**ASSIGNMENT 4** CMSC/PHYS 457 (Spring 2019)

Due by 12:30 pm on Thursday, April 4. Submit your solutions in PDF via Gradescope. Please include a list of students in the class with whom you discussed the problems, or else state that you did not discuss the assignment with your classmates.

1. *The Bernstein-Vazirani problem.*

   (a) [2 points] Suppose $f : \{0,1\}^n \to \{0,1\}$ is a function of the form

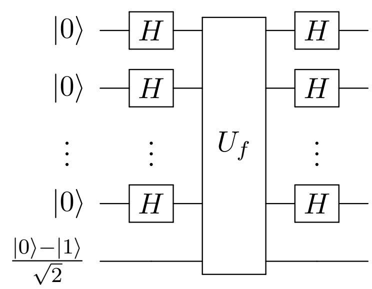
   $$f(x) = x_1 s_1 + x_2 s_2 + \cdots + x_n s_n \bmod 2$$

   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?

   (b) [3 points] Prove that for any $n$-bit string $u \in \{0,1\}^n$,

   $$\sum_{v \in \{0,1\}^n} (-1)^{u \cdot v} = \begin{cases} 2^n & \text{if } u = 00\ldots0 \\ 0 & \text{otherwise.} \end{cases}$$

   (c) [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 $|s\rangle(|0\rangle - |1\rangle)/\sqrt{2}$.




   (d) [1 point] What can you conclude about the quantum query complexity of learning $s$?

2. *A fast approximate QFT.*

   (a) [2 points] In class, we saw a circuit implementing the $n$-qubit QFT using Hadamard and controlled-$R_k$ gates, where $R_k|x\rangle = e^{2\pi i x/2^k}|x\rangle$ for $x \in \{0,1\}$. How many gates in total does that circuit use? Express your answer both exactly and using $\Theta$ notation. (Recall that we say $f(n) \in \Theta(g(n))$ if $f(n) \in O(g(n))$ and $g(n) \in O(f(n))$.)

   (b) [3 points] Let $\mathrm{C}R_k$ denote the controlled-$R_k$ gate, with $\mathrm{C}R_k|x,y\rangle = e^{2\pi i xy/2^k}|x,y\rangle$ for $x, y \in \{0,1\}$. Show that $E(\mathrm{C}R_k, I) \le 2\pi/2^k$, where $I$ denotes the $4 \times 4$ identity matrix, and where $E(U,V) = \max_{|\psi\rangle} \|U|\psi\rangle - V|\psi\rangle\|$. You may use the fact that $\sin x \le x$ for any $x \ge 0$.

   (c) [5 points] Let $F$ denote the exact QFT on $n$ qubits. Suppose that for some constant $c$, we delete all the controlled-$R_k$ gates with $k > \log_2(n) + c$ from the QFT circuit, giving a circuit for another unitary operation, $\tilde{F}$. Show that $E(F, \tilde{F}) \le \epsilon$ for some $\epsilon$ that is independent of $n$, where $\epsilon$ can be made arbitrarily small by choosing $c$ arbitrarily large. (Hint: Use equation 4.3.3 of KLM.)

   (d) [1 point] For a fixed $c$, how many gates are used by the circuit implementing $\tilde{F}$? It is sufficient to give your answer using $\Theta$ notation.

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

   (a) [2 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 $V = P_0 + iP_1$. Show that $V^2 = U$.

   (b) [2 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):

$$|0\rangle|\psi\rangle \mapsto \begin{cases} |0\rangle|\psi\rangle & \text{if } U|\psi\rangle = |\psi\rangle \\ |1\rangle|\psi\rangle & \text{if } U|\psi\rangle = -|\psi\rangle. \end{cases}$$

   (c) [4 points] Give a circuit of 1- and 2-qubit gates and controlled-$U$ gates that implements $V$, and show that it has the desired behavior. Your circuit may use ancilla qubits that begin and end in the $|0\rangle$ state.

4. *Fourier transforms and composite systems.* Recall that the quantum Fourier transform on $n$ qubits is defined as the transformation

$$|x\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i x y/2^n} |y\rangle$$

where we identify $n$-bit strings and the integers they represent in binary. More generally, for any nonnegative integer $N$, we can define the quantum Fourier transform modulo $N$ as the transformation

$$|x\rangle \overset{F_N}{\mapsto} \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i x y/N} |y\rangle$$

where the state space is $\mathbb{C}^N$, with orthonormal basis $\{|0\rangle, |1\rangle, \ldots, |N-1\rangle\}$.

   (a) [3 points] Show that $F_N$ is a unitary transformation.

   (b) [1 point] Write $F_5$ in matrix form.

   (c) [3 points] Show that $F_2 \otimes F_3 \cong F_6$, where $\cong$ denotes equivalence up to a permutation of the rows and columns (not necessarily the same permutation for the rows as for the columns).

   (d) [3 points] Show that $F_N \otimes F_M \cong F_{NM}$ does not hold in general.

   (e) [5 bonus points] Show that if $N$ and $M$ are relatively prime, then $F_N \otimes F_M \cong F_{NM}$.

5. *Factoring 21.*

   (a) [2 points] Suppose that, when running Shor's algorithm to factor the number 21, you choose the value $a = 2$. What is the order $r$ of $a \bmod 21$?

   (b) [3 points] Give an expression for the probabilities of the possible measurement outcomes when performing phase estimation with $n$ bits of precision in Shor's algorithm.

   (c) [2 points] In the execution of Shor's algorithm considered in part (a), suppose you perform phase estimation with $n = 7$ bits of precision. Plot the probabilities of the possible measurement outcomes obtained by the algorithm. You are encouraged to use software to produce your plot.

   (d) [2 points] Compute $\gcd(21, a^{r/2} - 1)$ and $\gcd(21, a^{r/2} + 1)$. How do they relate to the prime factors of 21?

   (e) [3 points] How would your above answers change if instead of taking $a = 2$, you had taken $a = 5$?