Assignment 3

Due: 11:59pm, October 9, 2025

1. **A query problem for a black-box function acting on qutrits [15 points].**

   Suppose that $f : \mathbb{Z}_3 \to \mathbb{Z}_3$ takes on the value 1 for exactly one element of $\mathbb{Z}_3$, and 0 for the other two elements (and never takes the value 2). There are three possibilities:

x	$f_0(x)$
0	1
1	0
2	0

x	$f_1(x)$
0	0
1	1
2	0

x	$f_2(x)$
0	0
1	0
2	1

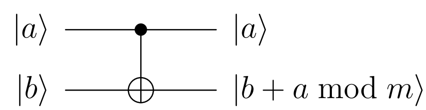
   Suppose you're given a black-box unitary that, for all $a, b \in \mathbb{Z}$, performs the mapping

$$|a\rangle|b\rangle \to |a\rangle|b + f(a) \bmod 3\rangle, \tag{1}$$

   where $f : \mathbb{Z}_3 \to \mathbb{Z}_3$ is one of the above three functions, and your goal is to determine whether f is f_0, f_1, or f_2. Give a quantum algorithm that solves this problem with a single f-query.

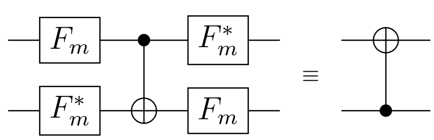
   (Hint: consider using the Fourier transform F_3 and its inverse F_3^* as part of your solution.) Also, remember that the inner product of $v, w \in \mathbb{C}^3$ is $\overline{v}_1 w_1 + \overline{v}_2 w_2 + \overline{v}_3 w_3$.)

2. **Control-target inversion for mod m registers [15 points].** Consider a scenario where the registers are m-dimensional ($m \geq 2$). Let the computational basis states be $|0\rangle, |1\rangle, \ldots, |m-1\rangle$. Define the two-register *addition (mod m)* gate as the unitary operation that acts on the computational basis states as



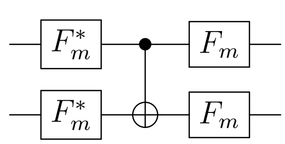
   (where $a, b \in \mathbb{Z}_m$). In the above circuit diagram, each wire represents an m-dimensional system (a qubit in the special case where $m = 2$).

   (a) [9 points] Prove that, for every $m \geq 2$, the following circuit equivalence holds:



   where F_m is the $m \times m$ Fourier transform.

   (b) [6 points] Consider the following circuit diagram where the F_m and F_m^* are arranged in a slightly different way:



   Give a simple expression for what the circuit does to computational basis states $|a\rangle|b\rangle$ (for $a, b \in \mathbb{Z}_m$). There is a very simple expression.

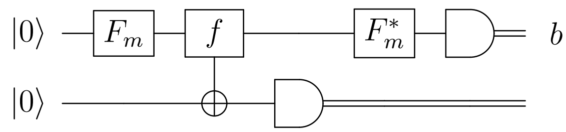
3. **A $d = 1$ case of the Simon mod m problem [15 points].**

Let $f : \mathbb{Z}_m \to \mathbb{Z}_m$ have the property that there exists an r that is a divisor of m, such that $f(a) = f(b)$ if and only if $a - b$ is a multiple of r.

(a) [5 points] Prove that, for any $a \in \mathbb{Z}_m$, the set of preimages of $f(a)$ is precisely

$$\left\{a,\, a + r,\, a + 2r,\, \ldots,\, a + (\tfrac{m}{r} - 1)r\right\}. \tag{2}$$

(b) [10 points] Consider this quantum circuit (acting on two m-dimensional registers):



Show that the outcome of the top measurement is a uniformly-distributed random element of the set $\{b \in \mathbb{Z}_m : \text{such that } r \cdot b = 0\}$ (with mod m arithmetic in $\mathbb{Z}_m$).

The analysis here is similar to that in Section 22.1 of the posted *Lecture Notes* (Sept. 29 or later). This is a $d = 1$ case; whereas the lecture notes analyze a $d = 2$ case. You can use the notes as a guide; however, some of the details are different, and your analysis should be fully self-contained. You may assume Eq. (205) in Exercise 21.1 without proof.

4. **A simple variant of the phase estimation problem [15 points].**

Suppose that you're given a two-qubit gate that is a controlled-U gate, for some unknown one-qubit unitary U. You are given this gate as a black box and you are also given a qubit whose state is *promised* to be an eigenvector of U, with eigenvalue either $\lambda_1 = e^{2\pi i/3}$ or $\lambda_2 = e^{4\pi i/3}$ (you don't know which case it is). Your goal is to determine whether the eigenvalue is λ_1 or λ_2.

Show how this can be accomplished *exactly* (with success probability 1) with *two* queries to the controlled-U gate. Of course, you may also use other gates of your choosing (that are independent of U and the state of the qubit, which you do not know).

5. **(This is an optional question for bonus credit)**
Factorizing certain two-variable polynomials [8 points; 4 each].
Let m be an integer such that $m \geq 2$. Let $a, b \in \mathbb{Z}_m$ and define $f : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$ as

$$f(x, y) = (x - a)(y - b) \bmod m, \tag{3}$$

for all $x, y \in \mathbb{Z}_m$.

Suppose that you are given access to a black-box that, on input (x, y), produces $f(x, y)$ as output, but you do not know what the constants a and b are. Your goal is to determine a and b *exactly* (meaning with success probability 1).

Give a quantum algorithm that solves this problem with one f-query. The f-query is a unitary operation that maps basis states $|x, y\rangle|z\rangle$ to $|x, y\rangle|z + f(x, y) \bmod m\rangle$, for all $x, y, z \in \mathbb{Z}_m$. Explain why your algorithm works.

Note: There is a solution that can be clearly explained in under one page. If you submit a solution to this question then it should be clearly explained and not exceed two pages.