Due: October 10th, 2019
Date: September 27, 2019

Assignment 3

Please submit it electronically to ELMS. This assignment is 10% in your total points. Note that we will reward the use of Latex for typesetting by bonus points (extra 5% of your points).

Problem 1. *The Bernstein-Vazirani problem.*

1. *(4 points)* Suppose $f : \{0,1\}^n \to \{0,1\}$ is a function of the form

$$f(\underline{x}) = x_1 s_1 + x_2 s_2 + \cdots + x_n s_n \bmod 2$$

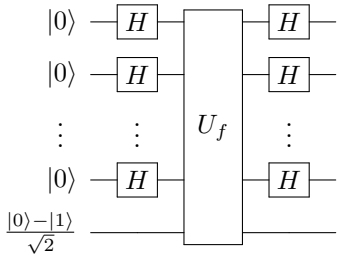
for some unknown $\underline{s} \in \{0,1\}^n$. Given a black box for f, how many classical queries are required to learn s with certainty?

2. *(5 points)* Prove that for any n-bit string $\underline{u} \in \{0,1\}^n$,

$$\sum_{\underline{v} \in \{0,1\}^n} (-1)^{\underline{u} \cdot \underline{v}} = \begin{cases} 2^n & \text{if } \underline{u} = \underline{0} \\ 0 & \text{otherwise} \end{cases}$$

where $\underline{0}$ denotes the n-bit string $00\ldots0$.

3. *(7 points)* Let U_f denote a quantum black box for f, acting as $U_f|\underline{x}\rangle|y\rangle = |\underline{x}\rangle|y \oplus f(\underline{x})\rangle$ for any $\underline{x} \in \{0,1\}^n$ and $y \in \{0,1\}$. Show that the output of the following circuit is the state $|\underline{s}\rangle(|0\rangle - |1\rangle)/\sqrt{2}$.



4. *(3 points)* What can you conclude about the quantum query complexity of learning s?

Problem 2. *The Fourier transform and translation invariance.* The quantum Fourier transform on n qubits is defined as the transformation

$$|x\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i x y / 2^n} |y\rangle$$

where we identify n-bit strings and the integers they represent in binary. More generally, for any nonnegative integer N, we can define the quantum Fourier transform modulo N as

$$|x\rangle \overset{F_N}{\mapsto} \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i x y / N} |y\rangle$$

where the state space is $\mathcal{C}^N$, with orthonormal basis $\{|0\rangle, |1\rangle, \ldots, |N-1\rangle\}$. Let P denote the unitary operation that adds 1 modulo N: for any $x \in \{0, 1, \ldots, N-1\}$, $P|x\rangle = |x+1 \bmod N\rangle$.

1. *(5 points)* Show that F_N is a unitary transformation.

2. *(7 points)* Show that the Fourier basis states are eigenvectors of P. What are their eigenvalues? (Equivalently, show that $F_N^{-1} P F_N$ is diagonal, and find its diagonal entries.)

3. *(4 points)* Let $|\psi\rangle$ be a state of n qubits. Show that if $P|\psi\rangle$ is measured in the Fourier basis (or equivalently, if we apply the inverse Fourier transform and then measure in the computational basis), the probabilities of all measurement outcomes are the same as if the state had been $|\psi\rangle$.

Problem 3. *Implementing the square root of a unitary.*

1. *(3 points)* Let U be a unitary operation with eigenvalues ± 1. Let P_0 be the projection onto the $+1$ eigenspace of U and let P_1 be the projection onto the -1 eigenspace of U. Let $V = P_0 + iP_1$. Show that $V^2 = U$.

2. *(3 points)* Give a circuit of 1- and 2-qubit gates and controlled-U gates with the following behavior (where the first register is a single qubit):

$$|0\rangle|\psi\rangle \mapsto \begin{cases} |0\rangle|\psi\rangle & \text{if } U|\psi\rangle = |\psi\rangle \\ |1\rangle|\psi\rangle & \text{if } U|\psi\rangle = -|\psi\rangle. \end{cases}$$

3. *(5 points)* Give a circuit of 1- and 2-qubit gates and controlled-U gates that implements V. Your circuit may use ancilla qubits that begin and end in the $|0\rangle$ state.

Problem 4. *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) *(5 points)* Prove that every classical algorithm for solving this problem must make two queries.

(2) *(5 points)* 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) *(5 points)* 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) *(5 points)* 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 5. *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 $\mathrm{span}\{|\phi\rangle, |\psi\rangle\}$, where $\langle\phi|\psi\rangle = e^{i\lambda}\sin(\theta)$ for some $\lambda, \theta \in \mathcal{R}$.

1. *(2 points)* Write the initial state $|\psi\rangle$ in the basis $\{|\phi\rangle, |\phi^\perp\rangle\}$.
2. *(4 points)* Write U_ϕ and V as matrices in the basis $\{|\phi\rangle, |\phi^\perp\rangle\}$.
3. *(4 points)* Let k be a positive integer. Compute $(VU_\phi)^k$.
4. *(4 points)* Compute $\langle\phi|(VU_\phi)^k|\psi\rangle$.
5. *(3 points)* 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 6. *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. *(6 points)* 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. *(6 points)* How should you choose K in part (a) to minimize the number of queries used?
3. *(5 points)* 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.
