CS419/939: Quantum Computing – Assignment 3

LaTeX submissions are preferred; handwritten submissions are acceptable, so long as your handwriting is clear. You may work in groups but you must write up your solutions individually. Questions marked with (*) are optional: you will get feedback but they do not count towards the final mark. You do not need to show your work unless the question asks you to, but it is always a good idea to do so since you may receive part marks for correct working even if you get the wrong answer.

Problem 1

(20 points) You are given a function $f\colon \{0,1\}^n \to \{0,1\}$ such that $f(x) = \langle x, s\rangle \bmod 2$ for some unknown $s \in \{0,1\}^n$.

1. Explain how to find s using n *classical* queries to f. (You do not need to draw a circuit.)
2. Express $H^{\otimes n}\,|s\rangle$ in the computational basis.
3. Compute $H^{\otimes n}\,|f\rangle$, where $|f\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}\,|x\rangle$. (Hint: recall that H is self-adjoint.)
4. Show how to find s using a single quantum query to f (i.e., a single U_f gate).

Problem 2

(20 points) Recall that Grover's search algorithm proceeds by applying unitary operators U_f and D in an alternating fashion, where $D = 2\,|+_n\rangle\langle+_n| - I$ is the "diffusion" operator that maps $|+_n\rangle = |+\rangle^{\otimes n}$ to itself and $|\psi\rangle$ to $-|\psi\rangle$ for all $|\psi\rangle$ orthogonal to $|+_n\rangle$. In this problem you will show how to implement D as a circuit. You may use standard gates ($X, Z, H, \mathsf{CNOT}, \mathsf{CCNOT}$) and ancilla qubits.

1. Suppose that you also have access to the n-qubit gate $D_0 = 2\,|0^n\rangle\langle 0^n| - I$. Show how to use this (along with standard gates) to build a circuit for D.
2. Show how to build a circuit for D_0. (Hint: what does D_0 do to each computational basis state $|x\rangle$?)

Problem 3

(30 points)

1. Open Circuit 3.3 in IBM Quantum Composer. This circuit computes the unitary $U\,|a\rangle = f(a)\,|a\rangle$ for a function $f\colon \{0,1\}^2 \to \{1,-1\}$. Write down the truth table of f.
2. Add gates to the circuit so that it generates the state $|f\rangle = \frac{1}{2}\sum_{x\in\{0,1\}^2} f(x)\,|x\rangle$.
3. We can view f as a function $\{0,1,2,3\} \to \{1,-1\}$ by identifying each $j \in \{0,1,2,3\}$ with its binary representation `a[1]a[0]`, so $j = 2$`a[1]` $+$ `a[0]`. Write down the truth table of f viewed as a function $\{0,1,2,3\} \to \{1,-1\}$.

4. Compute (by hand) the 4-point discrete Fourier transform $\hat{f}$ of f, given by

$$\hat{f}(k) = \frac{1}{2}\sum_{j=0}^{3} f(j) \cdot i^{jk}$$

for each $k \in \{0,1,2,3\}$, where $i = \sqrt{-1}$ is the complex unit.

5. Write down the state $\left|\hat{f}\right\rangle$.

6. In IBM Quantum Composer, implement the 4-point Quantum Fourier Transform to compute the state $\left|\hat{f}\right\rangle$. To obtain the controlled-$\sqrt{Z}$ gate described in the lecture notes, drag a P-gate on to the appropriate wire; you should see `pi/2` appear on the gate label. Next, click the P-gate, click the Edit button, and then click "Add control". You can then choose which wire you want to be the control. Include a screenshot of your circuit in your answer.

7. Check the box labelled "Phase angle" in the "Q-sphere" view. Include a screenshot of this view in your answer. This view shows you the components of the final superposition along with their phase angle; for example, a ray labelled "$|01\rangle$ $\pi/2$" means that the final superposition has a component $e^{i\pi/2}|01\rangle$. Explain what you see in this view by referring to your answer to (4).

NOTE: Qiskit has a confusing qubit ordering convention. If your output looks different from what you expect, check first if swapping the qubit order would fix things.

Problem 4

(30 points) Let $f\colon \{0,1\}^n \to \{0,1\}^{n/2}$ be a balanced function: that is, for every $y \in \{0,1\}^{n/2}$, $|f^{-1}(y)| = 2^{n/2}$, where $f^{-1}(y) = \{x : f(x) = y\}$. Your goal is to use queries to f to find a *collision*: any pair (x, x') where $x \neq x'$ and $f(x) = f(x')$.

1. Give a *classical deterministic* query algorithm for finding a collision, and argue briefly that your algorithm is optimal.

2. (*) Give a *classical randomized* query algorithm that finds a collision with 99% probability using $O(2^{n/4})$ queries. (Hint: consider the problem of throwing q balls into N bins; what is the probability that some bin contains two balls? You may find the inequality $1 - t \leq e^{-t}$ helpful.) Argue that this algorithm is asymptotically optimal.

3. In this exercise we will design a quantum query algorithm that finds a collision with fewer queries.

   (a) Let $X \subseteq \{0,1\}^n$ and $S \subseteq \{0,1\}^{n/2}$. Describe a *classical* circuit of size $O((|X| + |S|) \cdot n)$, that makes a single classical query to f, which computes the function $g_{X,S}\colon \{0,1\}^n \to \{0,1\}$, where

$$g_{X,S}(x) = \begin{cases} 1 & \text{if } x \notin X \text{ and } f(x) \in S, \text{ or} \\ 0 & \text{otherwise.} \end{cases}$$

   (b) Give a lower bound on $|g_{X,S}^{-1}(1)|$ in terms of $|X|$ and $|S|$.

   (c) Using part (a), argue that there is a *quantum* circuit, containing two U_f-gates, that computes the unitary $U_{X,S}$ mapping $|x, b\rangle$ to $|x, b \oplus g_{X,S}(x)\rangle$ for all $x \in \{0,1\}^n, b \in \{0,1\}$.

   (d) Design an algorithm which finds a collision with 99% probability using $O(2^{n/6})$ quantum queries. You may use the following fact without proof: there is a quantum query algorithm $\mathcal{A}$ which, for any $g\colon \{0,1\}^n \to \{0,1\}$, outputs x such that $g(x) = 1$ with 99.9% probability using $O(\sqrt{\frac{2^n}{|g^{-1}(1)|}})$ queries to g (i.e., U_g gates).
   (Hint: start by querying f on all $x \in X$ for an arbitrary set $X \subseteq \{0,1\}^n$ of size $2^{n/6}$.)

(Note: for this question you do not have to *draw* circuits unless it is helpful; a clear description will suffice.)