QIC710/CS667/CO681/PH767/AM871 Introduction to Quantum Information Processing (F12)

Assignment 2
Due date: October 9, 2012

1. **Can more entanglement improve superdense coding?** Recall the *superdense coding* protocol that enables Alice to convey two classical bits to Bob by sending just one qubit (assuming that Bob sends Alice a qubit beforehand). In this protocol, Bob creates the two-qubit state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and sends Alice the first qubit. Then Alice performs one of four unitary operations on her qubit (that depends on her two classical bits) and sends the qubit back to Bob, who can now perfectly distinguish between the four possible cases.

   Suppose that Bob can use more entanglement, say any n-qubit state ($n > 2$) of the form

   $$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle, \tag{1}$$

   where the amplitudes α_x are arbitrary subject to $\sum_{x \in \{0,1\}^n} |\alpha_x|^2 = 1$. Consider any protocol where the goal is for Alice to convey some $k \in \{1, 2, \ldots, m\}$ to Bob by the following approach. Bob constructs the state $|\psi\rangle$, sends its first qubit to Alice, who then performs a one-qubit unitary U_k (from a list of unitary operations $U_1, U_2, \ldots, U_m$) on her qubit and then sends the qubit back to Bob, who now has to determine what k is (without error). Clearly, this can be done when $m = 4$ (by superdense coding). Can this be done for $m = 5$ (which corresponds to more than two bits of information)? Prove that in fact it is impossible whenever $m > 4$. (Hint: you use the fact that, for a set of quantum states to be perfectly distinguishable from each other, they must be mutually orthogonal.)

2. **Distinguishing between pairs of unitaries.** In each case, you are given a black box gate that computes one of the two given unitaries, but you are not told which one. It is chosen uniformly: each is selected with probability $\frac{1}{2}$. Your goal is to guess which of the two unitaries it is with as high a probability as you can. To help you do this, you can create any one-qubit quantum state, apply the black box gate to this qubit, and then measure the answer in some basis (that is, you can apply a unitary of your choosing and then measure in the computational basis). You can only use the black-box gate once.

   For example, consider the case where the two unitaries are $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. In this case, setting the initial state to $|+\rangle$, applying the black-box unitary, followed by H and measuring yields 0 in the first case and 1 in the second case. So this is a perfect distinguishing procedure (it succeeds with probability 1).

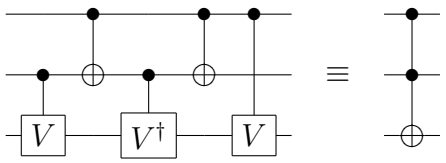
   (a) $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ (the latter is a rotation by $\pi/4$).

   (b) I and $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$.

   (c) I and H.

   (Hint: in two out of the above three cases there is a perfect distinguishing procedure.)

3. **Constructing a Toffoli gate out of two-qubit gates.** The Toffoli gate (controlled-controlled-NOT) is a 3-qubit gate, and here we show how to implement it with 2-qubit gates. The construction is given by the following quantum circuit



where

$$V = \frac{1}{\sqrt{2}} \begin{pmatrix} \omega & \overline{\omega} \\ \overline{\omega} & \omega \end{pmatrix}, \quad \text{with } \omega = e^{i\pi/4} \text{ and } \overline{\omega} = e^{-i\pi/4} \text{ } (\omega\text{'s conjugate}).$$

We *could* verify this by multiplying 8×8 matrices; however, we take a simpler approach.

(a) Show that $V^2 = X$ (this means V is a square root of NOT).

(b) Prove each of the following, where $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is an arbitrary 1-qubit state:

i. The circuit maps $|00\rangle|\psi\rangle$ maps to $|00\rangle|\psi\rangle$.

ii. The circuit maps $|01\rangle|\psi\rangle$ maps to $|01\rangle|\psi\rangle$.

iii. The circuit maps $|10\rangle|\psi\rangle$ maps to $|10\rangle|\psi\rangle$.

iv. The circuit maps $|11\rangle|\psi\rangle$ maps to $|11\rangle V^2|\psi\rangle$.

(c) Based on parts (a) and (b), write down the 8×8 unitary matrix that the above circuit computes.

4. **Determining a hidden "dot product vector".** Consider the problem where one is given black-box access to a function $f : \{0,1\}^n \to \{0,1\}$ such that $f(x) = a \cdot x$, where $a \in \{0,1\}^n$ is unknown. (Here $a \cdot x = a_1x_1 + a_2x_2 + \cdots + a_nx_n \bmod 2$, the dot product of a and x in modulo-2 arithmetic.) The goal is to determine the n-bit string a.

(a) Give a classical (i.e., not quantum) algorithm that solves this problem with n queries.

(b) Show that no classical algorithm can solve this problem with fewer than n queries. (Hint: you may use the fact that a system of k linear equations in n variables cannot have a unique solution if $k < n$, even in the setting of modulo-2 arithmetic.)

(c) Here and in part (d) we'll construct a quantum algorithm that solves this problem with a single query to f. The first step is to construct the $(n+1)$-qubit state $|0\rangle|0\rangle \cdots |0\rangle|1\rangle$ and apply a Hadamard operation to each of the $n+1$ qubits. The second step is to query the oracle for f. What is the state after performing these two steps?

(d) Describe a measurement on the state obtained from part (c) whose result is the bits $a_1a_2 \ldots a_n$. (Hint: the state from part (c) is not entangled; it can be expressed as a tensor product of 1-qubit states, and it might clarify matters if you express it in such a factorized form.)

5. **Entanglement among three qubits.** Suppose that Alice, Bob and Carol each possess a qubit and that the joint state of their three qubits is $|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$.

   (a) Suppose that Carol leaves the scene, taking her qubit with her, and without communicating with either Alice or Bob. Consider the two-qubit state of Alice and Bob's qubits. Is this state equivalent to $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$? Justify your answer.

   (b) Suppose again that Carol leaves the scene, taking her qubit with her, but she is allowed to send one classical bit to Alice. Carol wants to help Alice and Bob transform their state into the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ (and without Alice and Bob having to send any messages between each other). The framework is as follows:

      i. Carol applies some unitary operation U to her qubit, and then measures the qubit, yielding the classical bit b.

      ii. Carol sends just the classical bit b to Alice.

      iii. Alice applies a unitary operation, depending on b, to her qubit. In other words, Alice has two unitary operations V_0 and V_1, and she applies V_b to her qubit.

      At the end of this procedure, the two-qubit state of state of Alice and Bob's qubits should be $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Explain how to make this procedure work.

   (c) Is it possible for Alice, Bob and Carol to each possess a qubit such that the joint state of the three qubits has both of the following properties at the same time?

      Property 1: The two-qubit state of Alice and Bob's qubits is $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

      Property 2: The two-qubit state of Bob and Carol's qubits is $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

      Either give an example of a three-qubit state with these properties or show that such a state does not exist.