COL7160 : Quantum Computing

Lecture 11: Phase Estimation Problem

Instructor: Rajendra Kumar **Scribe:** Ansh Agrawal

1 Phase Estimation Preliminaries

1.1 Normal Matrices

Definition 1 (Normal matrix)**.** Let $M \in \mathbf{C}^{N\times N}$. We say that M is *normal* if it commutes with its adjoint:

$$MM^\dagger \;=\; M^\dagger M.$$

1.1.1 Spectral Decomposition

Normal matrices admit an especially clean eigen-decomposition.

Theorem 2 (Spectral decomposition of a normal matrix)**.** *If $M \in \mathbf{C}^{N\times N}$ is normal, then there exists an orthonormal basis of eigenvectors $\{|\psi_1\rangle, \ldots, |\psi_N\rangle\}$ with corresponding eigenvalues $\lambda_1, \ldots, \lambda_N \in \mathbf{C}$ such that*

$$M \;=\; \sum_{j=1}^{N} \lambda_j \; |\psi_j\rangle \langle\psi_j| \,.$$

Each term $|\psi_j\rangle\langle\psi_j|$ is a rank-1 projector onto the span of $|\psi_j\rangle$. where we define $|\psi_j\rangle$, λ_j as :

$$M\,|\psi_j\rangle \;=\; \lambda_j\,|\psi_j\rangle \,.$$

Here $|\psi_j\rangle$ denotes an eigenvector and λ_j denotes its eigenvalue.

1.2 Unitary Matrices

Unitary matrices by definition are normal matrices. A matrix $U \in \mathbf{C}^{N\times N}$ is *unitary* if

$$UU^\dagger \;=\; U^\dagger U \;=\; I.$$

Example 3 (The identity matrix)**.** The identity matrix is unitary and has many spectral decompositions.

1.2.1 Two spectral decompositions for I

1. **Computational basis:**

$$I \;=\; |0\rangle\langle 0| \;+\; |1\rangle\langle 1| \,.$$

2. **Hadamard basis:**

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Then

$$I \;=\; |+\rangle\langle +| \;+\; |-\rangle\langle -| \,.$$

If eigenvalues are degenerate (repeated), the spectral decomposition is not unique. For I, *any* orthonormal basis is an eigenbasis, hence many decompositions are possible.

1.3 Eigenvalues of Unitary Operators and Phase Representation

For phase estimation, we are interested in the eigenvalues of a unitary operator.
Suppose

$$U|\psi_j\rangle = \lambda_j |\psi_j\rangle .$$

Because U is unitary, it preserves vector norms:

$$\||\psi_j\rangle\| = \|U|\psi_j\rangle\| .$$

Substituting the eigenvalue equation,

$$\||\psi_j\rangle\| = \|\lambda_j |\psi_j\rangle\| = |\lambda_j| \cdot \||\psi_j\rangle\| .$$

Therefore ,

$$|\lambda_j| = 1.$$

Remark 4 (Phase form of eigenvalues). Since $|\lambda_j| = 1$, each eigenvalue lies on the unit circle in the complex plane and can be written as

$$\lambda_j = e^{2\pi i\theta}, \qquad \text{where } \theta \in [0, 1).$$

Thus, determining the eigenvalue of a unitary is equivalent to estimating its phase θ the central objective of the Phase Estimation algorithm.

2 Phase Estimation

2.1 Problem Statement

Given:

1. A quantum state $|\psi\rangle$ on n qubits.
2. Access to a unitary operator $U \in \mathbf{C}^{2^n \times 2^n}$.
3. **Given:** $|\psi\rangle$ is an eigenvector of U.

Goal: Find the eigenvalue λ corresponding to $|\psi\rangle$. Since U is unitary, every eigenvalue lies on the unit circle, so we can write

$$U|\psi\rangle = \lambda|\psi\rangle = e^{2\pi i\theta}|\psi\rangle , \qquad \theta \in [0, 1).$$

The objective of phase estimation is to estimate the phase θ.
Constraints:

- θ is a real number and may not be representable in finitely many bits.
- If θ *is* representable with m bits, say $\theta = 0.\theta_1\theta_2 \cdots \theta_m$ in binary, then we aim to recover these bits exactly.
- **Cost model:** each application of a controlled-U gate is considered expensive and is charged as computational cost.

