Due: April 5th, 2018
Date: March 27, 2018

Assignment 4

Please submit it electronically to ELMS. This assignment is 7% in your total points. For the simplicity of the grading, the total points for the assignment is 70.

Problem 1. *Determining the "slope" of a linear function over $\mathbb{Z}_4$.* Let $\mathbb{Z}_4 = \{0, 1, 2, 3\}$, with arithmetic operations of addition and multiplication defined with respect to modulo 4 arithmetic on this set. Suppose that we are given a black-box computing a linear function $f : \mathbb{Z}_4 \to \mathbb{Z}_4$, which of the form $f(x) = ax+b$, with unknown coefficients $a, b \in \mathbb{Z}_4$ (throughout this question, multiplication and addition mean these operations in modulo 4 arithmetic). Let our goal be to determine the coefficient a (the "slope" of the function). We will consider the number of quantum and classical queries needed to solve this problem.

Assume that what we are given is a black box for the function f that is in reversible form in the following sense. For each $x, y \in \mathbb{Z}_4$, the black box maps (x, y) to $(x, y + f(x))$ in the classical case; and $|x\rangle|y\rangle$ to $|x\rangle|y + f(x)\rangle$ in the quantum case (which is unitary).

Also, note that we can encode the elements of $\mathbb{Z}_4$ into 2-bit strings, using the usual representation of integers as a binary strings ($00 = 0$, $01 = 1$, $10 = 2$, $11 = 3$). With this encoding, we can view f as a function on 2-bit strings $f : \{0, 1\}^2 \to \{0, 1\}^2$. When refering to the elements of $\mathbb{Z}_4$, we use the notation $\{0, 1, 2, 3\}$ and $\{00, 01, 10, 11\}$ interchangeably.

(1) *(Points :5)* Prove that every classical algorithm for solving this problem must make two queries.

(2) *(Points :5)* Consider the 2-qubit unitary operation A corresponding to "add 1", such that $A|x\rangle = |x + 1\rangle$ for all $x \in \mathbb{Z}_4$. It is easy to check that

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Let $|\psi\rangle = \frac{1}{2}(|00\rangle + i|01\rangle + i^2|10\rangle + i^3|11\rangle)$, where $i = \sqrt{-1}$. Prove that $A|\psi\rangle = -i|\psi\rangle$.

(3) *(Points :5)* Show how to create the state $\frac{1}{2}((-i)^{f(00)}|00\rangle + (-i)^{f(01)}|01\rangle + (-i)^{f(10)}|10\rangle + (-i)^{f(11)}|11\rangle)$ with a single query to U_f. (Hint: you may use the result in part (2) for this.)

(4) *(Points :5)* Show how to solve the problem (i.e., determine the coefficient $a \in \mathbb{Z}_4$) with a single quantum query to f. (Hint: you may use the result in part (3) for this.)

Problem 2. *Factoring 21.*

1. *(Points :3)* Suppose that, when running Shor's algorithm to factor the number 21, you choose the value $a = 2$. What is the order r of a mod 21?

2. *(Points :3)* Give an expression for the probabilities of the possible measurement outcomes when performing phase estimation with n bits of precision in Shor's algorithm.

3. *(Points :3)* In the execution of Shor's algorithm considered in part (a), suppose you perform phase estimation with $n = 7$ bits of precision. Plot the probabilities of the possible measurement outcomes obtained by the algorithm. You are encouraged to use software to produce your plot.

4. *(Points :3)* Compute $\gcd(21, a^{r/2} - 1)$ and $\gcd(21, a^{r/2} + 1)$. How do they relate to the prime factors of 21?

5. *(Points :3)* How would your above answers change if instead of taking $a = 2$, you had taken $a = 5$?

Problem 3. *Searching for a quantum state.*

Suppose you are given a black box U_ϕ that identifies an unknown quantum state $|\phi\rangle$ (which may not be a computational basis state). Specifically, $U_\phi|\phi\rangle = -|\phi\rangle$, and $U_\phi|\xi\rangle = |\xi\rangle$ for any state $|\xi\rangle$ satisfying $\langle\phi|\xi\rangle = 0$.

Consider an algorithm for preparing $|\phi\rangle$ that starts from some fixed state $|\psi\rangle$ and repeatedly applies the unitary transformation VU_ϕ, where $V = 2|\psi\rangle\langle\psi| - I$ is a reflection about $|\psi\rangle$.

Let $|\phi^\perp\rangle = \frac{e^{-i\lambda}|\psi\rangle - \sin(\theta)|\phi\rangle}{\cos(\theta)}$ denote a state orthogonal to $|\phi\rangle$ in $\operatorname{span}\{|\phi\rangle, |\psi\rangle\}$, where $\langle\phi|\psi\rangle = e^{i\lambda}\sin(\theta)$ for some $\lambda, \theta \in \mathbb{R}$.

1. *(Points :2)* Write the initial state $|\psi\rangle$ in the basis $\{|\phi\rangle, |\phi^\perp\rangle\}$.

2. *(Points :5)* Write U_ϕ and V as matrices in the basis $\{|\phi\rangle, |\phi^\perp\rangle\}$.

3. *(Points :5)* Let k be a positive integer. Compute $(VU_\phi)^k$.

4. *(Points :4)* Compute $\langle\phi|(VU_\phi)^k|\psi\rangle$.

5. *(Points :4)* Suppose that $|\langle\phi|\psi\rangle|$ is small. Approximately what value of k should you choose in order for the algorithm to prepare a state close to $|\phi\rangle$, up to a global phase? Express your answer in terms of $|\langle\phi|\psi\rangle|$.

Problem 4. *The collision problem.*

Recall that the quantum search algorithm can find a marked item in a search space of size N using $O(\sqrt{N/M})$ queries, where M is the total number of marked items.

In the collision problem, you are given a black-box function $f\colon \{1, 2, \ldots, N\} \to S$ (for some set S) with the promise that f is two-to-one. In other words, for any $x \in \{1, 2, \ldots, N\}$, there is a unique $x' \in \{1, 2, \ldots, N\}$ such that $x \neq x'$ and $f(x) = f(x')$. The goal of the problem is to find such a pair (x, x') (called a collision).

1. *(Points :6)* For any $K \in \{1, 2, \ldots, N\}$, consider a quantum algorithm for the collision problem that works as follows:

   - Query $f(1), f(2), \ldots, f(K)$.
   - If a collision is found, output it.
   - Otherwise, search for a value $x \in \{K+1, K+2, \ldots, N\}$ such that $f(x) = f(x')$ for some $x' \in \{1, 2, \ldots, K\}$.

   How many quantum queries does this algorithm need to make in order to find a collision? Your answer should depend on N and K, and can be expressed using big-O notation.

2. *(Points :6)* How should you choose K in part (a) to minimize the number of queries used?

3. *(Points :8)* It turns out that the algorithm you found in part (b) is essentially optimal (although proving this is nontrivial). Discuss the relationship between the collision problem and Simon's problem in light of this fact.
