PHYS 7895 Spring 2014
Theory of Quantum Computation
Homework 2

Due Friday 7 March 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. Accuracy of Unitary Approximations:

   (a) Suppose that $\widetilde{U}$ realizes U with accuracy δ:
   $$\left\| U - \widetilde{U} \right\|_\infty \leq \delta.$$
   Prove that the inverse of U is realized with the same accuracy by the inverse of $\widetilde{U}$.

   (b) The diamond norm characterizes the ultimate distinguishability of one quantum channel from another. It is defined as
   $$\left\| \mathcal{N} - \mathcal{M} \right\|_\diamond \equiv \sup_d \max_{\rho_{R_d A}} \left\| (\mathrm{id}_{R_d} \otimes \mathcal{N})(\rho_{R_d A}) - (\mathrm{id}_{R_d} \otimes \mathcal{M})(\rho_{R_d A}) \right\|_1, \tag{1}$$
   where d is the dimension of the auxiliary register R_d and the optimization is over all density operators $\rho_{R_d A}$ on the auxiliary system R_d and the channel input A. It is well known that this is equal to
   $$\left\| \mathcal{N} - \mathcal{M} \right\|_\diamond = \max_{\psi_{RA}} \left\| (\mathrm{id}_{R} \otimes \mathcal{N})(\psi_{RA}) - (\mathrm{id}_{R} \otimes \mathcal{M})(\psi_{RA}) \right\|_1, \tag{2}$$
   where the maximization is over pure entangled states on an auxiliary system R and the channel input system A, with R not needing to be any larger than A. Prove that
   $$\left\| \mathcal{U}_1 - \mathcal{U}_2 \right\|_\diamond \leq 2 \left\| U_1 - U_2 \right\|_\infty,$$
   where the action of $\mathcal{U}_i$ on an input density operator σ is given by $\mathcal{U}_i(\sigma) = U_i \sigma U_i^\dagger$. From this, we can conclude that the operator norm is a good measure of distinguishability for unitary operations. (Bonus: Prove that (2) follows from (1).)

2. Classical reversible computation:

   (a) Prove that it is impossible for CNOT gates alone to realize universal reversible classical computation. (Consider a counting argument, i.e., all of the circuits on n bits that can be realized with CNOTs alone, versus the total number of possible functions.)

   (b) Prove that a Toffoli gate is universal for classical computation.

3. Given is a quantum channel that acts on n input qubits and produces m output qubits. Describe how to approximate this channel with a unitary circuit with elements chosen from a universal gate set and up to an accuracy ε in the diamond norm. (*Hint: Consider the Stinespring dilation theorem.*)

4. Deutsch-Jozsa: Let f be a function promised to be either constant or balanced (as in the setting of the Deutsch-Jozsa algorithm).

   (a) Show that a probabilistic classical algorithm making two evaluations of f can with probability at least $2/3$ correctly determine whether f is constant or balanced. (*Hint: Your guess does not need to be a deterministic function of the results of the two queries. Your result should not assume any particular a priori probabilities of having a constant or balanced function.*)

   (b) Show that a probabilistic classical algorithm that makes $O(n)$ queries can with probability at least $1-2^{-n}$ correctly determine whether f is constant or balanced. (*Hint: Use the Chernoff bound.*)

5. Let $N = 2^n$. Suppose that someone has given you the unknown state $\sum_{x\in\mathbb{Z}_N} \alpha_x|x\rangle$ and that you would like to draw a sample from the distribution over $y \in \mathbb{Z}_N$ given by $\frac{1}{N}|\sum_x \alpha_x\omega^{xy}|$ where $\omega = \exp\{2\pi i/N\}$.

   Using the quantum Fourier transform, this can be done using $O(n^2)$ gates and $O(n)$ measurements. Design a quantum circuit to do this with $O(n^2)$ single qubit gates, $O(n)$ measurements and no multiqubit gates. Your circuit will need to be adaptive in the sense that you will need to perform intermediate measurements, with the choice of subsequent gates depending on the measurement outcome. In case you had not noticed, this result is pretty amazing: the absence of multiqubit gates means there is no need for any interaction between registers in the quantum computer!

   Hints: Remember that the source and target registers are interchangeable for controlled-Z. Does something similar apply to the controlled-R_k gates in the QFT? Also, start small. The statement is trivial for $N = 2$ so start with $N = 4$.

6. Recall that the measurement of the observable

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1|$$

   consists of performing the measurement defined by the projection operators $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$. In general, if A is an observable of arbitrary size with eigenvalues ± 1 then it can be written as $A = P_+ - P_-$ where $P_\pm$ are projectors onto the ± 1 eigenspaces of A.

   (a) Show that any such A is unitary.

   (b) Suppose that you have access to the controlled-A circuit element. Design a quantum circuit that will perform a measurement of the observable A using only one use of controlled-A. *Hint: Phase estimation.*

   In more detail, suppose that A acts on n qubits. You should design a circuit acting on some number $m = n + k$ qubits where n are considered the input to be measured and the other k are ancilla starting in a fixed state, say $|0\rangle$. The circuit can contain the usual circuit elements plus the controlled-A gate and should contain a measurement gate acting on a single qubit. The circuit measurement should simulate the statistics of a measurement of A in the sense that for any input $|\psi\rangle$, outcome 0 should occur with probability $\langle\psi|P_+|\psi\rangle$ and 1 with probability $\langle\psi|P_-|\psi\rangle$. Moreover, the circuit should reproduce the post-measurement state: given that outcome 0 has occurred, some subset of the m qubits should be in the state proportional to $P_+|\psi\rangle$. Likewise for outcome 1 and $P_-|\psi\rangle$.

(c) Let $B = Q_+ - Q_-$ be another observable with ±1 eigenvalues such that $[A, B] = 0$. What measurement is performed if the controlled-A of part (b) is replaced by controlled-AB?

(d) Design a circuit that will measure the observable $P_+Q_+ - (P_+Q_- + P_-Q_+ + P_-Q_-)$ using at most one use each of controlled-A and controlled-B. Your circuit should reproduce the outcome statistics of the measurement but need not generate the correct post-measurement state.

(e) Redo part (d) but this time design a circuit that will reproduce the measurement outcome statistics and the correct post-measurement state. You may use controlled-A and controlled-B twice each (and will need to).

Hint: One circuit that does this is a palindrome: the gates are the same reading start-to-end and end-to-start. The main difficulty is that you need to make sure that you do not learn more than is absolutely necessary to perform the desired measurement. It will be necessary to uncompute unnecessary junk, hence the palindromic circuit.