2.2 The Single-Qubit Estimator Circuit

To begin estimating θ, we use one auxiliary qubit and the target eigenstate $|\psi\rangle$.

2.2.1 Circuit description

1. Initialize the first bit as $|0\rangle$.
2. Apply a Hadamard gate H to the first bit.
3. Apply a controlled-U operation controlled by the first bit.

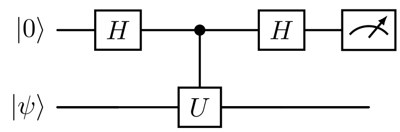


Figure 1: Single-qubit phase kickback circuit: measured in $|0\rangle$ and $|1\rangle$

2.2.2 State evolution

Step 1 (Initialization):

$$|\Psi_0\rangle \;=\; |0\rangle \otimes |\psi\rangle \,.$$

Step 2 (Hadamard on 1st bit):

$$|\Psi_1\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes |\psi\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle\,|\psi\rangle + |1\rangle\,|\psi\rangle \Big).$$

Step 3 (Apply controlled-U):

- If the control is $|0\rangle$, apply identity to $|\psi\rangle$.
- If the control is $|1\rangle$, apply U to $|\psi\rangle$.

Using $U\,|\psi\rangle = e^{2\pi i\theta}\,|\psi\rangle$, we obtain

$$|\Psi_{\text{final}}\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle\,|\psi\rangle + e^{2\pi i\theta}\,|1\rangle\,|\psi\rangle \Big) = \left(\frac{|0\rangle + e^{2\pi i\theta}\,|1\rangle}{\sqrt{2}}\right) \otimes |\psi\rangle \,.$$

2.3 Measurement Analysis

The first bit state after the controlled-U is

$$|\varphi_{\text{anc}}\rangle \;=\; \frac{|0\rangle + e^{2\pi i\theta}\,|1\rangle}{\sqrt{2}}.$$

To extract information about θ, we measure it in the Hadamard basis: Rewrite computational basis states in terms of $|+\rangle\,, |-\rangle$ and substituting into $|\varphi_{\text{anc}}\rangle$:

$$\begin{aligned}|\varphi_{\text{anc}}\rangle &= \frac{1}{\sqrt{2}}\left[\frac{|+\rangle + |-\rangle}{\sqrt{2}} + e^{2\pi i\theta}\,\frac{|+\rangle - |-\rangle}{\sqrt{2}}\right] \\ &= \frac{1}{2}\Big((1 + e^{2\pi i\theta})\,|+\rangle + (1 - e^{2\pi i\theta})\,|-\rangle\Big).\end{aligned}$$

2.3.1 Probability of measuring $|+\rangle$

The amplitude of $|+\rangle$ is $(1 + e^{2\pi i\theta})/2$, so

$$P(+) \;=\; \left|\frac{1 + e^{2\pi i\theta}}{2}\right|^2 .$$

Using $|z|^2 = zz^*$:

$$\begin{aligned}P(+) &= \frac{1}{4}(1 + e^{2\pi i\theta})(1 + e^{-2\pi i\theta}) \\ &= \frac{1}{4}\left(1 + e^{-2\pi i\theta} + e^{2\pi i\theta} + 1\right) \\ &= \frac{1}{4}\left(2 + 2\cos(2\pi\theta)\right) = \frac{1}{2}\left(1 + \cos(2\pi\theta)\right).\end{aligned}$$

Using $\cos^2(x) = \frac{1+\cos(2x)}{2}$ with $x = \pi\theta$, we get

$$P(+) \ = \ \cos^2(\pi\theta).$$

Similarly,

$$P(-) \ = \ \sin^2(\pi\theta).$$

2.4 Measurement Implementation

Measuring in the $\{|+\rangle, |-\rangle\}$ basis is equivalent to:

1. Apply a Hadamard gate H (or $H^\dagger$, which is the same since $H = H^\dagger$).
2. Measure in the computational basis $\{|0\rangle, |1\rangle\}$.

