QIC710/CS667/CO681/PH767/AM871 Introduction to Quantum Information Processing (F12)

Assignment 4
Due date: November 6, 2012

1. **Some consequences of putting inputs to unitaries in superposition.**

   (a) Let U be any n-qubit unitary, $|\psi_1\rangle$, $|\psi_2\rangle$ be orthogonal n-qubit states, and $a_1, a_2 \in \{0,1\}^n$ such that the following property holds. For each $j \in \{1,2\}$, if $U|\psi_j\rangle$ is measured in the computational basis then the outcome is a_j for sure (i.e., with probability 1). Let α_1, α_2 be such that $|\alpha_1|^2 + |\alpha_2|^2 = 1$. Does it follow that, if $U(\alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle)$ is measured in the computational basis, then the outcome is

   $$\begin{cases} a_1 & \text{with probability } |\alpha_1|^2 \\ a_2 & \text{with probability } |\alpha_2|^2? \end{cases}$$

   Either prove it or give a counterexample.

   (b) Let U be any n-qubit unitary, $|\psi_1\rangle$ and $|\psi_2\rangle$ be orthogonal n-qubit states, and $a_1, b_1, a_2, b_2 \in \{0,1\}^n$ such that the following property holds. For each $j \in \{1,2\}$, if $U|\psi_j\rangle$ is measured in the computational basis then the outcome is

   $$\begin{cases} a_j & \text{with probability } p_j \\ b_j & \text{with probability } q_j \end{cases}$$

   (where $p_k + q_k = 1$). Let α_1, α_2 be such that $|\alpha_1|^2 + |\alpha_2|^2 = 1$. Does it follow that if $U(\alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle)$ is measured in the computational basis then the outcome is

   $$\begin{cases} a_1 & \text{with probability } p_1|\alpha_1|^2 \\ b_1 & \text{with probability } q_1|\alpha_1|^2 \\ a_2 & \text{with probability } p_2|\alpha_2|^2 \\ b_2 & \text{with probability } q_2|\alpha_2|^2. \end{cases}$$

   Either prove it or give a counterexample.

2. **More consequences of putting inputs to unitaries in superposition.** This question is sort of a continuation of question 1, and pertains to a detail that arose in the quantum algorithm for order-finding that was discussed in class. Let W denote a generalized n-qubit controlled-U gate (i.e., for all $x, y \in \{0,1\}^n$, $W|x\rangle|y\rangle = |x\rangle U^x|y\rangle$) and let $|\psi_1\rangle$, $|\psi_2\rangle$ be two orthogonal eigenvectors of U. Let V be any n-qubit unitary (for order-finding, this was the inverse QFT $F^\dagger$). Also, let $|\phi\rangle$ be any n-qubit state initial state for the control-qubits of W (for order-finding, this was $\frac{1}{2^{n/2}}\sum_x |x\rangle$). Suppose that the following property holds. For each $j \in \{1,2\}$, if *the first register (i.e., the first n qubits)* of $(V \otimes I)W|\phi\rangle|\psi_j\rangle$ is measured in the computational basis then the outcome is

   $$\begin{cases} a_j & \text{with probability } p_j \\ b_j & \text{with probability } q_j \end{cases}$$

(where $p_k + q_k = 1$). Prove that then, if *the first register of* $(V \otimes I)W|\phi\rangle(\alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle)$ is measured in the computational basis, the outcome is

$$\begin{cases} a_1 & \text{with probability } p_1|\alpha_1|^2 \\ b_1 & \text{with probability } q_1|\alpha_1|^2 \\ a_2 & \text{with probability } p_2|\alpha_2|^2 \\ b_2 & \text{with probability } q_2|\alpha_2|^2. \end{cases}$$

3. **Classical reversible computations and invertibility.** There is an efficient classical algorithm for multiplying two integers, and we can implement this in terms a circuit consisting of reversible gates. Since everything implementable in terms of reversible gates can be inverted by just running the circuit backwards (inverting each gate and placing them in a backwards order), it would seem that we can efficiently invert multiplication by a classical circuit. Does this imply that there is an efficient classical algorithm that, given a product of two large primes, computes the factors efficiently? (This would mean that we don't need Shor's algorithm to factor.) The answer can be obtained by investigating precise definitions.

   Let $f : \{0,1\}^n \to \{0,1\}^n$ be an invertible (i.e., bijective) function. We define two ways of computing f. The first way, which we call the *input-preserving* computation of f, is where for each $x, y \in \{0,1\}^n$, $|x\rangle|y\rangle$ is mapped to $|x\rangle|y \oplus f(x)\rangle$. We allow additional qubits to be used in the computation as long as they are all initialized in state $|0\rangle$ and are reset to state $|0\rangle$ by the end of the computation (so the computation might be $|x\rangle|y\rangle|0^m\rangle \mapsto |x\rangle|y \oplus f(x)\rangle|0^m\rangle$). We call the second way of computing f the *input-erasing* computation of f, and this is where for each $x \in \{0,1\}^n$, $|x\rangle$ is mapped to $|f(x)\rangle$. (Again, with extra qubits, the actual compuytation can be $|x\rangle|0^m\rangle \mapsto |f(x)\rangle|0^m\rangle$.)

   (a) Given an efficient circuit (say, of size polynomial in n) consisting of reverible gates that computes f in an input-preserving manner, then we can reverse this circuit by inverting each gate of the circuit and putting the gates in reverse order. Does doing this yield an efficient circuit that computes f^{-1} in an input-preserving manner? Explain your answer.

   (b) Show that if both f and f^{-1} can be computed in an input-preserving manner then f can be computed in an input-erasing manner.

   (c) Show that if f can be computed in an *input-erasing* manner than f^{-1} can be computed in an *input-preserving* manner.

4. **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 $\text{Tr}(\rho^2) = 1$.

   (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

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

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

5. **Operations, states and the Bloch sphere.** Consider the unitary matrices of the form

$$M_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$$

where $\theta \in [0, 2\pi)$.

(a) Prove that, for any value of θ, M_θ is a *reflection*. In other words, that the eigenvalues of M_θ are from $\{+1, -1\}$. (Note: there is a very easy way of doing this.)

(b) Prove that, on the Bloch sphere, M_θ acts as a *rotation* (for any value of θ).
Give the axis of rotation and angle of rotation.

(c) Specify four *one-qubit* quantum states $|\phi_0\rangle$, $|\phi_1\rangle$, $|\phi_2\rangle$, $|\phi_3\rangle$, such that, for all $j \neq k$, $|\langle\phi_j|\phi_k\rangle| \leq r$, for as small an r as possible. Note that, using states $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$, achieves $r = 1/\sqrt{2}$, but a smaller r is achievable. You may specify the states by their density matrices; however, you should explicitly give the value of r obtained.