Assignment 3
Due date: 11:59pm, October 31, 2023

1. **Hidden multi-linear functions (part I) [12 points].**
Let p be prime. Let $a_1, a_2, \ldots, a_n, b \in \mathbb{Z}_p$ and define $f : (\mathbb{Z}_p)^n \to \mathbb{Z}_p$ as

$$f(x_1, x_2, \ldots, x_n) = a_1x_1 + a_2x_2 + \cdots + a_nx_n + b \bmod p, \tag{1}$$

for all $x_1, x_2, \ldots, x_n \in \mathbb{Z}_p$.

Suppose that you are given access to a black-box that, on input $(x_1, x_2, \ldots, x_n) \in (\mathbb{Z}_p)^n$, produces $f(x_1, x_2, \ldots, x_n)$ as output, but you don't know what the linear coefficients $a_1, a_2, \ldots, a_n$ are, nor the additive constant b. Your goal is to determine the linear coefficients $a_1, a_2, \ldots, a_n$ *exactly* (meaning with success probability 1).

(a) [4 points] Prove that any classical algorithm for this problem must make at least $n+1$ f-queries.

(b) [8 points] Give a quantum algorithm that solves this problem with one f-query. The f-query is a unitary operation that maps each basis state $|x_1, \ldots, x_n\rangle|y\rangle$ to

$|x_1, \ldots, x_n\rangle|y+f(x_1, \ldots, x_n) \bmod p\rangle$,

for all $x_1, \ldots, x_n, y \in \mathbb{Z}_p$. Explain why your algorithm works.

2. **Hidden multi-linear functions (part II) [12 points].**
Let p be prime and $n \geq 2$. Let $a_2, \ldots, a_n \in \mathbb{Z}_p$ and $\sigma : \mathbb{Z}_p \to \mathbb{Z}_p$ be any permutation (which means that the mapping σ is 1-to-1 and onto). Define $f : (\mathbb{Z}_p)^n \to \mathbb{Z}_p$ as

$$f(x_1, x_2, \ldots, x_n) = \sigma(x_1 + a_2x_2 + \cdots + a_nx_n \bmod p), \tag{2}$$

for all $x_1, x_2, \ldots, x_n \in \mathbb{Z}_p$. Note that this is similar to the function in question 1, Eq. (1), except for these two notable differences:

- In Eq. (2), the first coefficient is set to 1 (i.e., $a_1 = 1$).
- In Eq. (2), an arbitrary permutation on $\mathbb{Z}_p$ is applied to $x_1 + a_2x_2 + \cdots + a_nx_n \bmod p$ (whereas, in Eq. (1), the permutation is of the restricted form $\sigma(z) = z + b \bmod p$).

Suppose that you are given access to a black-box that, on input $(x_1, x_2, \ldots, x_n) \in (\mathbb{Z}_p)^n$, produces $f(x_1, x_2, \ldots, x_n)$ as output, but you do not know what the linear coefficients $a_2, \ldots, a_n$ are, nor the permutation σ. Your goal is to determine the linear coefficients $a_2, \ldots, a_n$. For this question, it suffices to determine the answer with success probability at least $1 - \frac{1}{p}$ in all cases (i.e., for every instance f of the form of Eq. (2)).

Give a quantum algorithm that solves this problem making only one f-query (with success probability at least $1 - \frac{1}{p}$). Explain why your algorithm works.

CONTINUED ON NEXT PAGE

For questions 3, 4, and 5 below: Let $m = r{\cdot}s$ where r and s are two distinct prime numbers, and suppose we are given m, but not its factors r and s. Define a function $f : \mathbb{Z}_m \to \mathbb{Z}_m$ to be *strictly r-periodic* if it has this property:

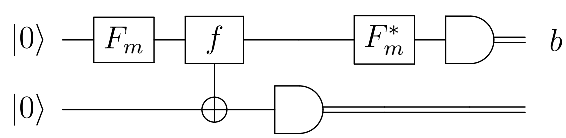
For any $a, b \in \mathbb{Z}_m$, $f(a) = f(b)$ *if and only if* $a - b$ is a multiple of r.

Suppose that we have an efficient implementation of an f-query. Also, suppose that we have an efficient implementation of the Fourier transforms F_m and F_m^*. Then we will see how to use these to construct a quantum algorithm that finds r, the periodicity of f. (And this quantum algorithm would also factor m.)

---

3. **Warm-up exercises [12 points; 4 each].**
Consider the case where $m = 35$, $r = 7$, and $s = 5$.
   (a) Give an example of a function $f : \mathbb{Z}_{35} \to \mathbb{Z}_{35}$ that is strictly 7-periodic. You may give the truth table or you may give a list of 35 numbers, that we'll interpret as $f(0), f(1), f(2), \ldots, f(34)$. Although any strictly 7-periodic function will get full marks here, please try to make your function look as irregular as you can subject to the condition of being strictly 7-periodic.
   (b) What are the *colliding sets* of your function in part (a)? These are the subsets of $\mathbb{Z}_{35}$ which f maps to the same value. List these sets. Also, show that each of these sets in of the form $\{a, a+7, a+2{\cdot}7, a+3{\cdot}7, a+4{\cdot}7\}$ (mod 35) for some $a \in \mathbb{Z}_{35}$.
   (c) List all $b \in \mathbb{Z}_{35}$ such that $b{\cdot}7 = 0$ (in mod 35 arithmetic).

4. **Using the Fourier transform to find a b such that $b{\cdot}r = 0$ [12 points].**
For any $f : \mathbb{Z}_m \to \mathbb{Z}_m$ that is strictly r-periodic, consider this quantum circuit (acting on two m-dimensional registers):



Show that the output of this circuit (more specifically, the outcome of the top measurement) is a uniformly-distributed random element of the set $\{b \in \mathbb{Z}_m : \text{such that } b{\cdot}r = 0\}$.

The analysis here is similar to that in Section 8.4 of the posted lecture notes on *Quantum Algorithms*. This is a $d = 1$ case; whereas the lecture notes analyzes 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 the fact that, for any primitive k-th root of unity of the form $\omega = e^{2\pi i/k}$ and $a \in \{1, 2, \ldots, k-1\}$, it holds that $\sum_{j=0}^{k-1} \omega^{a \cdot j} = 0$.

5. **Deducing r from b [12 points].**
Suppose that you are given a random $b \in \mathbb{Z}_m$ subject to $b \cdot r = 0$. Explain how to efficiently deduce r from m and b. You may use the fact that there is an efficient classical algorithm for computing the largest common divisor of two numbers. Note that some b's are useless; the success probability should be at least $\frac{1}{2}$.

CONTINUED ON NEXT PAGE

6. **(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).

(a) Show that any classical algorithm for this problem requires at least three f-queries.

(b) 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: If you submit a solution to this question then there is a size-limit of one page for part (a) and one page for part (b). In fact, each part has a solution that can be clearly explained in less than half a page.