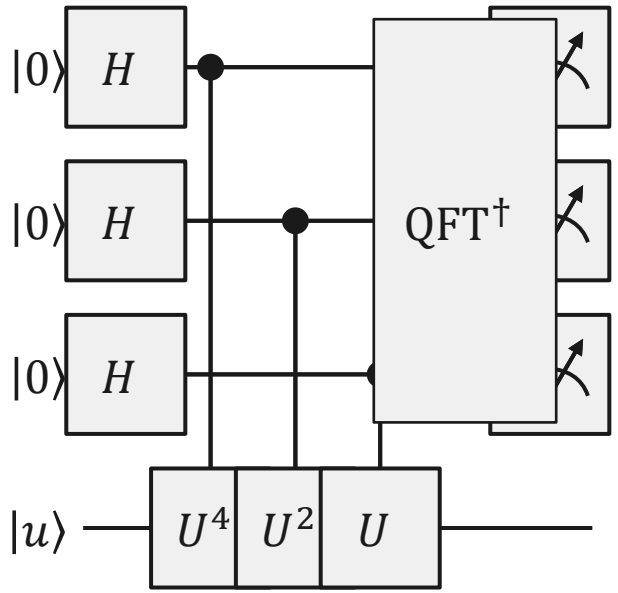
SAJID Lab
Smart & Advanced Junction of Intelligent Devices

EEE 6516 · QUANTUM COMPUTING

Phase Estimation

Reading the eigenphase of a unitary to t bits

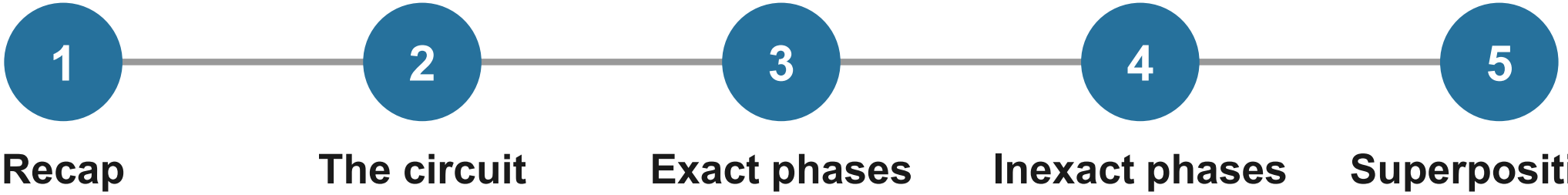


Chapter 6 · Lecture 13

Sajid Muhaimin Choudhury

Copyright © 2026 Sajid Muhaimin Choudhury. All rights reserved.

Today



By the end of this lecture you can

- state what phase estimation computes and draw its circuit with t counting qubits
- show that an exact t-bit phase is read with certainty
- derive the outcome probabilities for an inexact phase and prove the $4/\pi^2$ bound
- choose t for n bits at confidence $1 - \varepsilon$; explain what a superposition of eigenstates returns

YOUR TURN · RECALL

Recap: what does controlled-U² kick back?

Recall · 45 seconds

$U|u\rangle = e^{2\pi\, i\varphi}|u\rangle$. The control starts in $|+\rangle$ and controls U^2 on $|u\rangle$. The control becomes

A $\left(|0\rangle + e^{2\pi\, i\varphi}|1\rangle\right)/\sqrt{2}$

B $\left(|0\rangle + e^{2\pi\, i\cdot 2\varphi}|1\rangle\right)/\sqrt{2}$

C $|+\rangle$: the target becomes $U^2|u\rangle$

D $\left(|0\rangle + e^{2\pi\, i\varphi^2}|1\rangle\right)/\sqrt{2}$

ANSWER

B: the eigenvalue is squared, so the phase doubles

$$U^2|u\rangle = U\left(e^{2\pi\, i\varphi}|u\rangle\right) = e^{2\pi\, i\cdot 2\varphi}|u\rangle$$

D squares φ instead of the eigenvalue; C forgets that |u⟩ is an eigenvector of U², so the target is unchanged.

In turns: U^{2^m} multiplies φ by 2^m, a shift of its binary point by m places.

Powers of U write shifted copies of φ: today's circuit puts each on its own control qubit.

1 The phase-estimation circuit

How do many controls and powers of U read many bits of φ?

The problem: t bits of an eigenphase

Phase estimation: given

$$\mathrm{C}(U)\ \text{(repeatable)}, \qquad U|u\rangle = e^{2\pi\, i\varphi}|u\rangle$$

Returns

$$\text{an estimate of } \varphi \text{ to } t \text{ bits}, \qquad M = 2^t$$

One kickback puts φ on one qubit: at most one bit per run, with a probability.

