QIC710/CS768/CO681/PH767/AM871 Introduction to Quantum Information Processing (F15)

Assignment 4
Due date: November 10, 2015

1. **Action of unitary operations on the Bloch sphere [12 points; 4 each].** For every 2×2 unitary matrix U, the effect of applying U on a qubit can be viewed as a rotation of the states in the Bloch sphere. For example, it can be shown that

$$\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix} \tag{1}$$

corresponds to rotation by angle 2θ along the axis specified by state $|0\rangle$. In each case below, give the angle of rotation (which can be a function of the parameter θ, where $0 \leq \theta < \pi$) and specify the axis of rotation:

(a)

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \tag{2}$$

(b)

$$\begin{pmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{pmatrix} \tag{3}$$

(c)

$$\begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix} \tag{4}$$

2. **General conversion from Stinespring form to Krauss form [12 points].** Suppose that you are given a description of a quantum operation that takes an n-qubit state ρ as input and produces an n'-qubit state σ as output, where the description is of the following form (where $n + m = n' + m'$):

   i. Append an m qubits, in state $|0^m\rangle$ to the end of the input state.
   ii. Apply an $(n+m)$-qubit unitary operation U.
   iii. Trace out the *first* m' qubits (resulting in an n'-qubit output).

   Show how to implement this in Krauss form as

$$\rho \mapsto \sum_{j \in S} A_j \rho A_j^\dagger,$$

   where $\sum_{j \in S} A_j^\dagger A_j = I$. Please be careful with the dimensions of your matrices/vectors (so that they make sense). Also, to avoid ambiguity between multiplication and tensor product, write $\otimes$ explicitly to denote the latter (it will be assumed that AB means the matrix product of A and B, as opposed to $A \otimes B$).

3. **Square roots of channels [12 points; 4 each].** A *square root* of a channel $\mathcal{C}$ is another channel $\mathcal{C}'$ such that $\mathcal{C}'(\mathcal{C}'(\rho)) = \mathcal{C}(\rho)$ for all states ρ. In the following, let p be an arbitrary real-valued parameter such that $0 < p < 1$.

   (a) Give a square root of the channel specified by these Krauss operators:

$$A_0 = \begin{pmatrix} \sqrt{p} & 0 \\ 0 & \sqrt{p} \end{pmatrix} \quad \text{and} \quad A_1 = \begin{pmatrix} 0 & \sqrt{1-p} \\ \sqrt{1-p} & 0 \end{pmatrix}. \tag{5}$$

   (b) Give a square root of the channel specified by these Krauss operators:

$$A_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-p} \end{pmatrix} \quad \text{and} \quad A_1 = \begin{pmatrix} 0 & \sqrt{p} \\ 0 & 0 \end{pmatrix}. \tag{6}$$

   (c) Does every channel that maps qubits to qubits have a square root? Justify your answer.

4. **Separable versus entangled mixed states [12 points; 4 each].** A *pure* bipartite state shared by A(lice) and B(ob) is entangled iff it is not of the form $\rho_{AB} = |\psi\rangle_A \otimes |\phi\rangle_B$ (the subscripts are added here to help keep track of who has what). In the case of *mixed* states, it's more complicated because a bipartite state can include classical correlations. For example, the state $\frac{1}{2}|00\rangle\langle 00|_{AB} + \frac{1}{2}|11\rangle\langle 11|_{AB}$ corresponds to A and B sharing $|00\rangle_{AB}$ with probability $\frac{1}{2}$ and $|11\rangle_{AB}$ with probability $\frac{1}{2}$. Such a state is classically correlated but has no entanglement—it could never be used for, say, teleportation or superdense coding.

   A bipartite state ρ_{AB} is *separable* iff it can be written as a mixture (i.e., convex combination) of product states:

$$\rho_{AB} = \sum_{j=1}^{m} p_j |\psi_j\rangle\langle\psi_j|_A \otimes |\phi_j\rangle\langle\phi_j|_B \quad \text{(where, for all } j,\ p_j \geq 0).$$

   (Note that $|\psi_j\rangle\langle\psi_j|_A \otimes |\phi_j\rangle\langle\phi_j|_B = (|\psi_j\rangle_A \otimes |\phi_j\rangle_B)(\langle\psi_j|_A \otimes \langle\phi_j|_B)$.) A mixed state is deemed *entangled* if it is not separable. For the following, denote the four Bell states as

$$|\Phi_1\rangle_{AB} = \tfrac{1}{\sqrt{2}}|00\rangle_{AB} + \tfrac{1}{\sqrt{2}}|11\rangle_{AB} \tag{7}$$
$$|\Phi_2\rangle_{AB} = \tfrac{1}{\sqrt{2}}|01\rangle_{AB} + \tfrac{1}{\sqrt{2}}|10\rangle_{AB} \tag{8}$$
$$|\Phi_3\rangle_{AB} = \tfrac{1}{\sqrt{2}}|00\rangle_{AB} - \tfrac{1}{\sqrt{2}}|11\rangle_{AB} \tag{9}$$
$$|\Phi_4\rangle_{AB} = \tfrac{1}{\sqrt{2}}|01\rangle_{AB} - \tfrac{1}{\sqrt{2}}|10\rangle_{AB}. \tag{10}$$

   (a) Show that $\rho_{AB} = \frac{1}{4}|\Phi_1\rangle\langle\Phi_1|_{AB} + \frac{1}{4}|\Phi_2\rangle\langle\Phi_2|_{AB} + \frac{1}{4}|\Phi_3\rangle\langle\Phi_3|_{AB} + \frac{1}{4}|\Phi_4\rangle\langle\Phi_4|_{AB}$ is separable by giving another expression for ρ_{AB} that's a mixture of product states.

   (b) Show that $\rho_{AB} = \frac{1}{2}|\Phi_1\rangle\langle\Phi_1|_{AB} + \frac{1}{2}|\Phi_3\rangle\langle\Phi_3|_{AB}$ is separable by giving another expression for ρ_{AB} that's a mixture of product states.

   (c) Is $\rho_{AB} = \frac{1}{2}|\Phi_1\rangle\langle\Phi_1|_{AB} + \frac{1}{2}|00\rangle\langle 00|_{AB}$ entangled or separable? Justify your answer.

5. **Classical reversible computations and invertibility [12 points; 4 each].** 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 might 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 then f^{-1} can be computed in an *input-preserving* manner.