QIC710/CS768/CO681/PH767/AM871 Introduction to Quantum Information Processing (F16)

Assignment 3
Due date: November 1, 2016

1. **Approximating unitary transformations [12 points; 4 each].** There are 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 any $m \times m$ 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 $|||\psi\rangle|| = 1$). 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, for any any $m \times m$ matrix A and the $\ell \times \ell$ identity matrix I, $||A \otimes I|| = ||A||$.

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

2. **Approximate quantum Fourier transform modulo 2^n [12 points].** In class, we computed the QFT modulo 2^n by a quantum circuit of size $O(n^2)$. Here, we compute an approximation of this QFT within ϵ by a quantum circuit of size $O(n \log(n/\epsilon))$.

   (a) [4 points] 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) [8 points] 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 makes the circuit smaller but also changes the unitary transformation (it is equivalent to changing the P_k gate to an I gate). From part (a) and the properties of our measure of distance between unitary transformations from 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.)

3. **Computing the "square root" of a quantum circuit [12 points; 4 each].**

Suppose that you are given a quantum circuit acting on n qubits that consists of s 2-qubit gates. It corresponds to *some* $2^n \times 2^n$ unitary matrix U, but, in general, there is no way of efficiently calculating all the entries of U from the circuit. Suppose that we want to construct another circuit that computes a square root of U (i.e., a unitary V such that $V^2 = U$). You can check that just taking the square roots of each gates in the original circuit does not yield such a V.

We will use a clever trick involving the eigenvalue-estimation algorithm do this efficiently. We just consider a simplified case where we are promised that the eigenvalues of U are all in $\{1, i, -1, -i\}$; however, the basic approach can be extended to the arbitrary case.

Let $\{|\psi_x\rangle : x \in \{0, \ldots, 2^n - 1\}\}$ be a set of orthonormal eigenvectors of U. Then

$$U = \sum_{x=0}^{2^n-1} i^{\phi_x} |\psi_x\rangle\langle\psi_x|,$$

where $\phi_x \in \{00, 01, 10, 11\} \equiv \{0, 1, 2, 3\}$ for each x. Our method will compute

$$V = \sum_{x=0}^{2^n-1} \omega^{\phi_x} |\psi_x\rangle\langle\psi_x|,$$

where $\omega = e^{2\pi i/8}$, which is a square root of U.

An outline of the construction is the following. First construct a generalized-control-U gate, with two control-qubits. Then apply the eigenvalue-estimation algorithm to this controlled-U gate, which results in a circuit that computes $ab = \phi_x$, in two ancillary qubits, for any input $|\psi_x\rangle$. Next, apply gates to those two ancilliary qubits to induce the mapping $|ab\rangle \mapsto \omega^{ab}|ab\rangle$. Then apply the inverse of the eigenvalue estimation circuit. The net result is a circuit that maps every $|\psi_x\rangle$ to $\omega^{\phi_x}|\psi_x\rangle$. Note that this construction does exactly what V does when the input is an eigenvector $|\psi_x\rangle$. Moreover, since the circuit computes a linear operation and the $|\psi_x\rangle$ are a basis, the circuit must compute V.

Assume that we have a circuit computing U with s 2-qubit gates:

(a) Explain how to construct a circuit computing the two-qubit controlled-U operation using $3s$ 3-qubit gates.

(b) Explain how to construct a circuit computing $ab = \phi_x$ on input $|\phi_x\rangle$ using $3s$ 3-qubit gates plus one 2-qubit gate plus four 1-qubit gates.

(c) Give a 2-qubit quantum circuit consisting of two 1-qubit gates that maps each basis state $|ab\rangle$ to $\omega^{ab}|ab\rangle$.

Note that the total gate cost is 6s 3-qubit gates plus two 2-qubit gates plus eight 1-qubit gates. This can be converted into a circuit consisting of $O(s)$ 2-qubit gates, not much more than the original circuit.

4. **Basic questions about density matrices [12 points; 4 each].**

   (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).

5. **The density matrix is in the eye of the beholder [12 points; 3 each].** Consider the following scenario. Alice first flips a biased coin that has outcome 0 with probability $\cos^2(\pi/8)$ and 1 with probability $\sin^2(\pi/8)$. If the coin value is 0 she creates the state $|0\rangle$ and if the coin value is 1 she creates the state $|1\rangle$. Then Alice sends the state that she created to Bob (she does not send the coin value).

   (a) From Alice's perspective (who *knows* the coin value), the density matrix of the state she created will be either $|0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ or $|1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. What is the density matrix of the state from Bob's perspective (who does *not* know the coin value)? Give the four matrix entries of this density matrix.

   (b) Suppose that, upon receiving the state from Alice, Bob measures it in the computational basis. The measurement process yields a classical bit and an output state ("collapsed" to $|0\rangle$ or $|1\rangle$). Will Bob's density matrix for the state (with Bob knowing the classical measurement outcome) be the same as Alice's?

   Suppose that we modify the above scenario to one where Alice flips a *fair* coin (where outcomes 0 and 1 each occur with probability 1/2) and if the coin value is 0 she creates the state $|\psi_0\rangle = \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle$ and if the coin value is 1 she creates the state $|\psi_1\rangle = \cos(\pi/8)|0\rangle - \sin(\pi/8)|1\rangle$. Alice sends the state (but not the coin value) to Bob.

   (c) From Alice's perspective (who *knows* the coin value), the density matrix of the state she created will be either $|\psi_0\rangle\langle\psi_0|$ or $|\psi_1\rangle\langle\psi_1|$. What is the density matrix of the state from Bob's perspective (who does *not* know the coin value)? Give the four matrix entries of this density matrix.

   (d) Suppose that, upon receiving the state from Alice, Bob measures it in the computational basis, yielding a classical bit and an output state ("collapsed" to $|0\rangle$ or $|1\rangle$). Bob knows the classical bit outcome from his measurement, but does not reveal this to Alice. Will Bob's density matrix for the output state be the same as Alice's?