Use a counting register of t qubits, and powers U, U^2, U^4, ….

Then an inverse QFT turns the phases into the digits of φ.

DERIVATION

Powers of U write the phase into the register

$U^{2^m}|u\rangle = e^{2\pi\, i\varphi 2^m}|u\rangle$ — apply U 2^m times

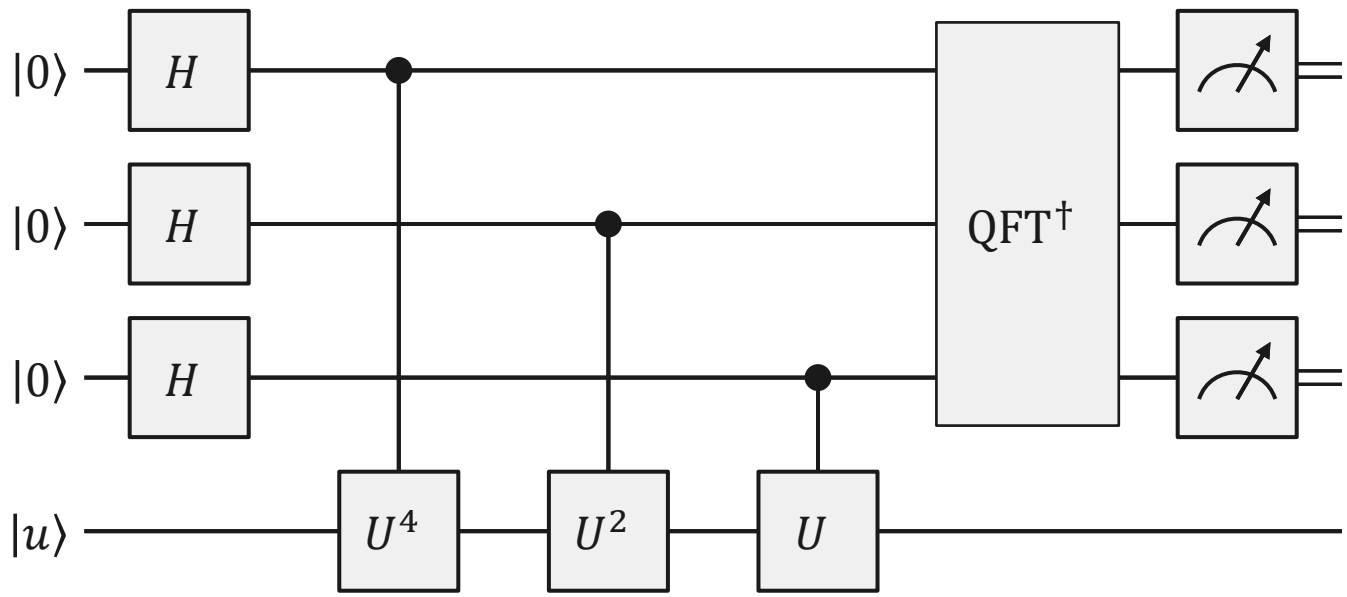
qubit j controls $U^{2^{t-1-j}}$: phase $2^{t-1-j}\varphi$ — qubit 0 (MSB) gets the highest power

$|k\rangle = |k_1 \ldots k_t\rangle$: $2\pi\varphi\sum_{l=1}^{t} k_l 2^{t-l} = 2\pi\varphi\, k$ — the phases of the set bits add up

$\frac{1}{\sqrt{M}}\sum_{k=0}^{M-1} e^{2\pi\, i\varphi\, k}|k\rangle \otimes |u\rangle$ — the state after the controlled gates

If φ = p/M for an integer p, this is exactly QFT|p⟩: the inverse QFT returns |p⟩.

The circuit, t = 3



t = 3: qubit 0 controls U⁴, qubit 1 controls U², qubit 2 controls U

1 Hadamards: the uniform superposition.

2 Controlled powers: qubit j gets the phase $2^{t-1-j}\varphi$.

3 Inverse QFT, then measure: the digits of φ.

The eigenvector register is never measured and never changes.

YOUR TURN · PREDICT

Predict: the exact case

Predict · 45 seconds

If $\varphi = p/M$ for an integer p, what does the inverse QFT do to $\frac{1}{\sqrt{M}}\sum_k e^{2\pi\, i\varphi\, k}|k\rangle$?

