is a special case of a normal matrix), we have the property that each eigenvalue can be written as

$\lambda_j = e^{2\pi i\theta_j}$ for some $\theta_j \in [0,1)$, i.e., U can be decomposed as

$$U = \sum_{j=0}^{N-1} \lambda_j |\psi_j\rangle \langle\psi_j| = \sum_{j=0}^{N-1} e^{2\pi i\theta_j} |\psi_j\rangle \langle\psi_j| .$$

The proof is left as an exercise in Homework 3.

2 Quantum Phase Estimation

Given a unitary U (say, which is specified by a quantum circuit) and some eigenvector $|\psi\rangle$ of U, one might wonder whether we can algorithmically compute the value of $\theta \in [0,1)$ such that

$$U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$$

By the spectral theorem and the fact thar U is unitary, we know that such a θ always exist. This question motivates the problem of phase estimation, which is defined as follows.

Problem (Phase estimation)

- **Input**: A description of a quantum circuit for a unitary $U \in \mathbb{C}^{2^n \times 2^n}$ and an n-qubit state $|\psi\rangle$.
- **Promise**: $|\psi\rangle$ is an eigenvector of U.
- **Output**: An approximation $\tilde{\theta}$ such that $\tilde{\theta} \approx \theta$ where $U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$.

Note that we cannot solve this problem directly as a classical linear algebra problem: the matrix U has dimension 2^n, which is exponentially large (and the quantum circuit is a succinct description of U).

The controlled-U operation. The quantum phase estimation problem may at first sight look impossible to solve because the value $e^{2\pi i\theta}$ looks like a global phase. However, we can easily apply so-called *controlled-U* operations such that $e^{2\pi i\theta}$ becomes a relative phase.

For any unitary U, we can define the corresponding controlled unitary operation

$$\text{controlled-}U = (|0\rangle\langle 0| \otimes I) + (|1\rangle\langle 1| \otimes U)$$

In quantum circuit notation, we can visualize the U and controlled-U operations via

Figure 1: U and controlled-U

To implement controlled-U given a circuit description U, we can simply add control wires to all the gates in U. Then we can apply the following quantum circuit.

The computation proceeds as follows.

- We start from the state $|\psi_0\rangle = |0\rangle|\psi\rangle$;

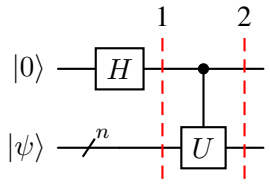

Figure 2: A quantum circuit that encodes $e^{2\pi i\theta}$ as a relative phase

- In Step 1, we get $|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle\,|\psi\rangle + |1\rangle\,|\psi\rangle)$;
- In Step 2, we get

$$\begin{aligned}|\psi_2\rangle &= \frac{1}{\sqrt{2}}(|0\rangle\,|\psi\rangle + |1\rangle\,(U\,|\psi\rangle)) \\ &= \frac{1}{\sqrt{2}}(|0\rangle\,|\psi\rangle + e^{2\pi i\theta}\,|1\rangle\,|\psi\rangle) \\ &= \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i\theta}\,|1\rangle)\,|\psi\rangle\,.\end{aligned}$$

As we can see, the value $e^{2\pi i\theta}$ now becomes a relative phase, which is detectable. But how exactly can we realize a quantum measurement which approximately reveals the value θ to us?

Extracting the value of θ. Now the only problem left is how to extract the value $\theta \in [0, 1)$ from the relative phase. For simplicity, we assume that θ has t digits under the binary expansion[1], i.e.,

$$\theta = 0.\theta_1\theta_2\ldots\theta_t = \sum_{j=1}^{t} \theta_j \cdot 2^{-j}.$$

Therefore, we only need t qubits to store the outcome.

The key idea behind QPE is that exctracting θ via a measurement is possible if we can algorithmically prepare a $\mathbb{Z}_{2^t}$-Fourier transform of the integer $2^t\theta$, which is given by

$$\begin{aligned}\mathsf{QFT}_{\mathbb{Z}_{2^t}}\,|2^t\theta\rangle &= \frac{1}{\sqrt{2^t}} \sum_{x\in\mathbb{Z}_{2^t}} e^{2\pi i\theta x}\,|x\rangle \\ &= \bigotimes_{j=1}^{t} \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(0.\theta_{t-j+1}\theta_{t-j+2}\ldots\theta_t)}\,|1\rangle\right).\end{aligned}$$

Notice the similarity to the previous lecture on the quantum Fourier transform. Crucially, if we can manage to prepare this state, then we are essentially done; we can simply perform the inverse quantum Fourier transform $\mathsf{QFT}^\dagger_{\mathbb{Z}_{2^t}}$, and measure in the computational basis.

