Assignment 5
Due: 11:59pm, October 26, 2021

1. **Interpolating a linear function with a single quantum query [15 points].** Let p be prime and $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be a function of the form $f(x) = ax + b \bmod p$, where a and b are unknown coefficients, and your goal is to determine the coefficient a with as few queries to f as possible. (You do not have to determine b.)

   (a) [5 points] Suppose that you are given a black-box that reversibly computes f as the mapping $(x, y) \mapsto (x, y + f(x) \bmod p)$, for all $x, y \in \mathbb{Z}_p$. Show that two classical queries are necessary to deduce a.

   (b) [10 points] Suppose that you're given a black-box unitary that reversibly computes f as $|x\rangle|y\rangle \mapsto |x\rangle|y + f(x) \bmod p\rangle$, for all $x, y \in \mathbb{Z}_p$. Show that one quantum query is sufficient to deduce a. (Hint: you may use the Fourier transform F_p and/or F_p^*.)

2. **Applying the Fourier transform to states with periodic structure [15 points].** Let p and q be integers greater than 1, and pq denote their product. Recall that the quantum Fourier transform modulo pq is the pq-dimensional unitary operation F_{pq} such that, for all $x \in \mathbb{Z}_{pq}$,

$$F_{pq}|x\rangle = \frac{1}{\sqrt{pq}} \sum_{y=0}^{pq-1} \omega^{xy}, |y\rangle \qquad \text{where } \omega = e^{2\pi i/pq}.$$

   (a) [7 points] Define two quantum states $|\psi_1\rangle$ and $|\psi_2\rangle$ as

$$|\psi_1\rangle = \frac{1}{\sqrt{q}} \left(|0\rangle + |p\rangle + |2p\rangle + \cdots + |(q-1)p\rangle \right) = \frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |xp\rangle$$

$$|\psi_2\rangle = \frac{1}{\sqrt{p}} \left(|0\rangle + |q\rangle + |2q\rangle + \cdots + |(p-1)q\rangle \right) = \frac{1}{\sqrt{p}} \sum_{x=0}^{p-1} |xq\rangle.$$

   Show that $F_{pq}|\psi_1\rangle = |\psi_2\rangle$.

   (b) [8 points] Let $s \in \{0, 1, \ldots, p-1\}$, and define $|\psi_3\rangle$ (a "shifted" version of $|\psi_1\rangle$) as

$$|\psi_3\rangle = \frac{1}{\sqrt{q}} \left(|s\rangle + |s+p\rangle + |s+2p\rangle + \cdots + |s+(q-1)p\rangle \right) = \frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |s + xp\rangle.$$

   What is $F_{pq}|\psi_3\rangle$? Find a simple expression for this quantity. If $F_{pq}|\psi_3\rangle$ is measured in the computational basis, what is the probability distribution describing the outcome?

CONTINUED ON NEXT PAGE

3. **(These are optional questions for bonus credit)**

All three questions relate to the following black-box problem. Suppose that $f : \mathbb{Z}_3 \to \mathbb{Z}_3$ is of the form $f(x) = ax^2 + bx + c$ (all arithmetic in this question is mod 3), for unknown coefficients $a, b, c \in \mathbb{Z}_3$, and the goal is to determine the value of $a \in \mathbb{Z}_3$ (the "leading coefficient").

You are given a black-box for f that maps (x, y) to $(x, y + f(x) \bmod 3)$ in the classical case; and a unitary operation that maps $|x\rangle|y\rangle$ to $|x\rangle|y + f(x) \bmod 3\rangle$ in the quantum case (for each $x, y \in \mathbb{Z}_3$). You are given no information about what the coefficients $a, b, c \in \mathbb{Z}_3$ are.

(a) [2 points] Show that any classical algorithm solving this problem must make at least three queries to f. (Note that the algorithm *only* has to determine a; it does *not* have to determine b or c.)

(b) [3 points] Give a quantum algorithm that solves this problem with two queries to f.

(c) [5 points] Prove that this problem cannot be solved by a quantum algorithm that makes only one query. More precisely, show that: if $a, b, c \in \mathbb{Z}_3$ are randomly generated (uniformly and independently) then there is no one-query algorithm that guesses a with probability greater than 1/3. (Warning: this part (c) is extra-challenging.)

You may submit a solution to any individual part(s) of this question: (a), (b), or (c). But, for each part, *only* submit a solution if you are confident that it is correct *and* you have a clear write-up of it.