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

Assignment 3

Due date: October 30, 2007

1. **Some properties of the quantum Fourier transform.** Let F_m be the quantum Fourier transform modulo m. That is,

$$F_m|j\rangle = \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} \omega^{jk}|k\rangle, \quad \text{for all } j \in \mathbb{Z}_m, \text{ where } \omega = e^{2\pi i/m}.$$

   (a) Shoe that the rows of F_m are orthonormal.

   (b) Show that $F_m \cdot F_m|0\rangle = |0\rangle$ and $F_m \cdot F_m|a\rangle = |m-a \bmod m\rangle$, for all $a \in \{1, \ldots, m-1\}$.

2. **A protocol that enables certain states to be remotely created.** Suppose that Alice and Bob each possess one qubit of the Bell state

$$\tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

   and that Alice also possesses an arbitrary real number θ (and Bob does not know what θ is). Let the goal be for Bob to end up with the state $\cos(\theta)|0\rangle + \sin(\theta)|1\rangle$. One way of doing this is for Alice to manufacture the state and then for her to teleport it to Bob. But recall that teleportation requires *two* bits of classical communication. Here, we consider how Alice and Bob can solve this problem (which is more restricted than teleportation) using only *one* classical bit of communication. The protocol begins by Alice applying a rotation by θ to her qubit. After this, Alice measures her qubit (in the computational basis) and sends the result (one classical bit) to Bob. Show how Bob can apply a unitary operation to his qubit—that depends on the bit he receives from Alice—so that his state is guaranteed to become $\cos(\theta)|0\rangle + \sin(\theta)|1\rangle$.

3. **Sharing a secret state among three parties.** Suppose that we have a qu*trit* in the "secret" state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle$ and we would like to send information about $|\psi\rangle$ to three parties, Alice, Bob, and Carol, so that *any two of them* can reconstruct $|\psi\rangle$ but *no individual* can. We do this by constructing the three-qutrit state

$$\frac{\alpha}{\sqrt{3}}(|000\rangle + |111\rangle + |222\rangle) + \frac{\beta}{\sqrt{3}}(|012\rangle + |120\rangle + |201\rangle) + \frac{\gamma}{\sqrt{3}}(|021\rangle + |102\rangle + |210\rangle),$$

   and then sending the first qutrit to Alice, the second to Bob, and the third to Carol.

   (a) Show that a copy of $|\psi\rangle$ can be constructed from just Alice and Bob's qutrits (i.e., without any interactions with Carol's qutrit).

   (b) Deduce that a copy of $|\psi\rangle$ can also be constructed from just Bob and Carol's qutrits. (It's similar for Alice and Carol's qutrits, but you need not show this.)

   (c) Prove that $|\psi\rangle$ cannot be reconstructed from any single party's qutrit. (Hint: consider the No-Cloning Theorem.)

4. **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.

5. **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.)