QIC710/CS768/CO681/PH767/AM871 Introduction to Quantum Information Processing (F14)

Assignment 3
Due date: October 28, 2014

Note on new grading policy: For any part of a question, if you do not know how to answer it, you have the option of clearly writing "I DO NOT KNOW HOW TO ANSWER THIS QUESTION" and nothing else. For this you will receive 25% of the grade for that part (rounded up to the nearest integer). For example, if you do this for 2(c), you will receive 1 (out of 4). This does not apply to any optional bonus questions—you should only answer those questions if you think you have a solution.

1. **Functions that compute the parity of two unknown input bits.** Consider the set of all functions $f : \{0,1\}^n \to \{0,1\}$ that are of the form $f(x_1, x_2, \ldots, x_n) = x_{j_1} \oplus x_{j_2}$ for some $j_1, j_2 \in \{1, 2, \ldots, n\}$ with $j_1 \neq j_2$. Suppose that we are given such a function as a black box (without information about j_1, j_2) and our task is to determine the set $\{j_1, j_2\}$.

   (a) Show that any *classical* algorithm must make at least $\Omega(\log n)$ queries to f to solve this problem exactly. (Hint: First, note that the data that a k-query classical algorithm obtains is a k-bit string. Next, consider how big k needs to be so that there are enough k-bit strings to be uniquely assigned to each $\{j_1, j_2\}$.)

   (b) Give a *quantum* algorithm that solves this problem exactly with a single query to f.

   (c) **Optional for bonus credit:** Regarding the classical query cost of this problem, we know from part (a) that it is asymptotically *at least* $\Omega(\log n)$. What is the classical asymptotic query complexity? Justify your answer. (Asymptotic means we can disregard constant multiplicative factors.)

2. **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 *(spectral) 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 $|||\psi\rangle|| = 1$). For this question, we define the *distance* between two $m \times m$ unitary matrices U_1 and U_2 as $||U_1 - U_2||$.

   (a) 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*.)

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

   (c) 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.

3. **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 ϵ 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 4×4 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.)

4. **Period inversion.** Let p and q be integers greater than 1, and pq denote their product. Recall that the quantum Fourier transform modulo pq is the pq-dimensional unitary operation F_{pq} such that

$$F_{pq}|x\rangle = \frac{1}{\sqrt{pq}} \sum_{y=0}^{pq-1} \left(e^{2\pi i/pq}\right)^{xy} |y\rangle$$

   for each $x \in \mathbb{Z}_{pq}$.

   (a) Define two quantum states $|\psi_1\rangle$ and $|\psi_2\rangle$ as

$$|\psi_1\rangle = \frac{1}{\sqrt{q}} \left(|0\rangle + |p\rangle + |2p\rangle + \cdots + |(q-1)p\rangle \right) = \frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |xp\rangle$$

   and

$$|\psi_2\rangle = \frac{1}{\sqrt{p}} \left(|0\rangle + |q\rangle + |2q\rangle + \cdots + |(p-1)q\rangle \right) = \frac{1}{\sqrt{p}} \sum_{x=0}^{p-1} |xq\rangle.$$

   Show that $F_{pq}|\psi_1\rangle = |\psi_2\rangle$.

(b) Let $s \in \{0, 1, \ldots, p-1\}$, and define $|\psi_3\rangle$ (a "shifted" version of $|\psi_1\rangle$) as

$$\begin{aligned} |\psi_3\rangle &= \frac{1}{\sqrt{q}} \left(|s\rangle + |s+p\rangle + |s+2p\rangle + \cdots + |s+(q-1)p\rangle \right) \\ &= \frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |s+xp\rangle. \end{aligned}$$

What is $F_{pq}|\psi_3\rangle$? Find a simple expression for this quantity. If $F_{pq}|\psi_3\rangle$ is measured in the computational basis, what is the probability distribution describing the outcome?

5. **Basic questions about density matrices.**

(a) A density matrix ρ corresponds to a *pure* state if and only if $\rho = |\psi\rangle\langle\psi|$. Show that ρ corresponds to a pure state if and only if $\mathrm{Tr}(\rho^2) = 1$.

(b) Show that, for any operator that is Hermitian, positive definite (i.e., has no negative eigenvalues), and has trace 1, there is a probabilistic mixture of pure states whose denisty matrix is ρ.

(c) Show that every 2×2 density matrix ρ can be expressed as an *equally weighted mixture* of pure states. That is

$$\rho = \frac{1}{2}|\psi_1\rangle\langle\psi_1| + \frac{1}{2}|\psi_2\rangle\langle\psi_2|$$

for states $|\psi_1\rangle$ and $|\psi_2\rangle$ (note that, in general, the two states will not be orthogonal).