A returns $|p\rangle$ with certainty

B gives a uniform superposition: every m equally likely

C returns $|M - p\rangle$, because of the minus sign

D depends on the eigenvector $|u\rangle$

ANSWER

A: the inverse QFT returns |p⟩ with certainty

$$\frac{1}{\sqrt{M}}\sum_k e^{2\pi\, ipk/M}|k\rangle = \mathrm{QFT}|p\rangle \;\Rightarrow\; \mathrm{QFT}^{\dagger}\mathrm{QFT}|p\rangle = |p\rangle$$

The measurement then gives the bits of p, and φ = p/M exactly.

C: the plus sign of the QFT matches the state, so the inverse gives p, not M − p. D: |u⟩ only sets φ.

If φ is not of the form p/M, the state is not a QFT of a basis state: part three.

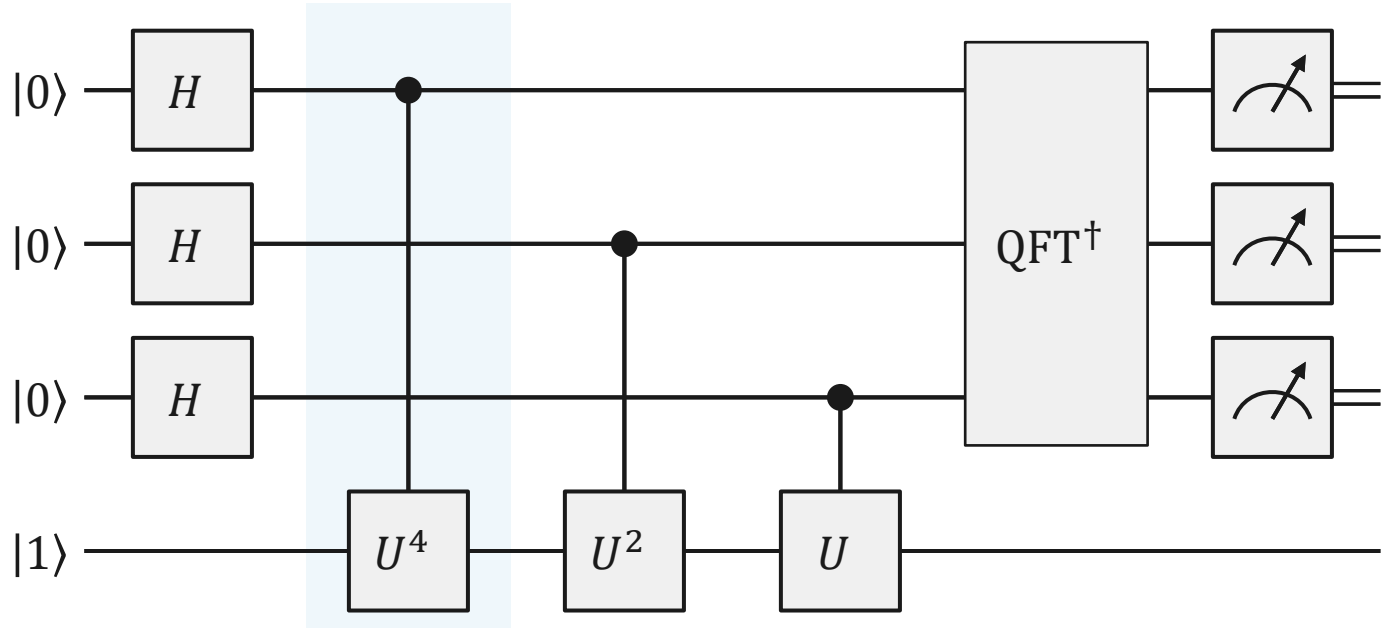
An exact t-bit phase is read without error.

2 The exact case

Can we follow an exact phase through the circuit by hand?

