Assignment 5

Due date: 11:59pm, October 22, 2020

Questions 1, 2, and 3 of this assignment are concerned with the relationship between the Simon mod m problem and the problem of finding the periodicity of a function.

> **Definition:** a function $f : \mathbb{Z}_m \to \mathbb{Z}_m$ is called *strictly r-periodic* if it has this property: $f(a) = f(b)$ *if and only if* $a - b$ is a multiple of r (for any $a, b \in \mathbb{Z}_m$).

For questions 1, 2, and 3 below: let $m = r \cdot s$ where r and s are two distinct primes, and suppose that we know m and have an efficient implementation of an f-query for a function $f : \mathbb{Z}_m \to \mathbb{Z}_m$ that is strictly r-periodic. 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.)

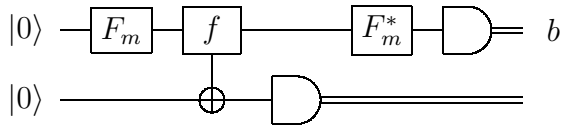
1. **Warm-up exercises [10 points].** Consider the case where $m = 35$, $r = 7$, and $s = 5$.

   (a) [4 points] 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) [3 points] What are the *colliding sets* of your function in part (a)? List these sets. Also, show that they satisfy the Simon mod 35 property, namely, that they are of the form $\{a, a + 7, a + 2 \cdot 7, \ldots, a + (s - 1) \cdot 7\}$ for some $a \in \mathbb{Z}_{35}$.

   (c) [3 points] List all $b \in \mathbb{Z}_{35}$ such that $b \cdot 7 = 0$ (in mod 35 arithmetic).

2. **Simon mod m algorithm in the $d = 1$ case [10 points].** Consider this quantum circuit.



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

   This is the $d = 1$ case of what was shown in Lecture 8 for $d = 2$. You can certainly use the lecture material as a guide; however, you should provide a full self-contained derivation of the result. You may assume the fact that, for any $j > 2$, if $\widetilde{\omega} = e^{2\pi i/j}$ (i.e., $\widetilde{\omega}$ is a primitive j-th root of unity) and $a \in \{1, 2, \ldots, j - 1\}$, then $\sum_{k=0}^{j-1} \widetilde{\omega}^{a \cdot k} = 0$.

3. **Deducing r from b [10 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

4. **(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 $(x, y + f(x))$ in the classical case; and a unitary operation that maps $|x\rangle|y\rangle$ to $|x\rangle|y + f(x)\rangle$ 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) [3 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) [5 points] Give a quantum algorithm that solves this problem with two queries to f.

(c) [6 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.