ECE/CSC/MA 467/567
Introduction to Quantum Algorithms

Final Exam – Spring 2026

May 4, 2026

Please remember to justify your answers carefully. We are interested not only in the final result but also in your reasoning and intermediate steps.

Last name: ______________________ First name: ______________________

Question 1 (Simon's algorithm.)

Consider a function

$$f : \{0,1\}^3 \to \{0,1\}^2,$$

where there exists a nonzero secret bitstring $s \in \{0,1\}^3$ such that

$$f(x) = f(y) \quad \text{if and only if} \quad x = y \text{ or } x = y \oplus s.$$

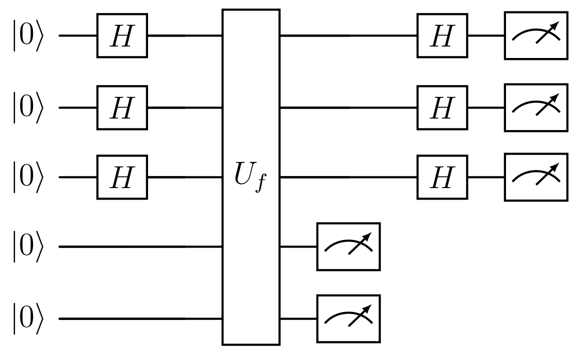
Suppose that two runs of Simon's algorithm yield the following measurement outcomes:

$$o^{(1)} = 110, \qquad o^{(2)} = 011.$$

(a) What equations must the secret string s satisfy?

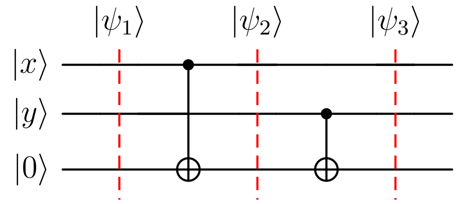
(b) Find all possible values of s that satisfy these equations.

(c) Below is the quantum circuit used in Simon's algorithm for $n = 3$. Recall that the second register has 2 qubits. What does the oracle unitary U_f do to a general computational-basis input $|x\rangle\,|y\rangle$? What is its action on $|x\rangle\,|00\rangle$?



Question 2 (XOR circuit.)

Consider the following three-qubit circuit, where the third qubit starts in $|0\rangle$:



In other words, we apply a CNOT from the first qubit to the third qubit, and then a CNOT from the second qubit to the third qubit.

(a) Show that for computational-basis inputs (i.e., when $x, y \in \{0, 1\}$), the circuit maps

$$|\psi_1\rangle = |x\rangle\,|y\rangle\,|0\rangle \quad \mapsto \quad |\psi_3\rangle = |x\rangle\,|y\rangle\,|x \oplus y\rangle\,,$$

where $|\psi_1\rangle$ is the input of the quantum circuit, $|\psi_2\rangle$ is the quantum state after the first CNOT, and $|\psi_3\rangle$ is the output after the second CNOT.

(b) Compute the output when the input is $|+\rangle\,|+\rangle\,|0\rangle$.

Question 3 (Hadamard transform identity.)

Recall that for the Hadamard gate H,

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

(a) Show that for a single bit $x_1 \in \{0,1\}$,

$$H\left|x_1\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle + (-1)^{x_1}\left|1\right\rangle\right).$$

(b) Using part (a), show that for two bits $x_1, x_2 \in \{0,1\}$,

$$H^{\otimes 2}\left|x_1 x_2\right\rangle = \frac{1}{\sqrt{4}}\Big(\left|00\right\rangle + (-1)^{x_2}\left|01\right\rangle + (-1)^{x_1}\left|10\right\rangle + (-1)^{x_1+x_2}\left|11\right\rangle\Big).$$

(c) The expression in part (b) is a special case (using $n = 2$) of the following identity,

$$H^{\otimes n} |x\rangle = \frac{1}{\sqrt{N}} \sum_{s \in \{0,1\}^n} (-1)^{\langle s,x \rangle} |s\rangle, \qquad N = 2^n,$$

where

$$\langle s, x \rangle = \sum_{i=1}^{n} s_i x_i \pmod 2.$$

Using this identity, compute $H^{\otimes 3} |001\rangle$.

