CS 410/510 Introduction to Quantum Computing

Homework 1

Portland State U, Spring 2017 — *Out: April 3, 2017*
Instructor: Fang Song — *Due: April 18, 2017*

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) "proof 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.

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. (Tensor product) Recall the *tensor product* of two matrices A and B is $A \otimes B := (a_{ij}B)$.
   (a) (5 points) Show that $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$.
   (b) (5 points) Show that if U and V are unitary matrices, then so is $U \otimes V$.

2. (Quantum states and gates)
   (a) (12 points) In each case, describe the resulting state. $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
      i) Apply H to the qubit $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.
      ii) Apply H to the first qubit of state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
      iii) Apply H to both qubits of $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
      iv) Apply $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$ to both qubits of state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
   (b) (10 points) (1-qubit gates) Let $X = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $Z = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.
      i) Suppose we have a qubit and we first apply X and then Z. Is it equivalent to first applying Z and then X?
      ii) Suppose we have two qubits. We apply X to both and then Z to both. Is it equivalent to applying Z to both and then applying X to both? Determine your answer by explicitly computing $X \otimes X$, $Z \otimes Z$, and their products both ways.
   (c) (8 points) (SWAP gate) A SWAP gate takes two inputs a and b and outputs b and a; i.e., it swaps the values of two input registers. Show how to build a SWAP gate using only CNOT gates. (Hint: youll need 3 of them.)

3. (Product states versus entangled states) In each of the following, either express the 2-qubit state as a tensor product of 1-qubit states or prove that it cannot be expressed this way.
   (a) (5 points) $\frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle - \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$
   (b) (5 points) $\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle$
   (c) (5 points) **[G]** $\frac{3}{4}|00\rangle + \frac{\sqrt{3}}{4}|01\rangle + \frac{\sqrt{3}}{4}|10\rangle + \frac{1}{4}|11\rangle$

4. (Distinguishing states by local measurements) In this question, we suppose Alice and Bob are physically separated from each other, and are each given one of the qubits of some 2-qubit state. Working as a team, they are required to distinguish between State I and State II with only local measurements. Namely they can each perform a local (one-qubit) unitary operation and then a measurement (in the computational basis) of their own qubit. After their measurements, they can send only classical bits to each other. (This is usually referred to as LOCC: local operation and classical communication.) In each case below, either give a perfect distinguishing procedure (that never errs) or explain why there is no perfect distinguishing procedure (i.e., that for any procedure the success probability must be less than 1).
   (a) (5 points) State I: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$; State II: $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$
   (b) (5 points) State I: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$; State II: $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$
   (c) (5 points) **[G]** State I: $\frac{1}{\sqrt{2}}(|00\rangle + i|11\rangle)$; State II: $\frac{1}{\sqrt{2}}(|00\rangle - i|11\rangle)$

5. (Simulating a biased coin) For $0 \leq p \leq 1$, let COIN_p denote a gate that has no input and one output, the output being a random bit which is 1 with probability p and 0 with probability $1 - p$. This question compairs the power of general COIN_p for an arbitrary rational p and the special case of fair coin gate $\text{COIN}_{1/2}$.
   (a) (10 points) In one sense, general COIN_p gates are more powerful than $\text{COIN}_{1/2}$ gates. Show that if we only allow $\text{COIN}_{1/2}$ gates (as well as AND, OR, NOT, etc.), it is impossible to construct a circuit that exactly simulates $\text{COIN}_{1/3}$.
   (b) (10 points) However, in another sense, COIN_p gates are not fundamentally more powerful than $\text{COIN}_{1/2}$. Show that for any $\varepsilon > 0$, there is a circuit of $\text{COIN}_{1/2}$ (and AND, OR, NOT etc.) of size $O(\log(1/\varepsilon)$ that almost exactly simulates a $\text{COIN}_{1/3}$ gate. Precisely, your circuit should have two output bits, called r and FAIL. The output bit FAIL should be 1 with probability at most ε And the output bit r should have the property that $\Pr[r = 1|\text{FAIL} \neq 1] = 1/3$ exactly.

      (Note: once you've figured how to do it for $1/3$, I believe you'll be able to do so for any rational value p.)