**Due: April 6th, 2023**
*Date: April 8, 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?

**Answer:** To learn s we can set an input string with all bits set to zero and one bit set to 1 (the ith bit). We can then query the black box with this input string as X. This will compute the ith bit of S as every other bit of S will be zeored out by our input string except for the ith bit which we set to 1. We do this n times for each bit in S and then concat all of the outputs. This results in n queries

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 $00\ldots0$.

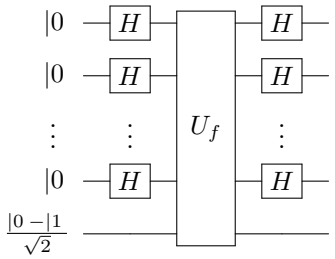
**Answer:**
Case 1: Where U = 0
our summation reduces to $\sum_{\underline{v} \in \{0,1\}^n} (-1)^{\underline{0} \cdot \underline{v}}$ This then reduces to $\sum_{\underline{v} \in \{0,1\}^n} (1)$.Which is == to $2^n$

Case 2: Where U != 0
if U != 0 then at least 1 bit of U = 1. Lets assume without loss of generality that the 1st bit of U is 1. From this assumption we have the summation : of $1 \cdot v_1 + u_2 \cdot v_2 + ... + u_n \cdot v_n$
Now we can represent everything past $v_1$ as A to give us the summation:

$\sum_{\underline{v} \in \{0,1\}^n} (-1)^{v_1 + a}$
Now when we look at the summation if $v_1$ is zero we get $-1^a$ and if $v_1$ is 1 we get $-1^{a+1}$
This reduces to $\sum_{\underline{v} \in \{0,1\}^n} (-1)^a - \sum_{\underline{v} \in \{0,1\}^n} (-1)^a$ which equals 0. As for the second summation we can pull out the $-1^1$

3. *(4 points)* Let $U_f$ denote a quantum black box for $f$, acting as $U_f |\underline{x}\,|y\, = |\underline{x}\,|y \oplus f(\underline{x})\,$ for any $\underline{x} \in \{0,1\}^n$

and $y \in \{0,1\}$. Show that the output of the following circuit is the state $|\underline{s}\,(|0\rangle - |1\rangle)/\sqrt{2}$.




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

---

**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.

**Answer:** f(x) = ax + b for [0,1,2,3]
Therefore, f(0) = b and f(1) = a + f(0) we know b from our first query. second query solves for a as f(1) - f(0) should give us a. Hence, 2 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 $A\,|\psi\rangle = -i\,|\psi\rangle$.

**Answer:**

$$|\psi\rangle = \begin{pmatrix} 1/2 \\ i/2 \\ i^2/2 \\ i^3/2 \end{pmatrix}$$

$$\mathrm{A}|\psi\rangle = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1/2 \\ i/2 \\ i^2/2 \\ i^3/2 \end{pmatrix} = \begin{pmatrix} -i/2 \\ 1/2 \\ i/2 \\ -1/2 \end{pmatrix} = \text{-i} \begin{pmatrix} 1/2 \\ i/2 \\ i^2/2 \\ i^3/2 \end{pmatrix} = -i\,|\psi\rangle$$

*(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.)
**Answer:**
First, you apply H gate to the 00 bits to get $\frac{1}{\sqrt{4}}\sum_{\underline{x}\in\{0,1\}^2}|x\rangle|\psi\rangle = 1/4\sum_{\underline{x}\in\{0,1\}^2}|x\rangle(|00\rangle + i|01\rangle + i^2|10\rangle + i^3|11\rangle$

Then apply $U_f$ :
$1/4\sum_{\underline{x}\in\{0,1\}^2}|x\rangle(f(x)|00\rangle + i(f(x)+|01\rangle) + i^2(f(x)+|10\rangle) + i^3(f(X)+|11\rangle)$

This can be reduced to:
$\frac{1}{4}\sum_{x\in\{0,1\}^2}|x\rangle(-i)^{f(x)}|\psi\rangle$
Which can be reduced to:

$\frac{1}{2}\sum_{x\in\{0,1\}^2}|x\rangle(-i)^{f(x)}\bigotimes|\psi\rangle = 1/2((-i)^{f(00)}|00\rangle + (-i)^{f(01)}|01\rangle + (-i)^{f(10)}|10\rangle + (-i)^{f(11)|11\rangle)}\bigotimes 1/2|\psi\rangle$

*(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.)
After applying $U_f weget$,$1/2((-i)^{f(00)}|00\rangle + (-i)^{f(01)}|01\rangle + (-i)^{f(10)}|10\rangle + (-i)^{f(11)|11\rangle)}$
Reduces to f(00) = 0, f(01) = a, f(10) = 2a, f(11) = 3a
Reduce to: $1/2(|00\rangle + (-i)^a|01\rangle + (-i)^{2a}|10\rangle + (-i)^{3a}|11\rangle$

Then we apply the Hadamard gate to the first bit and reduce to get the following cases:

$a = 0 : \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$
$a = 1 : \frac{1}{\sqrt{2}}(|10\rangle - i|11\rangle)$
$a = 2 : \frac{1}{\sqrt{2}}(|00\rangle - |01\rangle)$
$a = 3 : \frac{1}{\sqrt{2}}(|10\rangle + i|11\rangle)$