WORKED EXAMPLE · STEP 1 OF 4

Worked example: U = P(2π·⅝), t = 3



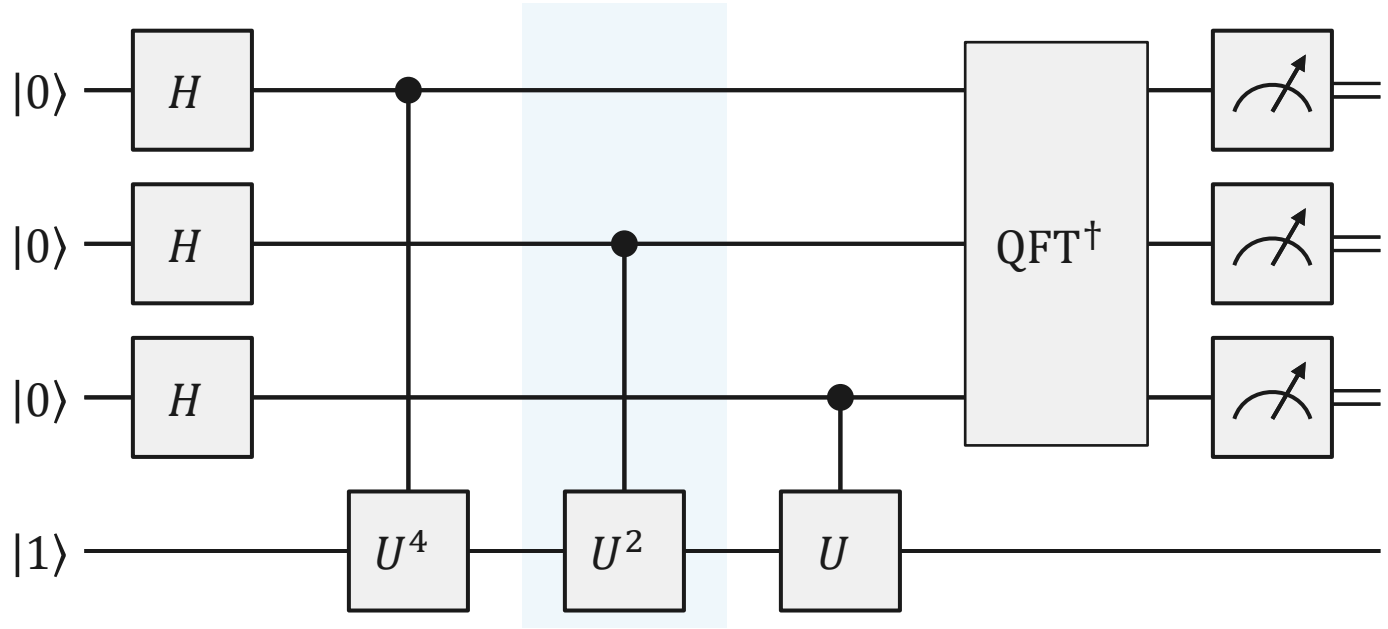
1 Qubit 0 controls U⁴: 4·⅝ = 5/2 turns ≡ ½: it becomes |0⟩ − |1⟩.

q_0: $4\varphi = 5/2 \equiv 1/2$: $|0\rangle - |1\rangle$

Before the next slide

What does qubit 1 pick up?

Worked example: U = P(2π·⅝), t = 3



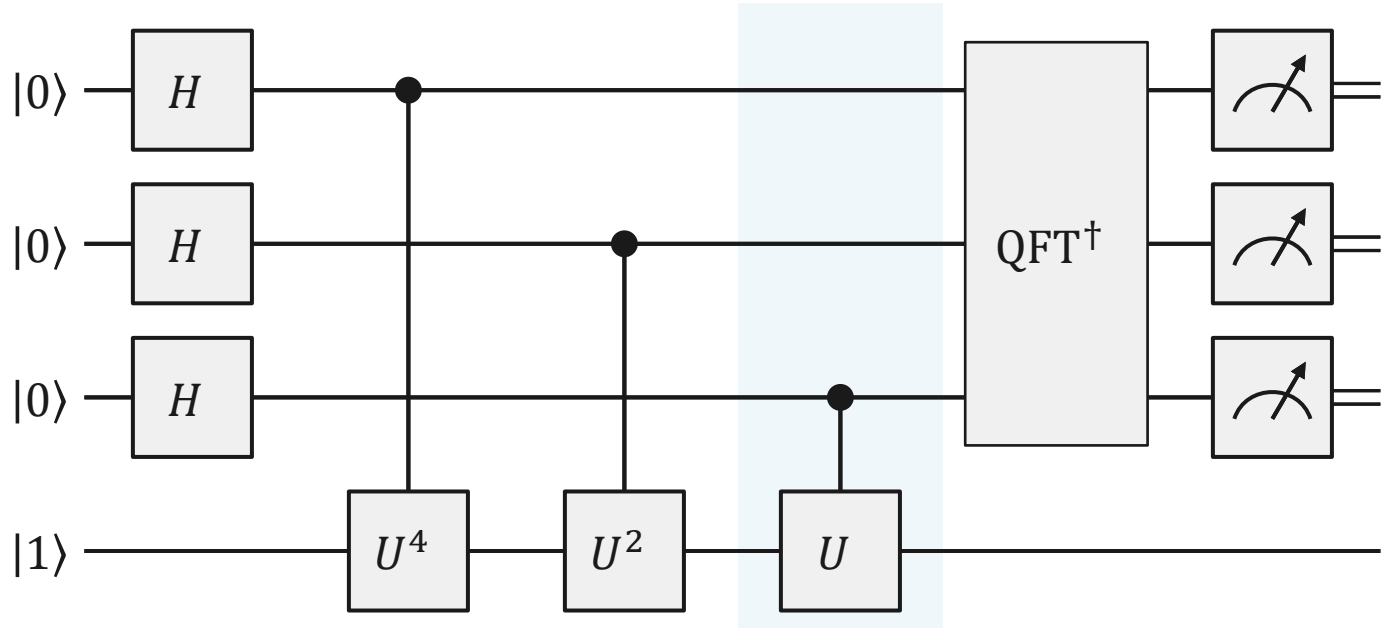
1 Qubit 0 controls U⁴: 4·⅝ = 5/2 turns ≡ ½: it becomes |0⟩ − |1⟩.