Recall that the inverse quantum Fourier transform is given by the unitary operator

$$\mathsf{QFT}^\dagger_{\mathbb{Z}_{2^t}} = \sum_{x,y\in\mathbb{Z}_{2^t}} \omega_{2^t}^{-x\cdot y}\,|y\rangle\,\langle x|$$

[1]In general, θ may contain many digits; by choosing t large enough, the truncated binary expansion allows us to get a good approximation $\tilde{\theta} \approx \theta$ which only incurs a small error. For simplicity, we only consider the exact QPE algorithm in this lecture.

In other words, the inverse quantum Fourier transform is the same operator as the standard quantum Fourier transform but with an additional minus sign in the phase.

Quantum phase estimation algorithm. Below in Figure 3 is the full quantum circuit for the quantum phase estimation algorithm, where for simplicity we assume that θ can be specified with t bits of precision.

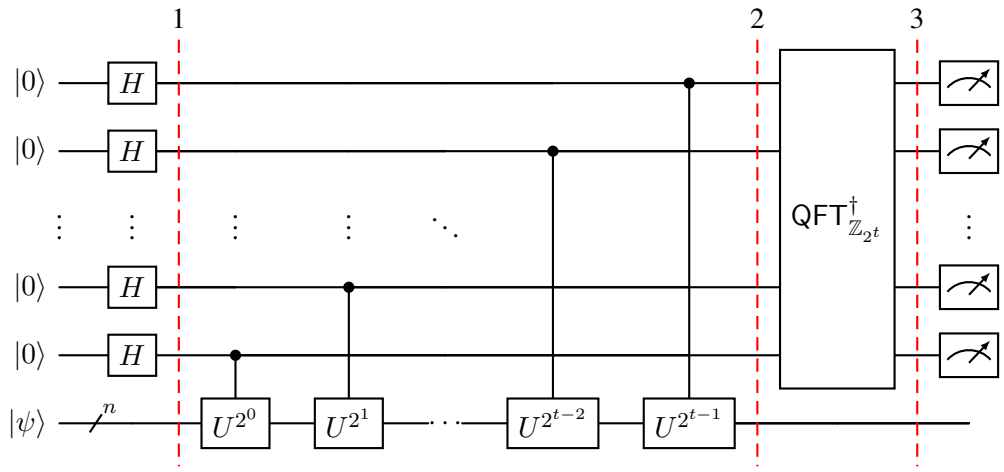

Figure 3: Quantum phase estimation

The computation proceeds as follows.

- We start from the state $|0\rangle^{\otimes t}|\psi\rangle$;
- In Step 1, we apply the Hadamard gates and get

$$|\psi_1\rangle = \frac{1}{\sqrt{2^t}} \sum_{x\in\mathbb{Z}_{2^t}} |x\rangle |\psi\rangle ;$$

- In Step 2, we apply controlled-U^x operation for each $x \in \mathbb{Z}_{2^t}$ and get

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{\sqrt{2^t}} \sum_{x\in\mathbb{Z}_{2^t}} |x\rangle \left(U^x |\psi\rangle\right) \\ &= \frac{1}{\sqrt{2^t}} \sum_{x\in\mathbb{Z}_{2^t}} e^{2\pi i\theta x} |x\rangle |\psi\rangle \\ &= \left(\mathsf{QFT}_{\mathbb{Z}_{2^t}} |2^t\theta\rangle\right) \otimes |\psi\rangle ; \end{aligned}$$

  In the second line, we used the promise that $|\psi\rangle$ is an eigenvector of U.

- In Step 3, we apply $\mathrm{QFT}^\dagger_{\mathbb{Z}_{2^t}}$ to the first t qubits and get $|2^t\theta\rangle|\psi\rangle$.
- After measuring the first t qubits, we get the value of $2^t\theta$, from which we can recover $\theta \in [0, 1)$.