CSE 190 / Math 152 – Introduction to Quantum Computing (Fall 2026)
Homework 5
Due Tuesday, November 17, 11:59pm

Instructions: There are two parts to this homework:

- Concept check (Problem 1): Complete individually on Gradescope.
- Written Homework (Problems 2–3): You may work individually or in a team of up to 3 people. If working in a group, make only one submission per group on Gradescope: one person uploads the submission and then adds the other group members to the submission by selecting their names in the "Add Group Members" dialog box. All problems will be graded for completeness. Completeness means that it looks like there was a good-faith effort to solve the problem. A LaTeX template for the homework is provided on Canvas.

Problems:

1. **Concept check**

   Complete the assignment "Homework 5 - Concept Check" on Gradescope.

   Must be completed individually even if working in a team for the rest of the assignment.

2. **Variants of Simon's problem**

   Let $f\colon \{0,1\}^n \to \{0,1\}^n$ be a function, and define

   $$\mathsf{Out} := \{f(x) : x \in \{0,1\}^n\}$$

   to be the set of all outputs of the function. Let's assume f satisfies Simon's promise: there exists a bit string $s \in \{0,1\}^n$ such that for all $x \neq y$, $f(x) = f(y)$ iff $x \oplus y = s$.

   (a) Suppose $s \neq 0^n$. Prove that for every output $o \in \mathsf{Out}$, there are *exactly* two inputs $x_1, x_2 \in \{0,1\}^n$ such that $f(x_1) = f(x_2) = o$.

   (b) Suppose $s = 0^n$. Prove that for every output $o \in \mathsf{Out}$, there is *exactly* one input $x \in \{0,1\}^n$ such that $f(x) = o$.

   In other words, when $s \neq 0^n$, the function f is 2-to-1 (there are two inputs per output); and when $s = 0^n$, the function f is 1-to-1 (there is one input per output). Based on this distinction, let's define a new variant of Simon's problem where the goal is to decide which setting we're in (notice we're no longer assuming that $s \neq 0^n$):

   Decision variant of Simon's problem

Function:	$f\colon \{0,1\}^n \to \{0,1\}^n$
Promise:	There exists $s \in \{0,1\}^n$ such that for all $x \neq y$, $f(x) = f(y)$ iff $x \oplus y = s$.
Question:	Decide if f is 2-to-1 or if f is 1-to-1.

(c) Show that there is a quantum query algorithm that solves this decision variant of Simon's problem using (roughly) n quantum queries.
Hint: Use the exact same quantum circuit for Simon's problem that we saw in class. You may use the fact that if you sample (roughly) n uniformly random $y \in \{0,1\}^n$ satisfying $y \cdot s = 0$, then you can compute s with high probability.

Let's now turn to a different way to generalize Simon's problem:

Simon's problem with more secrets

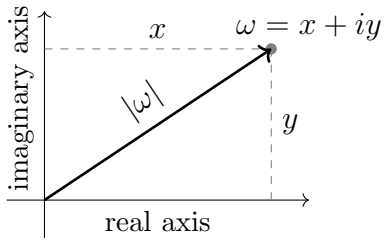
Function: $f\colon \{0,1\}^n \to \{0,1\}^n$
Promise: There is a secret group defined by $s \in \{0,1\}^n$ and $t \in \{0,1\}^n$.
For $x \neq y$, $f(x) = f(y) \iff y \in \{\, x \oplus s,\ x \oplus t,\ x \oplus t \oplus s \,\}$
Question: Determine the secret group $\{0^n, s, t, s \oplus t\}$.

(d) Suppose $s \neq 0^n$, $t \neq 0^n$, and $s \neq t$. Design a quantum query algorithm that determines the secret group $\{0^n, s, t, s \oplus t\}$ using (roughly) n quantum queries. (It suffices to output any two distinct nonzero elements of the group, since these determine the third.)
Hint: Start by working out which strings y the circuit for Simon's problem can output. You may assume that (roughly) n samples are enough to solve the resulting system of linear equations with high probability.