This converts the X-basis information into the standard Z-basis readout.

2.4.1 Summary of single-qubit estimator behavior

- If $\theta = 0$ (eigenvalue 1), then $P(+) = \cos^2(0) = 1$ and we always measure $|+\rangle$.
- If $\theta = \frac{1}{2}$ (eigenvalue -1), then $P(+) = \cos^2(\frac{\pi}{2}) = 0$ and we always measure $|-\rangle$.
- Therefore if we know that the θ is either 0 or $\frac{1}{2}$ we can measure in Hadamard basis to exactly find θ.
- For other values of θ, the outcomes follow the distribution $P(+) = \cos^2(\pi\theta)$ and $P(-) = \sin^2(\pi\theta)$.

2.5 Limitations of the Single-Qubit Estimator

Key observations:

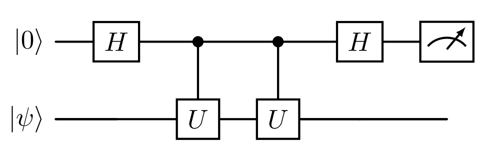
1. **Ambiguity in general:** For $\theta \in [0, 1)$ arbitrary, a single run only provides statistical evidence. One-shot measurements cannot identify θ with high precision.
2. **Error metric:** We measure estimation error using a wrap-around distance on $[0, 1)$:

$$\varepsilon \ = \ \left|(\hat{\theta} - \theta) \bmod 1\right|.$$

3 The U^2 Circuit

To gain more information about θ in particular, the next bit of its binary expansion we can apply a higher power of the unitary.

Circuit idea. In the last circuit apply two controlled-U gates in sequence.



Derivation. If $U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$, then

$$U^2|\psi\rangle = U\big(e^{2\pi i\theta}|\psi\rangle\big) = e^{2\pi i\theta}\,U|\psi\rangle = e^{2\pi i\theta}\,e^{2\pi i\theta}|\psi\rangle = e^{2\pi i(2\theta)}|\psi\rangle\,.$$

Thus the first bit after the circuit is

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

so this circuit effectively probes the phase $2\theta \bmod 1$.

Remark 5. Write θ in binary as $\theta = 0.\theta_1\theta_2\theta_3\cdots$. Then $2\theta = \theta_1.\theta_2\theta_3\cdots$. Since global integer parts are irrelevant modulo 1 in $e^{2\pi i(\cdot)}$, the phase $e^{2\pi i(2\theta)}$ is sensitive to the *next* bits (starting at θ_2).

Remark 6. Thus if we know θ_1 is either 0 or 1 we can also answer the question whether θ is [0 or $\frac{1}{4}$] and [$\frac{1}{2}$ and $\frac{3}{4}$]

4 Two-Qubit Phase Estimation

Setup. Combining the last 2 circuits:

1. 1st bit controls U (phase factor $e^{2\pi i\theta}$).
2. 2nd bit controls U^2 (phase factor $e^{2\pi i(2\theta)}$).

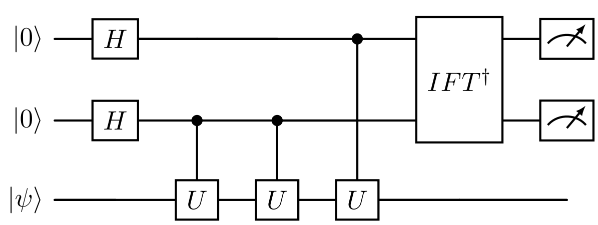


Figure 2: Two-qubits phase estimation, followed by $IFT^\dagger$ on the two extra bits.

(We use the tensor-product ordering where the first ancilla corresponds to θ and the second to 2θ.)