2 Qubit 1 controls U²: 2·⅝ = 5/4 ≡ ¼ turn: |0⟩ + i|1⟩.

q_0: $4\varphi = 5/2 \equiv 1/2$: $|0\rangle - |1\rangle$

q_1: $2\varphi = 5/4 \equiv 1/4$: $|0\rangle + i|1\rangle$

Worked example: U = P(2π·⅝), t = 3



1 Qubit 0 controls U⁴: 4·⅝ = 5/2 turns ≡ ½: it becomes |0⟩ − |1⟩.

2 Qubit 1 controls U²: 2·⅝ = 5/4 ≡ ¼ turn: |0⟩ + i|1⟩.

3 Qubit 2 controls U: ⅝ turn: $|0\rangle + e^{5\pi\, i/4}|1\rangle$. These are the factors of QFT|101⟩.

q_0: $4\varphi = 5/2 \equiv 1/2$: $|0\rangle - |1\rangle$

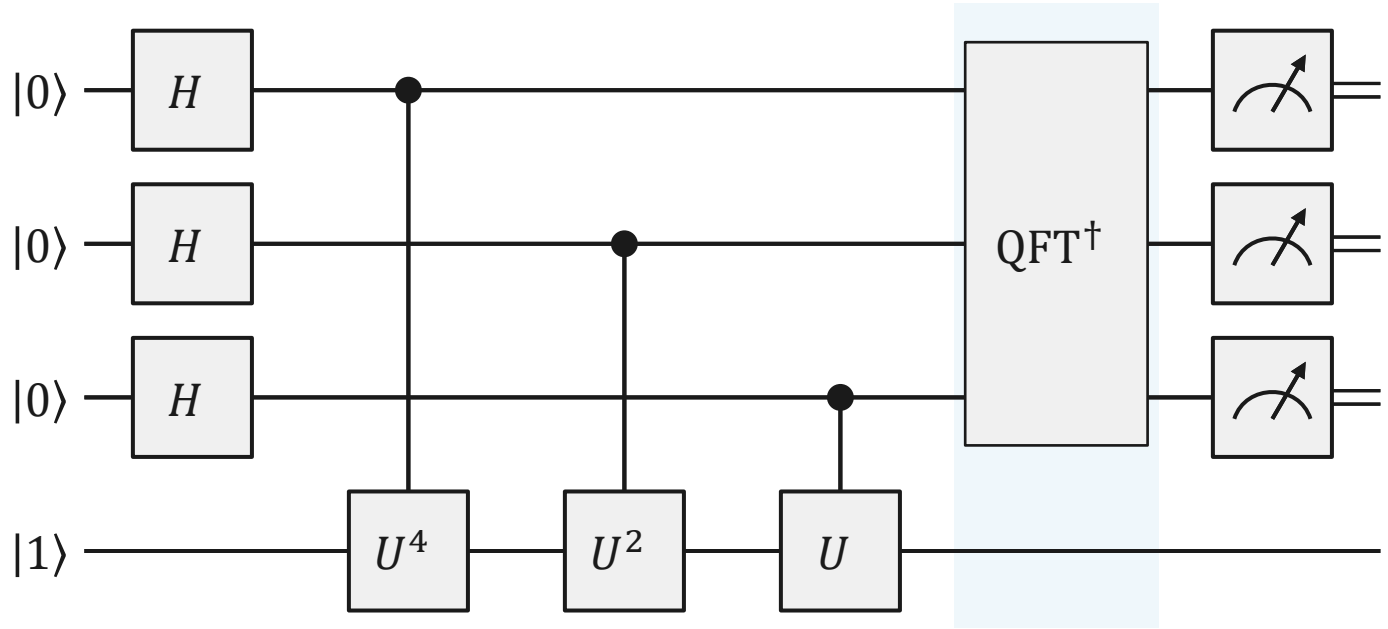
q_1: $2\varphi = 5/4 \equiv 1/4$: $|0\rangle + i|1\rangle$

q_2: $\varphi = 5/8$: $|0\rangle + e^{5\pi\, i/4}|1\rangle$

Before the next slide

So what does QFT† return?

