# CS667/CO681/PH767/AM871 Quantum Information Processing (Fall 09)

Assignment 3

Due date: October 27, 2009

1. **Distinguishing states by local measurements.** In this question, we suppose Alice and Bob (who are physically separated from each other, say, in separate labs) are each given one of the qubits of some two-qubit state. Working as a team, they are required to distinguish between State A and State B with only *local* measurements. We will take this to mean that they can each perform a one-qubit unitary operation and then a measurement (in the computational basis) on their own qubit. After their measurements, they can send only *classical* bits to each other. In each case below, either give a perfect distinguishing procedure (that never errs) or explain why there is no perfect distinguishing procedure (i.e., that for any procedure the success probability must be less than 1).

   (a) State A: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
   State B: $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$

   (b) State A: $|00\rangle$
   State B: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

   (c) State A: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
   State B: $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$

2.

3. **Approximating unitary transformations.** There are frequent situations where it is much easier to approximate a unitary transformation than to compute it exactly. For a vector $v = (v_0, \ldots, v_{m-1})$, let $||v|| = \sqrt{\sum_{j=0}^{m-1} |v_j|^2}$, which is the usual Euclidean length of $v$. For an arbitrary $m \times m$ matrix $M$, define its *norm* $||M||$ as

$$||M|| = \max_{|\psi\rangle} ||M|\psi\rangle||,$$

   where the maximum is taken over quantum states (i.e., vectors $|\psi\rangle$ such that $|||\psi\rangle|| = 1$). We can now define the *distance* between to $m \times m$ unitary matrices $U_1$ and $U_2$ as $||U_1 - U_2||$.

   (a) Show that if $||U_1 - U_2|| \leq \epsilon$ then, for any quantum state $|\psi\rangle$, $||U_1|\psi\rangle - U_2|\psi\rangle|| \leq \epsilon$.

   (b) Show that $||A - B|| \leq ||A - C|| + ||C - B||$, for any three $m \times m$ matrices $A$, $B$, and $C$. (Thus, this distance measure satisfies the *triangle inequality.*)

   (c) Show that $||A \otimes I|| = ||A||$ for any $m \times m$ matrix $A$ and the $l \times l$ identity matrix $I$.

   (d) Show that $||U_1 A U_2|| = ||A||$, for any $m \times m$ matrix $A$ and any two $m \times m$ unitary matrices $U_1$ and $U_2$.

4. **Approximate quantum Fourier transform modulo $2^n$.** Recall that in class we saw how to compute the QFT modulo $2^n$ by a quantum circuit of size $O(n^2)$. Here, we consider how to compute an approximation of this QFT within $\epsilon$ by a quantum circuit of size $O(n \log(n/\epsilon))$.

(a) Recall that the $O(n^2)$ size QFT quantum circuit uses gates of the form

$$P_k = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{2\pi i/2^k} \end{pmatrix},$$

for values of $k$ that range between 2 and $n$. Show that $||P_k - I|| \leq 2\pi/2^k$, where $I$ is the $4 \times 4$ identity matrix. (Thus, $P_k$ gets very close to $I$ when $k$ increases.)

(b) The idea behind the approximate QFT circuit is to start with the $O(n^2)$ circuit and then remove some of its $P_k$ gates. Removing a $P_k$ gate is equivalent to replacing it with an $I$ gate. Removing a $P_k$ gate makes the circuit smaller but it also changes the unitary transformation. From part (a) and the general properties of our measure of distance between unitary transformations in the previous question, we can deduce that if $k$ is large enough then removing a $P_k$ gate changes the unitary transformation by only a small amount. Show how to use this approach to obtain a quantum circuit of size $O(n \log(n/\epsilon))$ that computes a unitary transformation $\tilde{F}_{2^n}$ such that

$$||\tilde{F}_{2^n} - F_{2^n}|| \leq \epsilon.$$

(Hint: Try removing all $P_k$ gates where $k \geq t$, for some carefully chosen threshold $t$. The properties of our distance measure from the previous question should be useful for your analysis here.)

5. **Distinguishing between two families of states.** Consider the following two sets of $n$-qubit states: set A consists of just the state

$$\tfrac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \tag{1}$$

and set B consists of all states of the form

$$\tfrac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle, \tag{2}$$

where $f : \{0,1\}^n \to \{0,1\}$ is a balanced function (that is, $\sum_{x \in \{0,1\}^n} f(x) = 2^{n-1}$).

