CS667/CO681/PH767 Quantum Information Processing (Fall 07)

Assignment 2

Due date: October 16, 2007

1. **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 that Carol leaves the scene, again 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 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.

2. **Classical algorithms for the AND problem.** Recall that, for Deutsch's problem, there is a function $f : \{0,1\} \to \{0,1\}$ and the goal is to determine $f(0) \oplus f(1)$ with a single query to f. There is no classical algorithm that succeeds with probability more than $1/2$, whereas there is a quantum algorithm that succeeds with probability 1. This question and the next one pertain to a variation of Deutsch's problem, which we'll call the AND problem, where the goal is to determine $f(0) \wedge f(1)$ with a single query to f. ($\wedge$ denotes the logical AND operation.)

   Consider how well a *classical* algorithm can predict $f(0) \wedge f(1)$ with a single query to $f\{0,1\} \to \{0,1\}$. Give a classical probabilistic algorithm that makes a single query to f and predicts $f(0) \wedge f(1)$ with probability at least $2/3$.

   (Optional for bonus credit: prove that no classical algorithm can succeed with probability greater than $2/3$.)

3. **Quantum algorithms for the AND problem.** This is a continuation of the previous question. Here, we develop a quantum algorithm for AND that succeeds with probability higher than 2/3.

   (a) Give a quantum circuit that, with a single query to f, constructs the two-qubit state

   $$\tfrac{1}{\sqrt{3}}\left((-1)^{f(0)}|00\rangle + (-1)^{f(1)}|01\rangle + |11\rangle\right).$$

   (b) The quantum states of the form in part (a) are three-dimensional and have real-valued amplitudes. This makes it easy for us to visualize the geometry of these states (as vectors or lines in $\mathbb{R}^3$). Consider the four possible states that can arise from part (a), depending on which of the four possible functions f is. What is the absolute value of the inner product between each pair of those four states? (Note the symmetry!)

   (c) Based on parts (a) and (b), give a quantum algorithm for the AND problem that makes a single query to f and: succeeds with probability 1 whenever $f(0) \wedge f(1) = 1$; succeeds with probability 8/9 whenever $f(0) \wedge f(1) = 0$.

   (d) Note that the error probability of the algorithm from part (c) is one-sided in the sense that it is always correct in the case where $f(0) \oplus f(1) = 1$. Give a quantum algorithm for the AND problem that makes a single query to f and succeeds with probability 9/10. (Hint: take the output of the one-sided error algorithm from part (c) and do some classical post-processing on it, in order to turn it into a two-sided error algorithm with higher success probability.)

4. **A generalization of Deutsch's problem.** Consider the problem where one is given black-box access to a function $f : \{0,1\}^n \to \{0,1\}$ such that $f(x) = (a \cdot x) \oplus b$, where $a \in \{0,1\}^n$ and b are unknown. (Here $a \cdot x = (a_1 \wedge x_1) \oplus (a_2 \wedge x_2) \oplus \cdots \oplus (a_n \wedge x_n)$, the modulo-2 inner product of a and x.) The goal is to determine the n-bit string a. (Note that when $n = 1$ this is exactly Deutsch's problem.)

   (a) Show that any classical algorithm for this problem must make $n + 1$ queries.

   (b) Give a quantum algorithm for this problem that makes as few queries as possible. (For the quantum algorithm, each query is of the form $|x_1, x_2, \ldots, x_n, y\rangle \mapsto |x_1, x_2, \ldots, x_n, y \oplus f(x)\rangle$.)

5. **Optional bonus question: leading coefficients of quadratic polynomials.** Consider the problem where one is given black-box access to a function $f : \{0,1,2\} \to \{0,1,2\}$ such that $f(x) = ax^2 + bx + c$ (arithmetic here is modulo 3), where $a, b, c \in \{0,1,2\}$ are unknown coefficients. The goal is to determine the coefficient a.

   (a) Show that any classical algorithm for this problem must make 3 queries.

   (b) Give a quantum algorithm for this problem that makes only 2 queries.