3. **Introduction to roots of unity and the Quantum Fourier Transform**

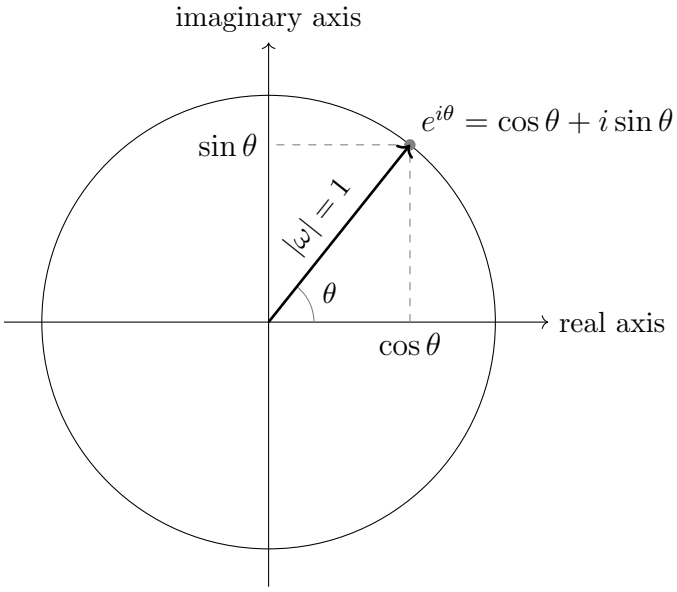
The purpose of this problem is to introduce you to a very important operation in quantum computation called the "Quantum Fourier Transform." Before we can even define the Quantum Fourier Transform, let's take a step back to introduce a key concept about complex numbers called a *root of unity*. An nth root of unity is a complex number ω such that $\omega^n = 1$.

To get some intuition about what these numbers look like, let's revisit our geometric picture of a complex number. In the complex plane, the real component of the complex number is drawn on the horizontal axis and the imaginary component is drawn on the vertical axis.



(a) Show that if ω is an nth root of unity, then $|\omega| = 1$.
Hint: You may use properties of complex numbers that you proved in Homework 1.

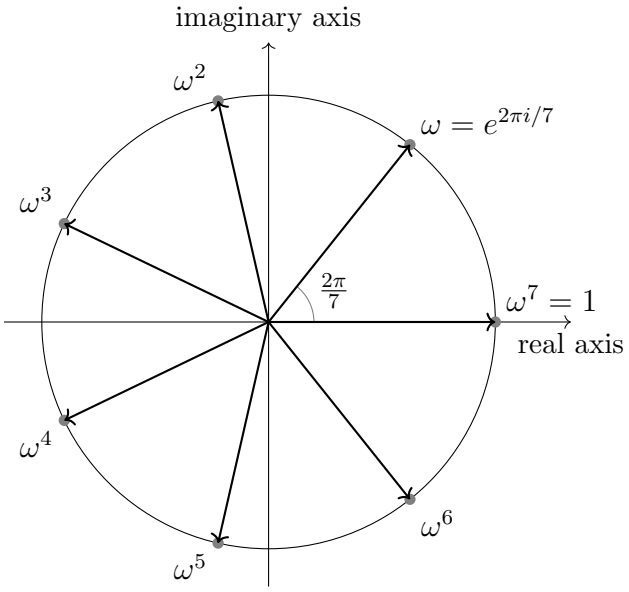
In other words, when we draw an nth root of unity in the complex plane, we know that it must lie somewhere on the unit circle:



Using the fact that $e^{i\theta_1}e^{i\theta_2} = e^{i(\theta_1+\theta_2)}$, we get that multiplying any complex number by $\omega = e^{i\theta}$ is a rotation by angle θ in the complex plane. We can think of the roots of unity as those complex numbers that rotate perfectly back to 1 by repeated multiplication:

$$\omega \to \omega^2 \to \omega^3 \to \cdots \to \omega^n = 1$$

The diagram below shows all of these points for a 7th root of unity: $\omega = e^{2\pi i/7}$.



We say that an nth root of unity ω is *primitive* if it is not an mth root of unity for any positive integer $m < n$.

(b) Prove that $\omega_n = e^{2\pi i/n}$ is a primitive nth root of unity.

We're finally ready to define the n-qubit Quantum Fourier Transform operator. For ease of notation, we will write $N = 2^n$. We have

$$\mathrm{QFT}_N := \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_N & \omega_N^2 & \omega_N^3 & \cdots & \omega_N^{N-1} \\ 1 & \omega_N^2 & \omega_N^4 & \omega_N^6 & \cdots & \omega_N^{2(N-1)} \\ 1 & \omega_N^3 & \omega_N^6 & \omega_N^9 & \cdots & \omega_N^{3(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_N^{N-1} & \omega_N^{2(N-1)} & \omega_N^{3(N-1)} & \cdots & \omega_N^{(N-1)(N-1)} \end{pmatrix}$$

In other words, QFT_N is an $N \times N$ unitary matrix such that the (j,k)th entry of the matrix is $\omega_N^{jk}/\sqrt{N}$ where we index j and k starting from 0. For now, let's just explore some basic properties of the QFT.

(c) Show that the Hadamard matrix is a QFT_N matrix for some value of N.

(d) Show that for every positive integer n, $\mathrm{QFT}_N |0^n\rangle$ can be written as a tensor product of single-qubit states.

Challenge question (not graded): Show that for every positive integer n and every bit string $x \in \{0,1\}^n$, $\mathrm{QFT}_N |x\rangle$ can be written as a tensor product of single-qubit states.