Worked example: U = P(2π·⅝), t = 3



q_0: $4\varphi = 5/2 \equiv 1/2$: $|0\rangle - |1\rangle$

q_1: $2\varphi = 5/4 \equiv 1/4$: $|0\rangle + i|1\rangle$

q_2: $\varphi = 5/8$: $|0\rangle + e^{5\pi\, i/4}|1\rangle$

$\mathrm{QFT}^\dagger$: $|101\rangle \Rightarrow \varphi = 5/8$

1 Qubit 0 controls U⁴: 4·⅝ = 5/2 turns ≡ ½: it becomes |0⟩ − |1⟩.

2 Qubit 1 controls U²: 2·⅝ = 5/4 ≡ ¼ turn: |0⟩ + i|1⟩.

3 Qubit 2 controls U: ⅝ turn: $|0\rangle + e^{5\pi\, i/4}|1\rangle$. These are the factors of QFT|101⟩.

4 QFT† maps the register to |101⟩: φ = 0.101 = ⅝ with probability 1.

SIMULATION

Simulation 6.3: an exact phase

```
t, phi = 3, 5 / 8
qc.x(t)
qc.h(range(t))
for j in range(t):
    qc.cp(2 * np.pi * phi * 2 ** (t - 1 - j), j, t)
p = Statevector(qc).probabilities_dict(range(t))
p = {k[::-1]: v for k, v in p.items()}
```

```
outcome 101 = 5/8
probability 1.000000
```

Inverse QFT: QFTGate(t).inverse() on the reversed counting qubits.

Exact probabilities from Statevector; textbook order.

YOUR TURN · VOTE

Quick vote: reading the register

Vote · 30 seconds

Phase estimation with $t = 3$ on $U = \mathrm{P}(2\pi \cdot 3/8)$ and its eigenvector $|1\rangle$. The counting register, in textbook order, reads

A 011 with certainty

B 110 with certainty

C the decimal digits 375

D a uniformly random three-bit string

3 The inexact case

What happens when φ has no exact t-bit expansion?

DERIVATION

The outcome probability is a geometric sum

$$\langle m|\mathrm{QFT}^{\dagger}\psi\rangle = \frac{1}{M}\sum_{k=0}^{M-1} e^{2\pi\, ik\delta}, \qquad \delta = \varphi - \frac{m}{M}$$

row m of the inverse QFT

$$= \frac{1}{M}\,\frac{1-e^{2\pi\, iM\delta}}{1-e^{2\pi\, i\delta}}$$

geometric series

$$\Pr(m) = \frac{\sin^2(\pi\, M\delta)}{M^2\sin^2(\pi\delta)}$$

$$\left|1-e^{i\theta}\right| = 2|\sin(\theta/2)|$$

Spectral leakage: a tone between two DFT bins spills into its neighbours.

DERIVATION

Proof: the nearest estimate has probability ≥ 4/π²

$0 < \lvert\delta\rvert \le 1/(2M) \;\Rightarrow\; \lvert\pi\, M\delta\rvert \le \pi/2$	m is the nearest estimate
$\sin x \ge 2x/\pi \text{ on } 0 \le\ x \le \pi/2 \;\Rightarrow\; \sin^2(\pi\, M\delta) \ge 4M^2\delta^2$	the sine lies above its chord
$\lvert\sin x\rvert \le \lvert x\rvert \;\Rightarrow\; \sin^2(\pi\delta) \le \pi^2\delta^2$	for the denominator
$\Pr(m) \ge \frac{4M^2\delta^2}{M^2\pi^2\delta^2} = \frac{4}{\pi^2} \approx 0.405$	combine

Theorem: the nearest t-bit estimate occurs with probability at least 4/π²; exactly 1 if φ = m/M.

