## CS667/CO681/PH767/AM871 Quantum Information Processing (Fall 09)

## Assignment 4

Due date: November 12, 2009

## 1. Easy questions about density matrices.

(a) A density matrix $\rho$ corresponds to a pure state if and only if $\rho=|\psi\rangle\langle\psi|$. Show that $\rho$ corresponds to a pure state if and only if $\operatorname{Tr}\left(\rho^{2}\right)=1$.
(b) Show that every $2 \times 2$ density matrix $\rho$ can be expressed as an equally weighted mixture of pure states. That is

$$
\rho=\frac{1}{2}\left|\psi_{1}\right\rangle\left\langle\psi_{1}\right|+\frac{1}{2}\left|\psi_{2}\right\rangle\left\langle\psi_{2}\right|
$$

for states $\left|\psi_{1}\right\rangle$ and $\left|\psi_{2}\right\rangle$ (note that, in general, the two states will not be orthogonal).
2. Separable versus entangled mixed states. A pure bipartite state shared by A (lice) and $\mathrm{B}(\mathrm{ob})$ is entangled iff it is not of the form $\rho_{A B}=|\psi\rangle_{A} \otimes|\phi\rangle_{B}$ (the subscripts are 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 $\frac{1}{2}|00\rangle\left\langle\left. 00\right|_{A B}+\right.$ $\frac{1}{2}|11\rangle\left\langle\left. 11\right|_{A B} \text { corresponds to A and B sharing } \mid 00\right\rangle_{A B}$ with probability $\frac{1}{2}$ and $|11\rangle_{A B}$ 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 $\rho_{A B}$ is separable iff it can be written as a mixture of product states:

$$
\rho_{A B}=\sum_{j=1}^{m} p_{j}\left|\psi_{j}\right\rangle\left\langle\left.\psi_{j}\right|_{A} \otimes \mid \phi_{j}\right\rangle\left\langle\left.\phi_{j}\right|_{B} \quad\left(\text { where, for all } j, p_{j} \geq 0\right)\right.
$$

(Note that $\left|\psi_{j}\right\rangle\left\langle\left.\psi_{j}\right|_{A} \otimes \mid \phi_{j}\right\rangle\left\langle\left.\phi_{j}\right|_{B}=\left(\left|\psi_{j}\right\rangle_{A} \otimes\left|\phi_{j}\right\rangle_{B}\right)\left(\left\langle\left.\psi_{j}\right|_{A} \otimes\left\langle\left.\phi_{j}\right|_{B}\right)\right.\right.\right.$.) A mixed state is deemed entangled if it is not separable.
(a) Show that the mixture of two Bell states $\frac{1}{2}\left|\Phi^{+}\right\rangle\left\langle\left.\left.\Phi^{+}\right|_{A B}+\frac{1}{2} \right\rvert\, \Phi^{-}\right\rangle\left\langle\left.\Phi^{-}\right|_{A B}\right.$ is separable by giving another expression for its density matrix that's a mixture of product states.
(b) Is $\frac{1}{2}\left|\Phi^{+}\right\rangle\left\langle\left.\left.\Phi^{+}\right|_{A B}+\frac{1}{2} \right\rvert\, 00\right\rangle\left\langle\left. 00\right|_{A B}\right.$ entangled or separable? Justify your answer.
3. Error-free measurements of non-orthogonal states. Consider the scenario where you are given either $|0\rangle$ or $|+\rangle=\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle$ and you can produce one of three outcomes: " 0 ", "+", or "?". If you produce outcome " 0 " then the state you received must have been $|0\rangle$. If you produce outcome " + " then the state you received must have been $|+\rangle$. But you may sometimes abstain and output "?".

The above task can be trivially achieved by always outputting "?", but that's not very interesting. Show how the above task can be accomplished such that the probability of abstaining is at most $\frac{1}{\sqrt{2}}$ (in other words, where your output is in $\{0,+\}$ with probability at least $\left.1-\frac{1}{\sqrt{2}}\right)$.
4. Constructing an AND gate as a quantum operation. Here we consider operations that map the two-qubit state $|a, b\rangle$ to the one-qubit state $|a \wedge b\rangle$, for all $a, b \in\{0,1\}$. Of course, no unitary operation can perform this mapping, since the input and output dimension do not match; however, general quantum operations can compute this mapping.
(a) Give four $2 \times 4$ matrices $A_{1}, A_{2}, A_{3}, A_{4}$ such that $\sum_{j=1}^{4} A_{j}^{\dagger} A_{j}=I$ that compute the above mapping in that, for all $a, b \in\{0,1\}$, when $\rho=|a, b\rangle\langle a, b|$,

$$
\begin{equation*}
\sum_{j=1}^{4} A_{j} \rho A_{j}^{\dagger}=|a \wedge b\rangle\langle a \wedge b| \tag{1}
\end{equation*}
$$

(b) Your operation from part (a) maps all basis states to pure states. Does it map all pure input states to pure output states? Either prove the answer is yes, or provide a counterexample.
(c) Here we implement the mapping in the Stinespring form, using additional qubits at the beginning, performing a unitary operation, and then tracing out qubits. Consider this three-step process (where the input is any two-qubit quantum state):
i. Append a third qubit in state $|0\rangle$ to the end of the two input qubits.
ii. Apply a 3 -qubit unitary operation $U$.
iii. Trace out the second and third qubit (resulting in a single qubit, taken as the output).

Describe a 3-qubit unitary $U$ that causes this process to implement the mapping above (that is, to map $|a, b\rangle$ to $|a \wedge b\rangle$, for all $a, b \in\{0,1\}$ ).
5. General conversion from Stinespring form to Krauss form. Suppose that you are given a description of a quantum operation that takes an $n$-qubit state $\rho$ as input and produces an $n^{\prime}$-qubit state $\sigma$ as output, where the description is of the following form (where $n+m=n^{\prime}+m^{\prime}$ ):
i. Append an $m$ qubits, in state $\left|0^{m}\right\rangle$ to the end of the input state.
ii. Apply an $(n+m)$-qubit unitary operation $U$.
iii. Trace out the first $m^{\prime}$ qubits (resulting in an $n^{\prime}$-qubit output).

Show how to implement this in Krauss form as

$$
\begin{equation*}
\rho \mapsto \sum_{j \in S} A_{j} \rho A_{j}^{\dagger}, \tag{2}
\end{equation*}
$$

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 (I will assume that $A B$ means the matrix product of $A$ and $B$, as opposed to $A \otimes B$ ).

