CS 593/MA 595 - Intro to Quantum Computation
Midterm Exam 2 **PRACTICE**

Name:____

Fall 2025

Instructions: This exam should have 4 pieces of paper. The last page should be blank and can be used as scratch paper.

There are 2 problems. You have 50 minutes to solve both. You must show your work to get full credit.

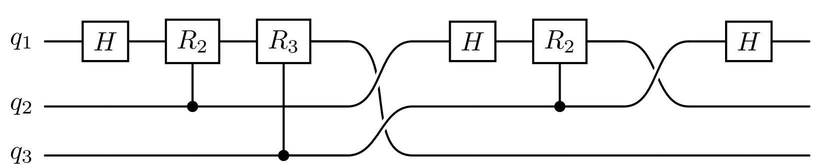
For your convenience, here is a reminder of some of the standard qubit quantum gates, expressed as matrices in the computational basis.

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad X = \text{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

$$R_x(\theta) = \begin{pmatrix} \cos\theta/2 & -i\sin\theta/2 \\ -i\sin\theta/2 & \cos\theta/2 \end{pmatrix} \qquad R_y(\theta) = \begin{pmatrix} \cos\theta/2 & -\sin\theta/2 \\ \sin\theta/2 & \cos\theta/2 \end{pmatrix} \qquad R_z(\theta) = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}$$

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad \text{Toffoli} = \text{CCNOT} = CCX = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

For your referencce, recall that the Fourier transform $\mathcal{FT}_{\mathbb{Z}/2^3\mathbb{Z}}$ has a circuit given by



where

$$R_l = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^l} \end{pmatrix}.$$

If any notation on the exam is unclear, please raise your hand to let us know.

Question	Score
1	
2	
TOTAL	

1. Suppose S is a set of n integral points in a bounded region of the plane, *i.e.* $S \subset ([0, M]^2 \cap \mathbb{Z}^2) \subset \mathbb{R}^2$, where $M = O(\text{poly}(n))$. Let

$$\textbf{3PointsOnALine}(S) = \begin{cases} 1 & \text{if there exist distinct } a, b, c \in S \text{ that lie on a common line} \\ 0 & \text{else.} \end{cases}$$

Assume we have a classical circuit R with $O(\text{polylog } n) \subseteq O(n^{o(1)})$ gates[1] that outputs (x_j, y_j) when its input is j.[2] Assume for this problem that all elementary arithmetic operations over $\mathbb{Z} \cap [0, \text{poly}(M)]$ (addition, multiplication, and equivalence checking) can be done with $O(\text{polylog } M) \subseteq O(n^{o(1)})$ gates.[3] Describe a quantum algorithm with $O(n^{1.5+o(1)})$ gates that computes **3PointsOnALine**.

[1] $O(n^{o(1)})$ includes all functions that are asymptotically smaller than $O(n^{\epsilon})$ for any $\epsilon > 0$.

[2] By what we know from class, this means we can use R to build a quantum circuit Q with $O(\text{polylog } n)$ gates and ancillary qubits so that

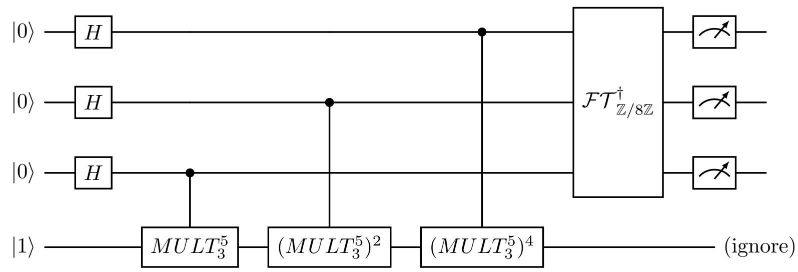
$$|j\rangle |0\rangle |0\rangle \xrightarrow{Q} |j\rangle |x_j\rangle |y_j\rangle .$$

[3] We're working in kind of quantum "word RAM" model, roughly, for what it's worth.

2. Let $\mathbb{C}^5 = \mathbb{C}\mathbb{Z}/5\mathbb{Z}$ be a qudit with $d = 5$ and let $MULT_x^5$ be the multiplication by x mod 5 operation:

$$\begin{aligned} MULT_x^5 : \mathbb{C}^5 &\to \mathbb{C}^5 \\ |k\rangle &\mapsto |xk \mod 5\rangle \end{aligned}$$

Let $x = 3$ and consider the following quantum phase estimation circuit on $\left(\mathbb{C}^2\right)^{\otimes 3} \otimes \mathbb{C}^5$:



Compute the probability distribution of outcomes over the set $\{0, 1, \ldots, 7\} = \{000, 001, \ldots, 111\}$.