YOUR TURN · VOTE

Quick vote: an inexact phase

Vote · 30 seconds

U has eigenphase $\varphi = 0.3$, which is not a t-bit fraction. The most likely outcome of phase estimation with t counting qubits is

A exactly 0.3, provided that enough shots are taken

B the t-bit fraction just below 0.3, in every case

C the t-bit fraction nearest 0.3, with probability at least $4/\pi^2$

D a uniformly random t-bit fraction, since φ is inexact

YOUR TURN · CALCULATE

Your turn: φ = ⅓ with t = 3

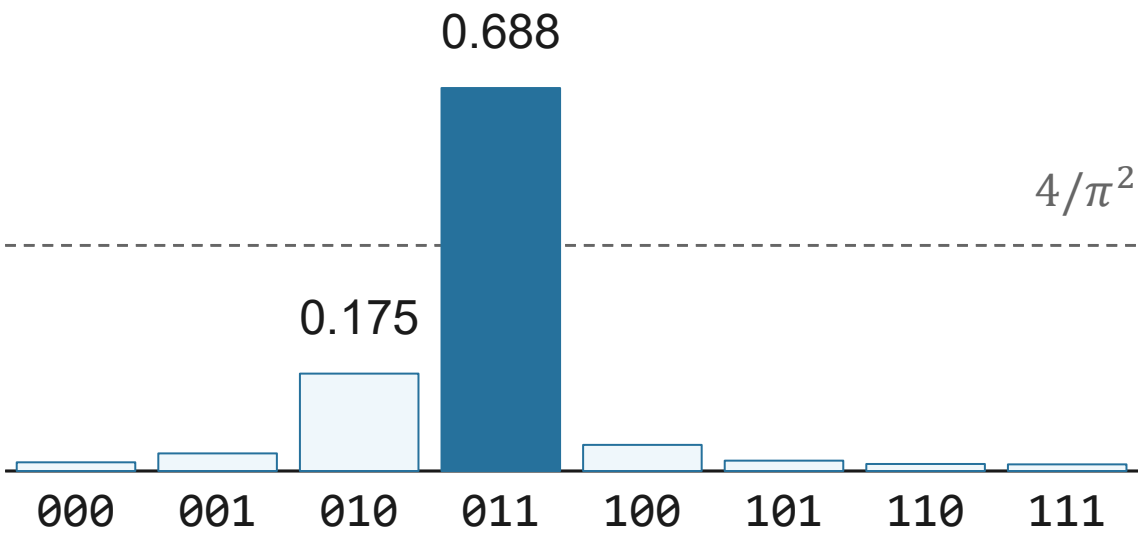
Pairs · 2 minutes

U has eigenphase $\varphi = 1/3$. With $t = 3$, find $\Pr(011)$ and $\Pr(010)$, and compare the larger with $4/\pi^2$.

$$\Pr(m) = \frac{\sin^2(\pi M\delta)}{M^2\sin^2(\pi\delta)}$$

ANSWER

⅜ is most likely: 0.688, above $4/\pi^2$



t = 3, φ = ⅓: exact probabilities (Simulation 6.4)

$$\Pr(011) = \frac{\sin^2(\pi/3)}{64\sin^2(\pi/24)} \approx 0.688$$

$$\Pr(010) = \frac{\sin^2(2\pi/3)}{64\sin^2(\pi/12)} \approx 0.175$$

Together 0.863; the other six outcomes share the remaining 14 %.

The recorded simulation agrees: the bars on the left.

The nearest estimate wins, but not with certainty.

YOUR TURN · VOTE

Quick vote: more bits of φ

Vote · 30 seconds

A phase must be known to n bits with high probability. Which statement is correct?

A With $t = 3$ counting qubits, more shots alone give more bits

B $t = n$ counting qubits give n correct bits with probability 0.99

C t must equal the number of qubits in the eigenstate register

D t must exceed n by a few qubits to give high confidence

How many counting qubits?

n bits with probability ≥ 1 − ε

$$t = n + \lceil \log_2 \left(2 + \frac{1}{2\varepsilon} \right) \rceil$$

Example: n = 3, ε = 0.1

$$t = 3 + \lceil \log_2 7 \rceil = 6$$

Resolution is $1/M = 2^{-t}$: t qubits give about t bits.

Confidence costs a few extra qubits, to suppress the far outcomes.

More shots do not replace qubits: they cannot resolve φ finer than 2^{-t}.

Report an estimate with its resolution, $\pm 2^{-t-1}$.

SIMULATION

Simulation 6.4: φ = ⅓ for t = 3, 4, 6, 8

```
qc.h(range(t))
for j in range(t):
    qc.cp(2 * np.pi * phi * 2 ** (t - 1 - j), j, t)
phi, sim = 1 / 3, AerSimulator(seed_simulator=6564)
for t in (3, 4, 6, 8):
    m = round(phi * 2 ** t)
    p = Statevector(qc).probabilities_dict(range(t))
```

Exact P from Statevector; counts from 2000 shots (seed 6564).