Question 4 (Can H and X generate the T gate?)

Recall the one-qubit gates

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \qquad T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}.$$

Suppose that we are allowed to design one-qubit circuits using only the gates H and X. We want to see if they can generate the T gate.

(a) A first attempt is to check whether some product of H and X can equal T exactly. Use determinants to show that this is impossible. You may use the identity

$$\det(AB) = \det(A)\det(B).$$

(b) In quantum mechanics, two gates that differ only by a global phase are physically equivalent. Therefore, a more meaningful question is whether some product of H and X can equal

$$e^{i\theta}T$$

for some real number θ. Explain why every product of H and X has only real entries.

(c) Show that there is no value of θ for which

$$e^{i\theta}T = \begin{bmatrix} e^{i\theta} & 0 \\ 0 & e^{i(\theta+\pi/4)} \end{bmatrix}$$

has only real entries. Hence conclude that the T gate cannot be implemented using only H and X, even up to a global phase. (Hint: if both diagonal entries are real, then their ratio must also be real.)

Question 5 (Quantum phase estimation.)

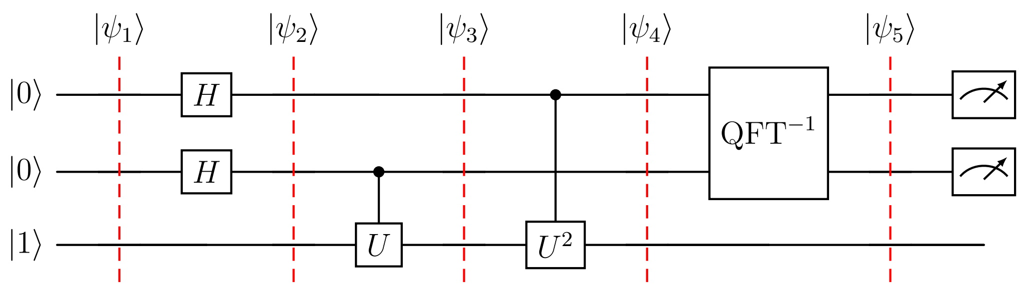
Consider quantum phase estimation for the one-qubit unitary

$$U = \begin{bmatrix} 1 & 0 \\ 0 & e^{i2\pi/3} \end{bmatrix}.$$

The state $|1\rangle$ is an eigenvector of U with eigenvalue

$$e^{i2\pi/3} = e^{i2\pi\varphi}, \qquad \varphi = \frac{1}{3}.$$

We use two qubits in the first register and one qubit in the second register. The first register is initialized at $|00\rangle$, and the second register is initialized at the eigenvector $|1\rangle$.



(a) Express the quantum state $|\psi_2\rangle$ after the two Hadamard gates are applied to the first register.

(b) Express the quantum state $|\psi_4\rangle$ after the controlled-U and controlled-U^2 gates. (Hint: how do U and U^2 act on $|1\rangle$?)

(c) Let $|y\rangle$ denote the quantum state of the first register in $|\psi_5\rangle$ after QFT^{-1} has been applied to the first register in $|\psi_4\rangle$. Let $y \in \{0, 1, 2, 3\}$ denote the decimal representation of $|y\rangle$. The quantum amplitudes of the state $|y\rangle$ are

$$a_y = \frac{1}{4} \sum_{k=0}^{3} e^{i2\pi k(\varphi - y/4)}.$$

Based on a_y, what is $|y\rangle$?

(d) It can be shown that the probabilities for the four possible measurement outcomes are

$$\Pr(00) \approx 0.063, \qquad \Pr(01) \approx 0.700, \qquad \Pr(10) \approx 0.188, \qquad \Pr(11) \approx 0.050.$$

Which outcome is most likely? What estimate of φ does this outcome represent?

(e) Explain why the answer in part (d) is not exact, although $\varphi = 1/3$ is rational.