We then apply the controlled S gate to the first bit and then the hardamard gate to the second bit to get:

$a = 0 : |00\rangle$
$a = 1 : |11\rangle$
$a = 2 : |01\rangle$
$a = 3 : |11\rangle$

Therefore a can be retrieved from one quantum query

---

**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.

   **Answer:**
   When we run simon's algorithm we have two different cases (where s = $0^n$ and when s !=$0^n$
   For these two cases we run the algorithm n-1 times to get n-1 strings such that $y1 \cdots s = 0 .....y_{n-1} \cdot s = 0$

We now have a system of n-1 linear equations with n unkown bits of the string s.
If the strings are linearly independent we solve the system to a get a candidate solution s' != $0^n$ and test that $f(0^n) = f(s')$. If $f(0^n) = f(s')$, we know that s' = s and we are done. Otherwise, we are in the second case where s = $0^n$. We repeat the process 4n times and find the probability of not finding a linearly independent set is less than $(1 - 1/4)^4 n < e^{-n}$ there fore our probability of success is $1 - e^{-n}$ and our time complexity is O(n) because of our 4n iterations.

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 $s, t, s \oplus t$?

Since s and t are nonzero we follow the original algorithm until we get the probability to measure a given string to be $(\frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{xy} |f(x)\rangle)^2$

Let A be the range of f. If z exists in A then there must be 4 distinct strings $x_z, x'_z, x''_z, x'''_z \in 0, 1^n$ such that f($x_z$) = f($x'_z$) = z and $x_z \bigoplus x'_z = s, x_z \bigoplus x''_z = t, x_z \bigoplus x'''_z = s \bigoplus t$.
From this we get $||\frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{xy} |f(x)\rangle)^2||^2$
$= ||\frac{1}{2^n} \sum_{x \in \{a\}} (-1)^{x_z \cdot y} (1 + (-1)^{s \cdot y} + (-1)^{t \cdot y} + (-1)^{(s \cdot y) \bigoplus (t \cdot y) |z\rangle}||^2$

$$= \begin{cases} 2^{-(n-2)} & \text{if } s \cdot y = 0 \text{ and } t \cdot y = 0 \\ 0 & \text{if } s \cdot y = 0 \text{ and } t \cdot y = 1 \\ 0 & \text{if } s \cdot y = 10 \text{ and } t \cdot y = 1 \\ 0 & \text{if } s \cdot y = 10 \text{ and } t \cdot y = 0 \end{cases}$$

With this we can find s,t, and $s \bigoplus t$. with a very low probability of failure, so we can follow the same processed in the original Simon's algorithm.

---

**Problem 4.** *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 $\phi|\xi\rangle = 0$.

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 $\phi|\psi\rangle = e^{i\lambda} \sin(\theta)$ for some $\lambda, \theta \in$.

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

   **Answer:** $|\psi\rangle = \frac{\cos\theta|\phi^\perp\rangle + \sin\theta|\phi\rangle}{e^{-i\lambda}}$

2. *(3 points)* Write $U_\phi$ and $V$ as matrices in the basis $\{|\phi\rangle, |\phi^\perp\rangle\}$.

   **Answer:**
   $U_\phi = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$
   $V = \begin{pmatrix} -\cos 2\theta & \cos\theta \sin\theta \\ \cos\theta \sin\theta & \cos 2\theta \end{pmatrix}$

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

   **Answer:**

   $$VU_\phi = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ -\sin 2\theta & \cos 2\theta \end{pmatrix}$$

   Now to get $(VU_\phi)^k$ we need to diagonalize the matrix, giving us:
   $SJ^kS^{-}1 =$

   $$\begin{pmatrix} i & -i \\ 1 & 1 \end{pmatrix} \begin{pmatrix} e^{i2\theta k} & 0 \\ 0 & e^{-i2\theta k} \end{pmatrix} \begin{pmatrix} -i/2 & 1/2 \\ i/2 & 1/2 \end{pmatrix}$$

   Note: we can simplify J by using euler's formula/trig identities

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

   **Answer:**
   $\phi|(VU_\phi)^k|\psi = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} i & -i \\ 1 & 1 \end{pmatrix} \begin{pmatrix} e^{i2\theta k} & 0 \\ 0 & e^{-i2\theta k} \end{pmatrix} \begin{pmatrix} -i/2 & 1/2 \\ i/2 & 1/2 \end{pmatrix} \begin{pmatrix} \sin\theta e^{i\lambda} \\ \cos\theta e^{i\lambda} \end{pmatrix}$

   After simplifying this expression you get to:

   $\frac{ie^{i\lambda}}{2}(e^{i\theta+i2k\theta} - e^{-i\theta-i2k\theta})$

5. *(2 points)* Suppose that $|\phi|\psi\,|$ 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 $|\phi|\psi\,|$.

   **Answer:**

   $|\phi|\psi\,|$ is small that means $|\psi\rangle$ is close to $|\phi^\perp\rangle$ and is $\theta$ away.we need to rotate the initial vector $\frac{\pi}{2}$ closer to $|\phi\rangle$. Each rotation rotates the vector by $2\theta$ degrees

   $k * 2\theta + \theta = \frac{\pi}{2}$
   $k = \frac{\pi}{4}$

---