CS 410/510 Introduction to Quantum Computing	
Homework 4	
Portland State U, Spring 2018	*May 16, 2018*
Lecturer: Fang Song	*Due: May 30, 2018*

Instructions. Your solutions will be graded on *correctness* and *clarity*. You should only submit work that you believe to be correct; if you cannot solve a problem completely, you will get significantly more partial credit if you clearly identify the gap(s) in your solution. It is good practice to start any long solution with an informal (but accurate) summary that describes the main idea. For this problem set, a random subset of problems will be graded. Problems marked with "**[G]**" are required for graduate students. Undergraduate students will get bonus points for solving them. Download the TeX file if you want to typeset your solutions using LaTeX.

You may collaborate with others on this problem set. However, you must ***write up your own solutions*** and ***list your collaborators*** for each problem.

1. (OR gate as a quantum operation) Recall the binary OR operation, denoted as $\vee$, defined as $a \vee b = 0$ if $a = b = 0$ and $a \vee b = 1$ otherwise. Here we consider operations that map the two-qubit state $|a,b\rangle$ to the one-qubit state $|a \vee b\rangle$, 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) (8 points) Give a sequence of 2×4 matrices $A_1, \dots, A_k$ with $\sum_{j=1}^{k} A_j^\dagger A_j = I$ that compute the OR operation in the sense that, for all $a,b \in \{0,1\}$, when $\rho = |a,b\rangle\langle a,b|$, $\sum_{j=1}^{k} A_j \rho A_j \dagger = |a \vee b\rangle\langle a \vee b|$.
   (b) (7 points) The operation from part (a) maps all basis states to pure states. Does it map all pure input states to pure output states? Prove it, or give a counterexample.

2. (Partial Trace) Let $Tr_Y(\cdot)$ be the operation of partial trace of a subsystem Y.
   (a) (5 points) Let $\rho_{AB} = \rho_A \otimes \rho_B$ with A and B both n-qubit systems. Show that $Tr_Y(\rho_{AB}) = \rho_A$.
   (b) (5 points) Let $|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}|00\rangle + |11\rangle$ be an EPR state. Compute $Tr_B(|\phi^+\rangle\langle\phi^+|)$.
   (c) (Bonus 5pts) Show that for any density operator ρ on a system A, there exists a pure state $|\psi\rangle$ on some larger system $A \otimes B$ such that $Tr_B(|\psi\rangle\langle\psi|) = \rho$.

3. (Quantum measurement)
   (a) (5 points) Let $|\phi_0\rangle = \frac{1}{\sqrt{2}}|00\rangle + |11\rangle$, $|\phi_1\rangle = \frac{1}{\sqrt{2}}|00\rangle - |11\rangle$, $|\phi_2\rangle = \frac{1}{\sqrt{2}}|01\rangle + |10\rangle$, and $|\phi_3\rangle = \frac{1}{\sqrt{2}}|01\rangle - |10\rangle$ be the four Bell states. We know that they form a basis

for 2-qubit systems. Find the measurement operators $M = \{M_0, M_1, M_2, M_3\}$, under the general measurement formalism, for the measurement under the Bell basis.

(b) (5 points) Continuing from above. Let ρ be a state on two qubits, and measure it under the Bell basis. When $\rho = |\psi\rangle\langle\psi|$ is a pure state, the measurement postulate states that the probability of observing outcome $i \in \{0, 1, 2, 3\}$ is $|\langle\psi|\phi_i\rangle|^2$. Show that for general density ρ, one observes i with probability $\langle\phi_i|\rho|\phi_i\rangle$. Verify that this probability also equals $Tr(M_i \rho M_i^+)$ for the M_i you identified in part a).

