PHYS 7895 Spring 2014
Theory of Quantum Computation
Homework 3

Due Friday 4 April 2014, by 3pm in Nicholson 447
You are allowed to work with others as long as you write down who your collaborators are. The expectation is that this system will not be abused (i.e., you try all the problems first on your own and then discuss with collaborators after doing so.) Any detection of copying of solutions will be penalized with no credit for the assignment. Any late assignments will be penalized in the amount of 25% per day late.

1. Simon generalized. Suppose you are given a 4-to-1 function $f : \{0,1\}^n \to \{0,1\}^m$ with the promise that there exist strings $a, b \in \{0,1\}^n \backslash \{0^n\}$ with $a \neq b$ such that $f(x) = f(x \oplus a) = f(x \oplus b) = f(x \oplus a \oplus b)$. Give an efficient quantum algorithm to find a and b.

2. Consider the following problem: You are given $f : \{0,1\}^n \to \{0,1\}$ an unknown function implemented as a black box. You are also promised that f has the form $f(x) = x \cdot s$ for some $s \in \{0,1\}^n$ with the dot product taken mod 2. Find s. Show that there is a gap between the classical and quantum query complexities of the problem:

   (a) How many queries does the best deterministic classical algorithm require in the worst case? Explain.

   (b) Show that in order to find s with constant probability, any randomized classical algorithm will require $\Omega(n)$ queries.

   (c) Find a quantum algorithm that solves the problem using a single query.

3. *Period finding and NP-completeness.* Let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean formula. Determining whether there exists $(x_0, \ldots, x_n) \in \{0,1\}^n$ such that $f(x_1, \ldots, x_n) = 1$ is the canonical NP-complete problem known as SAT. The problem remains NP-hard even with the promise that there is at most one satisfying assignment. Now let $g : \{0,1\}^{n+m} \to \{0,1\}$ be given by $g(x_0, \ldots, x_{m+n-1}) = f(x_0, \ldots, x_{n-1})$. Regard $(x_{m+n-1}, \ldots, x_0)$ as the integer $x = \sum_{j=0}^{m+n-1} 2^j x_j$. Note that if f is not satisfiable, then g is periodic with period one. Now suppose that f is satisfiable with only one satisfying assignment. Then g will be periodic with period $2n$. Will the quantum period finding algorithm distinguish these two possibilities in polynomial time? Explain why or why not.

4. *Hidden linear function.* Let h be a function from $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_N$ defined by $h(x; y) = x + ay$ mod N, with a unknown, and let π be an unknown permutation of $\mathbb{Z}_N$. Suppose you have a quantum black box U_f capable of evaluating the function $f = \pi \circ h$, meaning that $U_f|x\rangle|y\rangle|0\rangle = |x\rangle|y\rangle|f(x, y)\rangle$.

   (a) Show how to place this task in the hidden subgroup framework.

   (b) Find a polynomial time quantum algorithm to determine a mod N. You may assume for simplicity that $N = 2^n$ is a power of two.

5. Quantum computing with poor initialization. One of the requirements for quantum computing is the ability to prepare the initial state of the computer to be a computational basis state encoding the input plus potentially some ancilla registers set to a fixed state such as $|0\rangle$. Perhaps surprisingly, quantum computers can still do interesting things even when it is not possible to initialize them very well. (That is the case for liquid state NMR experiments, for example.) As a toy model of that situation, suppose that you have many qubits at your disposal but that you can only initialize one of them to the state $|0\rangle$. The others start in a uniformly random state: if there are k of them, the 2×2^k real and imaginary coefficients of the state vector are chosen to give a uniformly random point on the unit sphere.

   Given access to a controlled-U gate, where U is a unitary operator acting on k qubits, design a procedure to estimate $\mathrm{Tr}\{U\} = 2k$, which is a complex number of modulus at most 1. More specifically:

   (a) Design a circuit for which the probability of a fixed measurement outcome has the form $A + B\,\mathrm{Re}\{\mathrm{Tr}\{U\}\}/2^k$ with A and B constants independent of k. Repeating the circuit will therefore lead to an accurate estimate of $\mathrm{Re}\{\mathrm{Tr}\{U\}\}/2^k$. (You may use the fact that if $|\varphi\rangle$ is a uniformly random state on k qubits, then $\mathbb{E}\{|\langle\varphi|\psi\rangle|^2\} = 1/2^k$ for any fixed state $|\psi\rangle$ but you might get bonus points if you can prove it.)

   (b) Do the same for $\mathrm{Im}\{\mathrm{Tr}\{U\}\}/2k$.