Combined state (ignoring $|\psi\rangle$).

$$|\Psi\rangle = \left(\frac{|0\rangle + e^{2\pi i\theta}|1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + e^{2\pi i(2\theta)}|1\rangle}{\sqrt{2}}\right).$$

Expanding,

$$|\Psi\rangle = \frac{1}{2}\Big(|00\rangle + e^{2\pi i\theta}|10\rangle + e^{2\pi i(2\theta)}|01\rangle + e^{2\pi i(3\theta)}|11\rangle\Big).$$

4.1 Distinguishing Exact Phases (Example)

Consider the four phases

$$\theta \in \left\{0, \frac{1}{4}, \frac{1}{2}, \frac{3}{4}\right\}.$$

Substituting into the expanded state yields four distinct vectors:

1. $\theta = 0$: $|\psi_0\rangle = \frac{1}{2}\big(|00\rangle + |10\rangle + |01\rangle + |11\rangle\big)$.
2. $\theta = \frac{1}{4}$: $|\psi_{1/4}\rangle = \frac{1}{2}\big(|00\rangle + i|10\rangle - |01\rangle - i|11\rangle\big)$.
3. $\theta = \frac{1}{2}$: $|\psi_{1/2}\rangle = \frac{1}{2}\big(|00\rangle - |10\rangle + |01\rangle - |11\rangle\big)$.
4. $\theta = \frac{3}{4}$: $|\psi_{3/4}\rangle = \frac{1}{2}\big(|00\rangle - i|10\rangle - |01\rangle + i|11\rangle\big)$.

Remark 7. The states $|\psi_0\rangle, |\psi_{1/4}\rangle, |\psi_{1/2}\rangle, |\psi_{3/4}\rangle$ are mutually orthogonal. Hence there exists a measurement basis . Specifically, the inverse of matrix which convert the computational basis to these orthonormal basis.

Remark 8. Using k control bits and controlled powers up to $U^{2^{k-1}}$, we can exactly recover θ whenever θ is representable with bits.

4.2 Resemblance to the Discrete Fourier Transform

After applying the controlled unitaries, the first 2 qubits ends up in a state of the form.

$$|\Psi\rangle \;=\; \frac{1}{2}\sum_{x=0}^{3} e^{2\pi i\theta x}\,|x\rangle$$

The coefficient pattern $e^{2\pi i\theta x}$ is exactly a complex exponential sampled on $x = 0, 1, 2, 3$, i.e., the same structure that appears in the Discrete Fourier transform.

4.3 The Matrix Representation

Now we want to convert these orthonormal basis back into the computational basis for measurement. Thus we can define matrix V which takes standard basis to these orthonormal basis. For $N = 4$ we can define V as

$$V_4 \;=\; \frac{1}{\sqrt{4}}\begin{pmatrix}1 & 1 & 1 & 1\\ 1 & \omega & \omega^2 & \omega^3\\ 1 & \omega^2 & \omega^4 & \omega^6\\ 1 & \omega^3 & \omega^6 & \omega^9\end{pmatrix} \;=\; \frac{1}{2}\begin{pmatrix}1 & 1 & 1 & 1\\ 1 & i & -1 & -i\\ 1 & -1 & 1 & -1\\ 1 & -i & -1 & i\end{pmatrix}.$$

, where

$$\omega \;=\; e^{2\pi i/N},\;\&\;\; N = 4$$

This representation of V is the DFT of the first 2 qubits with frequency ω. To convert the bits to computational basis, we apply the Inverse Fourier Transform which corresponds to $V_4^{-1} = V_4^{\dagger}$.

4.4 Measurement Accuracy

The accuracy depends on whether θ is exactly representable with the available number of extra qubits.

- **Exact case:** If θ has an m-bit binary expansion $\theta = 0.x_1x_2\cdots x_m$, then the IQFT outputs $|x_1x_2\cdots x_m\rangle$ with probability 1.
- **Approximate case:** If θ requires more than m bits (or is irrational), the output distribution is concentrated near the closest representable bit strings, giving a small approximation error.

4.5 Time Complexity

Taking the Inverse Fourier Transform is bounded by $O(mlog(m))$ for a vector of size m. Thus in the case of n qubits it will be $O(2^n.n)$ in this case.