Each state in B is orthogonal to the state in A, so in principle the two sets of states can be distinguished perfectly. Show explicitly how to distinguish between the two sets by describing a an $n$-qubit unitary operation $U$ in terms of a circuit consisting of 1-qubit gates and/or 2-qubit gates with the following property: $U$ maps the state in $A$ to $|00\ldots0\rangle$ and $U$ maps every state in B to some state that is orthogonal to $|00\ldots0\rangle$. Include a proof that your $U$ has this property. (Note that, with this $U$, the distinguishing procedure becomes easy: given a state $|\psi\rangle$, apply $U$ and measure the result in the computational basis; if the result is $00\ldots0$ then $|\psi\rangle \in$ A, otherwise $|\psi\rangle \in$ B.)

6. **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 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 $a_1 a_2 \ldots a_n$. (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.)

7. **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 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.

8. **Quantum Fourier transform.** Let $F_N$ denote the $N$-dimensional Fourier transform

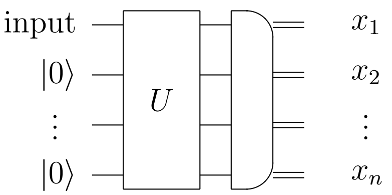
$$F_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \cdots & \omega^{(N-1)^2} \end{pmatrix}, \quad \text{where } \omega = e^{2\pi i/N} \ (i = \sqrt{-1})$$

(an $N \times N$ matrix, whose entry in position $jk$ is $\frac{1}{\sqrt{N}}(e^{2\pi i/N})^{jk}$ for $j, k \in \{0, 1, \ldots, N-1\}$).

   (a) Show that any two rows of $F_N$ are orthonormal.

   (b) What is $(F_N)^2$? The matrix has a very simple form.

9. **A qubit cannot be used communicate more than one bit.** Suppose that Alice wants to convey a trit of information (an element of $\{0, 1, 2\}$) to Bob and all she is allowed to do is prepare one qubit and send it to Bob. If Bob's measurement procedure is to apply a 1-qubit unitary operation and then apply a standard measurement then it is clear that this cannot work, because the measurement has only two outcomes. But this type of argument does not rule out the possibility that, with a more complex kind of measurement on Bob's side, they might be able to do it: Bob could prepare $n - 1$ additional qubits, each in state $|0\rangle$, and apply an $n$-qubit unitary operation to the entire $n$ qubit system and *then* perform a standard measurement.



$\mapsto f(x_1, x_2, \ldots, x_n) \in \{0, 1, 2\}$

Bob's more complex measurement of a qubit

The outcome will be an element of $\{0, 1\}^n$. It is conceivable that Bob could somehow determine the trit from these $n$ bits. We shall prove that this is impossible.

The framework is that Alice starts with a trit $j \in \{0, 1, 2\}$ (unknown to Bob) and, based on $j$, prepares a one-qubit state, $\alpha_j|0\rangle + \beta_j|1\rangle$, and sends it to Bob. Then Bob applies some $n$-qubit unitary $U$ to $(\alpha_j|0\rangle + \beta_j|1\rangle)|00\ldots0\rangle$ and does a standard measurement to the resulting state, obtaining some $x \in \{0, 1\}^n$ as outcome. Next, Bob then applies a function $f : \{0, 1\}^n \to \{0, 1, 2\}$ to $x$ to obtain a trit. The scheme works if and only if, starting with any $j \in \{0, 1, 2\}$, the resulting $x$ will satisfy $f(x) = j$.

   (a) Note that each row of the matrix $U$ is a $2^n$-dimensional vector. For $j \in \{0, 1, 2\}$, define the space $V_j$ to be the span of all rows of $U$ that are indexed by an element of the set $f^{-1}(j) \subseteq \{0, 1\}^n$. Prove that $V_0$, $V_1$, and $V_2$ are mutually orthogonal spaces.

   (b) Explain why, for a scheme to work, $(\alpha_j|0\rangle + \beta_j|1\rangle)|00\ldots0\rangle \in V_j$ must hold for all $j \in \{0, 1, 2\}$.

   (c) Prove that it is impossible for $(\alpha_j|0\rangle + \beta_j|1\rangle)|00\ldots0\rangle \in V_j$ to hold for all $j \in \{0, 1, 2\}$.

The contradiction between parts (b) and (c) imply that no scheme can work. It is straightforward to extend this proof to show that, for any $r > 2^m$, Alice cannot convey one of $r$ possibilities by just sending $m$ qubits to Bob (you are not asked to do this here).