Assignment 3

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

**Problem 1. The Bernstein-Vazirani problem.**

1. *(3 points)* Suppose $f : \{0,1\}^n \to \{0,1\}$ is a function of the form
   
   $$f(x) = x_1s_1 + x_2s_2 + \cdots + x_ns_n \mod 2$$

   for some unknown $s \in \{0,1\}^n$. 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 $u \in \{0,1\}^n$, 
   
   $$\sum_{z \in \{0,1\}^n} (-1)^u \cdot z = \begin{cases} 2^n & \text{if } u = 0 \\ 0 & \text{otherwise} \end{cases}$$

   where $\emptyset$ denotes the $n$-bit string $00\ldots 0$.

3. *(4 points)* Let $U_f$ denote a quantum black box for $f$, acting as $U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$ for any $x \in \{0,1\}^n$ and $y \in \{0,1\}$. Show that the output of the following circuit is the state $|s\rangle (|0\rangle - |1\rangle)/\sqrt{2}$.

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

**Problem 2. One-out-of-four search.** Let $f : \{0,1\}^2 \to \{0,1\}$ be a black-box function taking the value 1 on exactly one input. The goal of the one-out-of-four search problem is to find the unique $(x_1, x_2) \in \{0,1\}^2$ such that $f(x_1, x_2) = 1$.

1. *(2 points)* Write the truth tables of the four possible functions $f$.

2. *(3 points)* How many classical queries are needed to solve one-out-of-four search?

3. *(7 points)* Suppose $f$ is given as a quantum black box $U_f$ acting as

   $$|x_1, x_2, y\rangle \xrightarrow{U_f} |x_1, x_2, y \oplus f(x_1, x_2)\rangle.$$
Determine the output of the following quantum circuit for each of the possible black-box functions $f$:

\[
\begin{array}{c}
|0\rangle \\
|0\rangle \\
|1\rangle \\
\end{array}
\begin{array}{c}
H \\
U_f \\
H \\
\end{array}
\]

4. (3 points) Show that the four possible outputs obtained in the previous part are pairwise orthogonal. What can you conclude about the quantum query complexity of one-out-of-four search?

---

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

1. (3 points) Let $U$ be a unitary operation with eigenvalues $\pm 1$. 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 $V = P_0 + i P_1$. 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. (4 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 referring 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 $A|\psi\rangle = -i|\psi\rangle$. 

2
(3) (5 points) Show how to create the state \( \frac{1}{2}((-i)^{f(00)}|00⟩ + (-i)^{f(01)}|01⟩ + (-i)^{f(10)}|10⟩ + (-i)^{f(11)}|11⟩) \)
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 \( |φ⟩ \) (which may not be a computational basis state). Specifically, \( U_φ|φ⟩ = -|φ⟩ \), and \( U_φ|ξ⟩ = |ξ⟩ \) for any state \( |ξ⟩ \) satisfying \( ⟨φ|ξ⟩ = 0 \).

Consider an algorithm for preparing \( |φ⟩ \) that starts from some fixed state \( |ψ⟩ \) and repeatedly applies the unitary transformation \( VU_ϕ \), where \( V = 2(|ψ⟩⟨ψ| − I) \) is a reflection about \( |ψ⟩ \).

Let \( |φ^⊥⟩ = \frac{e^{-iλ}|ψ⟩ - \sin(θ)|φ⟩}{\cos(θ)} \) denote a state orthogonal to \( |φ⟩ \) in \( \text{span}\{|φ⟩, |ψ⟩\} \), where \( ⟨φ|ψ⟩ = e^{iλ} \sin(θ) \) for some \( λ, θ \in \mathbb{R} \).

1. (2 points) Write the initial state \( |ψ⟩ \) in the basis \( \{ |φ⟩, |φ^⊥⟩ \} \).
2. (3 points) Write \( U_φ \) and \( V \) as matrices in the basis \( \{ |φ⟩, |φ^⊥⟩ \} \).
3. (3 points) Let \( k \) be a positive integer. Compute \( (VU_φ)^k \).
4. (3 points) Compute \( ⟨φ|(VU_φ)^k|ψ⟩ \).
5. (2 points) Suppose that \( |⟨φ|ψ⟩| \) is small. Approximately what value of \( k \) should you choose in order for the algorithm to prepare a state close to \( |φ⟩ \), up to a global phase? Express your answer in terms of \( |⟨φ|ψ⟩| \).