Outcomes converted to textbook order.

t	estimate	P	counts
3	3/8	0.6878	1406
4	5/16	0.6849	1327
6	21/64	0.6840	1329
8	85/256	0.6839	1328

2000 shots each; $4/\pi^2 = 0.4053$ estimate → ⅓, P stays ≈ 0.68

COMMON MISTAKE

“Phase estimation returns the phase”

✗ “the output is φ”

φ = ⅓ measured with t = 3

reported as φ = 0.375

No outcome is ever exactly ⅓.

✓ estimate ± resolution, with a probability

φ ≈ 0.375 ± 0.0625 (t = 3)

probability ≈ 0.69 for this outcome

more bits: increase t (eq. for t)

A t-bit fraction $m/2^t$, found with a probability.

Phase estimation returns a t-bit fraction $m/2^t$, and only with a probability: report its resolution and confidence.

4 A superposition of eigenstates

What if the second register is not an eigenvector?

DERIVATION

Input: a superposition of eigenstates

$\sum_s c_s |u_s\rangle, \qquad U|u_s\rangle = e^{2\pi\, i\varphi_s}|u_s\rangle$

$\rightarrow \sum_s c_s |\Phi_s\rangle|u_s\rangle$

$\Pr(m) = \sum_s |c_s|^2 \Pr(m|\varphi_s)$

any state is a combination of eigenvectors

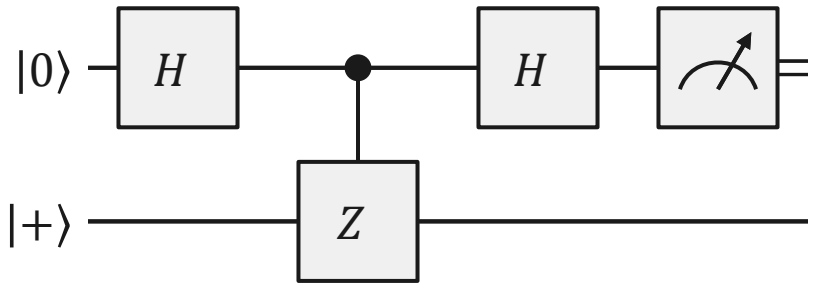
linearity; $|\Phi_s\rangle$ is the estimate register for φ_s

the $|u_s\rangle$ are orthogonal: no cross terms

Each run returns an estimate of one eigenphase φ_s, chosen with probability $|c_s|^2$.

YOUR TURN · PREDICT

Predict: Z on |+⟩ with one counting qubit



t = 1: the inverse QFT is H

Predict · 45 seconds

$U = Z$ has eigenvectors $|0\rangle$ (φ = 0) and $|1\rangle$ (φ = ½). Run phase estimation with $t = 1$ on $|+\rangle$. The outcome is

A always 0

B always 1

C 0 or 1, each with probability ½

D 0 with probability ¾

ANSWER

C: 0 or 1, each with probability ½

$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$: weights ½ and ½

φ = 0 alone gives outcome 0; φ = ½ alone gives outcome 1 (both exact for t = 1).

Afterwards the target is |0⟩ or |1⟩, matching the outcome: the eigenvector was selected.

Each run reports one eigenphase, at random; the mixture rule in miniature.

Recap

1 **The circuit**

H, controlled $U^{2^{t-1-j}}$, then $\mathrm{QFT}^{\dagger}$; the register holds a tone of frequency φ

2 **Exact phases**

a t-bit fraction is read with certainty

3 **Inexact phases**

$\Pr \geq 4/\pi^2$ for the nearest estimate; $t = n + \lceil \log_2(2 + 1/2\varepsilon) \rceil$

4 **Superpositions**

each run estimates one eigenphase, with probability $|c_s|^2$

After the break: Lecture 14

Order finding and Shor's algorithm

Read: handout 6.4 again; 6.5–6.7 for after the break.

Exit ticket

Which unitary, acting on the integers modulo N, would have the order of a modulo N in the denominator of its eigenphases? Bring a guess to the next lecture.

Copyright © 2026 Sajid Muhaimin Choudhury. All rights reserved.

Rights and attributions

Copyright (c) 2026 Sajid Muhaimin Choudhury. All rights reserved.

Public edition of Lecture 13: Phase Estimation. Release qc-2026-10-15, prepared 2026-10-15 from source revision 3df9449aa6.

This edition omits speaker notes, instructor-only material and every figure whose publication rights are not cleared for public distribution.