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 $f: \{0, 1\}^n \rightarrow \{0, 1\}$ is a function of the form
   \[ f(x) = x_1 s_1 + x_2 s_2 + \cdots + x_n s_n \mod 2 \]
   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 $0$ denotes the $n$-bit string $00\ldots 0$.

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

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

Problem 2. One-out-of-four search. Let $f: \{0, 1\}^2 \rightarrow \{0, 1\}$ 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 \( f \):

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

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):

\[
|0\rangle|\psi\rangle \rightarrow \begin{cases} 
|0\rangle|\psi\rangle & \text{if } U|\psi\rangle = |\psi\rangle \\
|1\rangle|\psi\rangle & \text{if } U|\psi\rangle = -|\psi\rangle.
\end{cases}
\]

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 \( f : \mathbb{Z}_4 \rightarrow \mathbb{Z}_4 \), 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 \( f : \{0, 1\}^2 \rightarrow \{0, 1\}^2 \). 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 \( A|\psi\rangle = -i|\psi\rangle \).
(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 \(U_\phi\) 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 \(VU_\phi\), 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 \(\lambda, \theta \in \mathbb{R}\).

1. *(2 points)* Write the initial state \(|\psi\rangle\) in the basis \(\{|\phi\rangle, |\phi^\perp\rangle\}\).
2. *(3 points)* Write \(U_\phi\) 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 \(|\langle \phi | \psi \rangle|\).