QIC710/CS678/CO681/PH767/AM871 Introduction to Quantum Information Processing (F13)

Assignment 2
Due date: October 10, 2013

1. **Can a function be evaluated at two places with a single quantum query?** Here we consider the problem where we have a query oracle for a function $f : \{0,1\} \to \{0,1\}$ and the goal is to obtain information about both $f(0)$ and $f(1)$ with a single query. We assume that the query oracle is in the usual form of a unitary operator U_f that, for all $a, b \in \{0,1\}$, maps $|a,b\rangle$ to $|a, b \oplus f(a)\rangle$. For simplicity, we consider methods that employ only two qubits in all and are expressible by a circuit of the form

$$\begin{array}{ccccc} |0\rangle & & & & \chi \\ & V & U_f & W & \\ |0\rangle & & & & \chi \end{array}$$

where V and W are two-qubit unitaries and the gates labelled χ are measurements in the computational basis. Therefore, it can be assumed that the input state to the query is a two-qubit state of the form $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$, where $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$.

   (a) For each of the four functions of the form $f : \{0,1\} \to \{0,1\}$, give the quantum state right after the query has been performed.

   (b) If there is a measurement procedure that perfectly distinguishes between the four states in part (a) then they must be mutually orthogonal. Show that, for a measurement to be able to perfectly determine the value of $f(0)$, it must be the case that $\alpha_{10} = \alpha_{11}$. (Hint: think of the orthogonality relationships that need to hold.)

   (c) Show that, if the states are such that $f(0)$ can be determined perfectly from them, then $f(1)$ cannot be determined with probability better than $1/2$ (which is no better than random guessing). (Hint: You may use the result in part (b) for this.)

   (d) **Optional for bonus credit:** The above analysis is restricted to methods that use two qubits. Show that, for all $m \geq 2$, any strategy that uses m qubits (V and W are m-qubit unitaries and the query gate U_f acts on the last two qubits) and determines $f(0)$ perfectly cannot determine $f(1)$ with probability better than $1/2$.

2. **Classical and quantum algorithms for the OR problem (Part I).** In these next two questions, we consider the problem where we are given a black box for a function $f : \{0,1\} \to \{0,1\}$ and the goal is to determine $f(0) \vee f(1)$ (the logical OR of $f(0)$ and $f(1)$) with a *single* query to f.

   (a) Give a classical probabilistic algorithm that makes a single query to f and predicts $f(0) \vee f(1)$ with probability $2/3$. The probability is respect to the random choices of the algorithm; the input instance of f is assumed to be arbitrary (worst-case). (Note that it is *not* correct to give an algorithm that always outputs 1, and claim that this succeeds with probability $3/4$ because, for three of the four functions, $f(0) \vee f(1) = 1$. There exists an f for which the success probability of that algorithm is 0.)

   It turns out that no classical algorithm can succeed with probability greater than $2/3$ (but you are not asked to show this here).

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

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

(Hints: First construct a circuit for $\frac{1}{\sqrt{3}}\left((-1)^{f(0)}|00\rangle + (-1)^{f(1)}|01\rangle + (-1)^{f(1)}|11\rangle\right)$. The gate

$$\begin{pmatrix} \sqrt{1/3} & \sqrt{2/3} \\ \sqrt{2/3} & -\sqrt{1/3} \end{pmatrix}$$

and the controlled-Hadamard gate might be helpful for this. Next think about how to "supress" the phase for $|11\rangle$.)

(c) The quantum states of the form in part (b) 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?

3. **Classical and quantum algorithms for the OR problem (Part II).**

(a) Based on the results of Part I (question 2), give a quantum algorithm for the OR problem that makes a single query to f and: succeeds with probability 1 whenever $f(0) \vee f(1) = 0$; succeeds with probability 8/9 whenever $f(0) \vee f(1) = 1$.

(b) Note that the error probability of the algorithm from part (a) is one-sided in the sense that it is always correct in the case where $f(0) \vee f(1) = 0$. Give a quantum algorithm for the OR 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 (a) and do some classical post-processing on it, in order to turn it into a two-sided error algorithm with higher success probability.)

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.

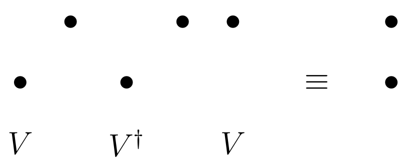
(a) Give a classical (i.e., not quantum) algorithm that solves this problem with n queries.

(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 $a_1 a_2 \dots a_n$. (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. **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

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

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.