Due: April 6th, 2023
Date: March 17, 2023

Assignment 3

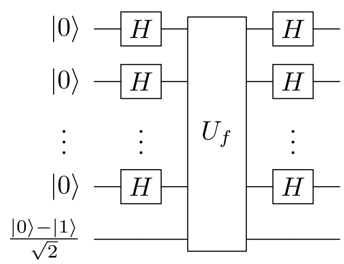
Please submit it electronically to ELMS. This assignment is 6% in your total points. For the simplicity of the grading, the total points for the assignment are 60. Note that we will reward the use of Latex for typesetting with bonus points (an extra 5% of your points).

Problem 1. *The Bernstein-Vazirani problem.*

1. *(3 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. *(4 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. *(4 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. *(1 points)* What can you conclude about the quantum query complexity of learning s?

Problem 2. *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 3. *Simon's algorithm and its extension.* In Simon's problem, recall that we're given oracle access to a function $f : \{0,1\}^n \to \{0,1\}^n$ with the promise that there exists a secret string $s \neq 0^n$ such that $f(x) = f(y)$ if and only if $y = x \oplus s$ for all different $x, y \in \{0,1\}^n$.

1. *(5 points)* Recall the algorithm described during the lecture. Rigorously prove that $O(n)$ repetitions of Simon's algorithm are enough if we want to succeed with $1 - e^{-n}$ probability.

2. *(10 points)* Suppose instead that there are two nonzero secret strings, $s \neq t$, such that $f(x) = f(x \oplus s) = f(x \oplus t) = f(x \oplus s \oplus t)$ for all x. Describe a variation of Simon's algorithm that finds the entire set $s, t, s \oplus t$ in time polynomial in n. When you measure a state in your algorithm, what are the possible results of the measurement? How do you use those measurement results to reconstruct the set $s, t, s \oplus t$?

Problem 4. *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 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. *(3 points)* Write U_ϕ and V as matrices in the basis $\{|\phi\rangle, |\phi^\perp\rangle\}$.

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

4. *(3 points)* Compute $\langle\phi|(VU_\phi)^k|\psi\rangle$.

5. *(2 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 $|\langle\phi|\psi\rangle|$.