(c) (Bonus 10pts) (Simulating POVM) We've mentioned in class that any admissible quantum operation may be simulated by unitary operations and ordinary projective measurement under standard basis. In this problem, you will prove a special case, the POVM measurement. Recall in a POVM, we are only interested in the probabilities of observing each outcome, and dont care about how the state collapses afterward. Let's consider a POVM measurement specified by positive semi-definite operators $E_1, \ldots, E_m$ on n qubits satisfying $\sum_j E_j = I$. Let $m = 2^k$ for some integer k. Show how to simulate it by applying a unitary operation on a lager quantum system and then measuring under standard basis. (Hint: consider $m2^n \times 2^n$ matrix V formed by vertically stacking E_j. Show the columns are orthogonal, and extend V to a unitary of dimension $m2^n$.)

4. (Entropy) Let $H(\cdot)$ denote the Shannon entropy and $S(\cdot)$ be the von Neumann entropy. $S(A:B)$ denotes quantum mutual information.

   (a) (Exercise) Let X be a random variable taking values in $\{0, \ldots, 2^{m^2}\}$ with probability distribution $p_x = \begin{cases} 1 - 1/m & \text{if } x = 0 \\ \frac{1}{m2^{m^2}} & \text{otherwise} \end{cases}$. Calculate $H(X)$? Conclude that $H(X) \to \infty$ as $m \to \infty$, but one sample of X is almost certainly 0.

   (b) (5 points) Let $\rho = p|0\rangle\langle 0| + (1-p)|+\rangle\langle +|$. Compute $S(\rho)$. How does it compare to the entropy of a biased coin X which is HEADS with probability p?

   (c) (8 points) Consider $\rho_{AB} = \rho_A \otimes \rho_B$ where A and B are both n-qubit systems. Compute the von Neumann entropy $S(\rho_{AB})$ and the quantum mutual information $S(A:B)$.

5. (Quantum error-correcting)

   (a) (10 points) Let E be an arbitrary 1-qubit unitary, and I, X, Y, Z are the four 2×2 Pauli matrices.

      i) Show that it can be written as $E = \alpha_0 I + \alpha_1 X + \alpha_2 Y + \alpha_3 Z$, for some complex coefficients α_i with $\sum_{i=0}^{3} |\alpha_i|^2 = 1$. (Hint: compute the trace $Tr(E^\dagger E)$ in two ways, and use the fact that $Tr(AB) = 0$ if A and B are distinct Pauli matricies, and $Tr(AB) = Tr(I) = 2$ if A and B are the same Pauli.)

      ii) Write the 1-qubit Hadamard transform H as a linear combination of the four Pauli matrices.

(b) (10 points) Show that there cannot be a quantum code that encodes one logical qubit by $2k$ physical qubits while being able to correct errors on up to k of the qubits. (Hint: No-cloning theorem)

6. (Testing entanglement) Suppose that Alice and Bob share a two-qubit state, and they want to test if it is the EPR pair $|\phi^+\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ with local measurements and classical communication. Consider the following procedure: they randomly select a measurement basis: with probability $1/2$, they both measure in the standard basis $\{|0\rangle, |1\rangle\}$; and, with probability $1/2$, they both measure in the Hadamard (diagonal) basis $\{|+\rangle, |-\rangle\}$. Then they perform the measurement and they accept if and only if their outcomes are the same.

   (a) (5 points) Show that the state ϕ^+ is always accepted by this test with zero-error.

   (b) (8 points) Show that, for an arbitrary 2-qubit state $|\mu\rangle$, the probability that it passes the test is at most
   $$\frac{1 + |\langle\mu|\phi^+\rangle|^2}{2}.$$
   (Hint: decomposing $|\mu\rangle$ under the four Bell states.)

   (c) (7 points) Now consider another (malicious) party Eve, who may have intervened with the state that Alice shares with Bob. Let ρ_{ABE} be their joint state. Now assume that Alice and Bob are certain that they two perfectly share $|\phi^+\rangle$, show that Alice and Eve's state cannot be in $|\phi^+\rangle$ as well.

   Note: we can actually show that ρ_{ABE} must be of form $|\phi^+\rangle\langle\phi^+|_{AB} \otimes \rho_E$ (i.e., Eve's state is uncorrelated with that of Alice and Bob). This is an example of *monogamy of entanglement*: the more system A is entangled with B, the less A is entangled with another system C.