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

Final Exam – Spring 2026

May 4, 2026

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

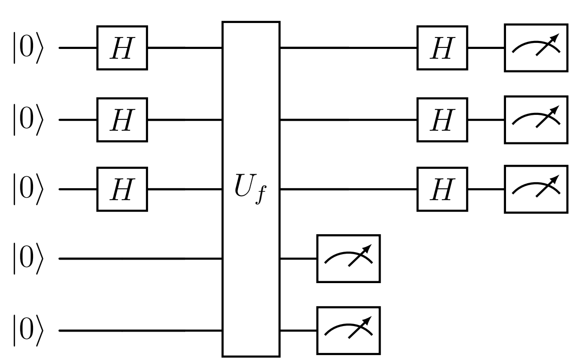
(a) What equations must the secret string s satisfy?

Solution. The unknown s must be orthogonal to $o^{(1)}$ and $o^{(2)}$. Therefore, $s_1 \times 1 + s_2 \times 1 + s_3 \times 0 = s_1 + s_2 = 0 \mod 2$ and $s_1 \times 0 + s_2 \times 1 + s_3 \times 1 = s_2 + s_3 = 0 \mod 2$.

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

Solution. Considering the constraints from Part (a), $s_1 = s_2$ and $s_3 = s_2$. Therefore, $s_1 = s_2 = s_3$. The trivial value of $s = 000$ is always a solution; the interesting solution is $s = 111$.

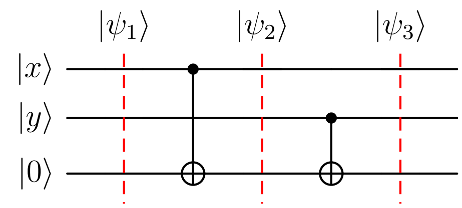
(c) Below is the quantum circuit used in Simon's algorithm for $n = 3$. Recall that the second register has 2 qubits. What does the oracle unitary U_f do to a general computational-basis input $|x\rangle |y\rangle$? What is its action on $|x\rangle |00\rangle$?



Solution. $U_f |x\rangle |y\rangle \to |x\rangle |f(x) \oplus y\rangle$.

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.

Solution. $|\psi_2\rangle = |x\rangle\,|y\rangle\,|0 \oplus x\rangle = |x\rangle\,|y\rangle\,|x\rangle$, hence $|\psi_3\rangle = |x\rangle\,|y\rangle\,|x \oplus y\rangle$.

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

Solution. The input is $|\psi_1\rangle = \frac{1}{2}(|000\rangle + |010\rangle + |100\rangle + |110\rangle)$, hence the output is

$$|\psi_3\rangle = \frac{1}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle).$$

Question 3 (Hadamard transform identity.)

Recall that for the Hadamard gate H,

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

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

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

Solution. For $x_1 = 0$, $H|0\rangle = |+\rangle$ and $\frac{1}{\sqrt{2}}(|0\rangle + (-1)^0|1\rangle) = |+\rangle$. For $x_1 = 1$, $H|1\rangle = |-\rangle$ and $\frac{1}{\sqrt{2}}(|0\rangle + (-1)^1|1\rangle) = |-\rangle$.

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

$$H^{\otimes 2}|x_1x_2\rangle = \frac{1}{\sqrt{4}}\Big(|00\rangle + (-1)^{x_2}|01\rangle + (-1)^{x_1}|10\rangle + (-1)^{x_1+x_2}|11\rangle\Big).$$

Solution.

$$\begin{aligned} H^{\otimes 2}|x_1x_2\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_1}|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_2}|1\rangle) \\ &= \frac{1}{\sqrt{4}}(|00\rangle + (-1)^{x_2}|01\rangle + (-1)^{x_1}|10\rangle + (-1)^{x_1+x_2}|11\rangle). \end{aligned}$$

(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 $H^{\otimes 3}|001\rangle$.

Solution. There are multiple ways how to solve this part. One approach is to realize that there is a tensor product between $H|0\rangle$, $H|0\rangle$, and $H|1\rangle$, which is $|{+}{+}{-}\rangle$. A more elaborate approach is to consider the $N = 2^3 = 8$ computational basis states, compute the sign of each one, and the end result will be,

$$H^{\otimes 3}|001\rangle = \frac{1}{\sqrt{8}}(|000\rangle + |010\rangle + |100\rangle + |110\rangle - |001\rangle - |011\rangle - |101\rangle - |111\rangle).$$

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

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

Solution. It can be readily seen that $\det\{H\} = \det\{X\} = -1$. Therefore, using the identity provided, the determinany of any product of H and X will be either -1 or $+1$. However, the determinant of T is different.

(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.

Solution. Matrix products involve sums and products over individual entries, hence with real entries the matrix product is real. Specifically, H and X have real valued entries hence all products of these matrices have 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.)

Solution. The ratio of diagonal entries is $e^{i\pi/4} \notin \mathbb{R}$ for all values of θ. Therefore, the matrix cannot have only real values, and cannot be implemented using only H and T.

Question 5 (Quantum phase estimation.)

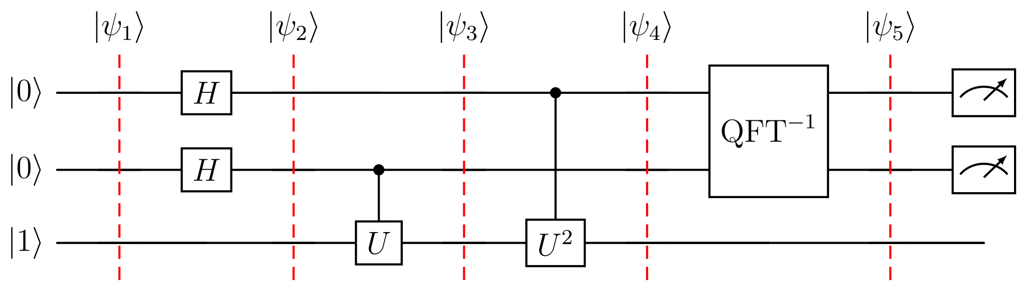
Consider quantum phase estimation for the one-qubit unitary

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

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.

Solution. $|\psi_1\rangle = |++1\rangle = \frac{1}{2}(|001\rangle + |011\rangle + |101\rangle + |111\rangle)$.

(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 $|1\rangle$?)

Solution. $|\psi_4\rangle = \frac{1}{2}(|001\rangle + e^{i2\pi(\phi)}|011\rangle + e^{i2\pi(2\phi)}|101\rangle + e^{i2\pi(3\phi)}|111\rangle)$.

(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 $|y\rangle$?

Solution. $|y\rangle = a_0|00\rangle + a_1|01\rangle + a_2|10\rangle + a_3|11\rangle$.

(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?

Solution. The outcome 01 is most likely. It corresponds to the number 1, and the estimated phase is $\frac{1}{N} = 0.25$.

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

Solution. The number 1/3 can be represented as a binary decimal, $1/3 = (0.010101\ldots)_2$. This binary decimal is closest to 1/4, hence the answer in Part b. However, because the binary decimal does not fit nicely into 2 binary digits (bits), the other quantum amplitudes are nonzero.