CS333 - Problem Set 6

1. Alice and Bob would like to share the entangled state $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Unfortunately, they do not initially share any entanglement. But fortunately, they have a mutual friend, Charlie, who shares a copy of $|\beta_{00}\rangle$ with Alice and another copy of $|\beta_{00}\rangle$ with Bob.

   (a) Write the initial state using ket notation as a superposition of standard basis states, and use subscripts to indicate which qubit is in which person's posession. The first qubit should belong to Alice, the second and third qubits belong to Charlie (the second is entangled with Alice's qubit and the third is entangled with Bob's qubit), and the fourth qubit belongs to Bob.

   (b) Suppose Charlie performs a Bell measurement on his two qubits (one of which is entangled with Alice and the other of which is entangled with Bob). For each possible measurement outcome, give the probability with which it occurs and the resulting post-measurement state for Alice and Bob. Note the Bell measurement uses the basis:

$$\begin{aligned}
|\beta_{00}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
|\beta_{01}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\
|\beta_{10}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\
|\beta_{11}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)
\end{aligned} \tag{1}$$

   (c) Consider the system after Charlie's measurement, and design a protocol whereby Charlie sends a classical message to Alice, and Alice applies a unitary to her quantum state based on that message, such that after doing this, Alice and Bob share the state $|\beta_{00}\rangle$.

2. In class, we will discuss how classical probabilistic computation can be represented mathematically using vectors to represent the state of the system, and left stochastic matrices to represent operations. In this problem, we'll examine a similar approach for reversible deterministic (non-probabilisitc) classical computation. If the system consists of n bits, and those bits are in the state $s \in \{0,1\}^n$ (i.e. s is some n bit string), then we can represent s using the vector $|s\rangle$ that is length 2^n and contains all 0s except for a 1 in the sth position. ($|s\rangle$ doesn't represent a quantum state, but just represents the standard basis vector). In this reperesentation, deterministic gates are reversible matrices.

   (a) What class of matrices describe the set of possible gates in this model? (For example, in the case of quantum, we had *unitary*, in the case of probabilistic, we had *left stochastic*.)

(b) Please give a matrix representation of each of the following gates:

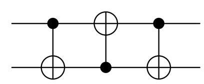
i. NOT (acts on a single bit and flips the value)

ii. TOFFOLI (acts on 3 bits and flips the value of the third bit if both of the first bits have value 1)

(c) NOT and TOFFOLI are universal, which means that any deterministic (non-random) classical computation can be implemented using just these gates. Are the matrices from part (b) also valid left stochastic matrices? Are these matrices also valid unitaries? Based on your answers, please comment on the ability of probabilistic computers to simulate deterministic computers, and the ability of quantum computers to simulate determistic computers. If it is possible to do this simulation, explain how you would do it.

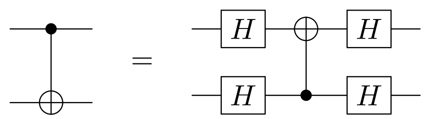
3. CNOT properties:

(a) What does the following circuit do? (Your answer should be a simple description in English, not math.)



(2)

(b) Prove the following two circuits are equal.



(3)

(If you would like to use ket-bra notation for the analysis, it is helpful to know that $|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$ and $X = |+\rangle\langle +| - |-\rangle\langle -|$.)

(c) Which qubit is the control qubit in the CNOT gate?

4. In class, I said that you can do universal quantum computation with a circuit which always starts with n qubits prepared as $|0\rangle^{\otimes n}$, applies a unitary U, and always measures each qubit in the standard basis. However, perhaps the optimal computation calls for starting with a state $|\psi\rangle \neq |0\rangle^{\otimes n}$, applying a unitary V, and then measuring in a basis $\{|\phi_0\rangle, |\phi_1\rangle, \dots, |\phi_{2^n-1}\rangle\}$. In this question, you will describe how you can implement the ideal circuit by starting with the state $|0\rangle^{\otimes n}$, applying a unitary V_{prep}, then the unitary V, and then a unitary V_{meas}, followed by a measurement in the standard basis. In other words, the unitary we apply between state preparation and final measurement is $V_{meas} V V_{prep}$. (For this question, ignore the fact that we can only approximately implement any unitary - instead assume that we can exactly implement any unitary.)

(a) If $\{|\phi_1\rangle, |\phi_2\rangle, |\phi_{2^n}\rangle, \}$ and $\{|\psi_1\rangle, |\psi_2\rangle, \dots, |\psi_{2^n}\rangle\}$ are each an orthonormal basis for an n-qubit system, show that $U = \sum_{i=1}^{2^n} |\psi_i\rangle\langle\phi_i|$ is a unitary.

(b) Please give a description of a unitary V_{prep}, and explain why it works. (Part (a) is helpful here!)

(c) Please give a description of a unitary V_{meas}, and explain why it works. (Part (a) is helpful here!)