Quantum Computation **CMU 15-859BB, Fall 2015**

Homework 2

Due: Tuesday September 22, 11:59pm, email the pdf to pgarriso@andrew.cmu.edu

---

Solve any 5 out of 7

1. **[The square-root of NOT.]**

   (a) Let $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, the matrix for a 1-qubit NOT gate. Find a 2×2 matrix V (i.e., 1-qubit gate) such that $V^2 = X$.

   (b) Let CV denote a "Controlled-V" gate. By this we mean a 2-qubit gate defined by the following property: if the input is $|0\rangle \otimes |\psi\rangle$ then the output is $|0\rangle \otimes |\psi\rangle$ and if the input is $|1\rangle \otimes |\psi\rangle$ then the output is $|1\rangle \otimes (V |\psi\rangle)$. Write the unitary matrix representing CV.

   (c) Show how to build a Toffoli (CCNOT) gate using CNOT gates and CV gates.

2. **[Linear algebra formulation of randomized circuits.]** In Lecture 2 we discussed the linear-algebraic way to formalize quantum states and circuits: the state of n qubits is represented by a ket $|\psi\rangle \in \mathbb{C}^{2^n}$ with $\langle\psi|\psi\rangle = 1$, a gate operating on k qubits may be any $2^k \times 2^k$ unitary matrix, etc. Describe the analogous linear-algebraic way to formalize *randomized* states and circuits. Assume for simplicity that all circuits operate on n randomized-bits and each gate has the same number of inputs as outputs. How does one represent the state of the bits with a vector? What properties does a legal state vector satisfy? How does one represent a (possibly randomized) gate with k input/output bits? What properties does a legal such gate satisfy? If one gate A is applied to the first m randomized-bits and another gate B is applied to some other m' randomize-bits, how do we represent the overall transformation on $m + m'$ randomized-bits? Give examples to illustrate your explanations.

3. **[Tensor products.]** Let A and B be matrices (not necessarily square). Suppose A's rows and columns are indexed by sets I_A and J_A, respectively (the most typical case being $I_A = \{1, 2, \dots, m\}$ and $J_A = \{1, 2, \dots, n\}$). Similarly, suppose B's rows and columns are indexed by sets I_B and J_B. Then $A \otimes B$ is the matrix whose rows are indexed by pairs from $I_A \times I_B$ and whose columns are indexed by pairs from $J_A \times J_B$ and whose $((i, i'), (j, j'))$-th entry is $A_{i,j}B_{i',j'}$. Pictorially, $A \otimes B$ is given by the matrix

$$\begin{bmatrix} A_{1,1}B & \dots & A_{1,m_1}B \\ \vdots & \ddots & \vdots \\ A_{\ell_1,1}B & \dots & A_{\ell_1,m_1}B \end{bmatrix} = \left[\begin{array}{ccccccc} A_{1,1}B_{1,1} & \dots & A_{1,1}B_{1,m_2} & & A_{1,m_1}B_{1,1} & \dots & A_{1,m_1}B_{1,m_2} \\ \vdots & \ddots & \vdots & \cdots & \vdots & \ddots & \vdots \\ A_{1,1}B_{\ell_2,1} & \dots & A_{1,1}B_{\ell_2,m_2} & & A_{1,m_1}B_{\ell_2,1} & \dots & A_{1,m_1}B_{\ell_2,m_2} \\ & \vdots & & \ddots & & \vdots & \\ A_{\ell_1,1}B_{1,1} & \dots & A_{\ell_1,1}B_{1,m_2} & & A_{\ell_1,m_1}B_{1,1} & \dots & A_{\ell_1,m_1}B_{1,m_2} \\ \vdots & \ddots & \vdots & \cdots & \vdots & \ddots & \vdots \\ A_{\ell_1,1}B_{\ell_2,1} & \dots & A_{\ell_1,1}B_{\ell_2,m_2} & & A_{\ell_1,m_1}B_{\ell_2,1} & \dots & A_{\ell_1,m_1}B_{\ell_2,m_2} \end{array}\right].$$

   (a) Show that $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$.

(b) Show that $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$. (This assumes of course that $J_A = I_C$ and $J_B = I_D$.) Note that in the special case of $|J_C| = |J_D| = 1$, we see that for any two unitary operators U_1, U_2 and quantum states $|\psi_1\rangle, |\psi_2\rangle$, we have that

$$(U_1 \otimes U_2)(|\psi_1\rangle \otimes |\psi_2\rangle) = (U_1|\psi_1\rangle) \otimes (U_2|\psi_2\rangle).$$

(c) Show that if A and B are invertible then so is $(A \otimes B)$, and $(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$.

(d) Show that if U and V are unitary then so is $U \otimes V$.

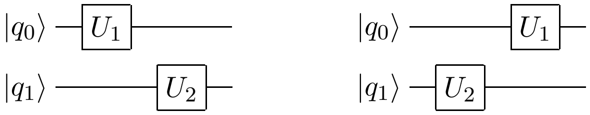
(e) Show that the state

$$\tfrac{1}{\sqrt{2}}|00\rangle + \tfrac{1}{\sqrt{2}}|11\rangle$$

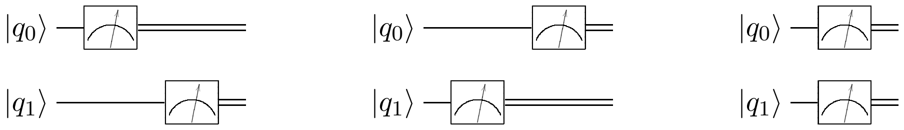
is not expressible as the tensor product of two states $|\psi_1\rangle, |\psi_2\rangle \in \mathbb{C}^2$. In general, a multi-qubit state which is not expressible as the tensor product of individual qubit states is known as an *entangled* state.

4. [**Operations applied to separate systems can be done in any order.**]

(a) Show that the following two circuits output the same state, assuming that the (possibly entangled) 2-qubit system is described by some state $|\psi\rangle$.



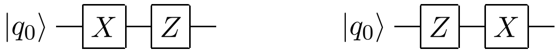
(b) Show that given a (possibly entangled) 2-qubit system described by some state $|\psi\rangle$, the order in which one decides to measure the two qubits is irrelevant. In other words, show that the following three circuits output the same distribution on pairs of classical bits.



The final circuit measures both qubits simultaneously, as in Lecture 1.

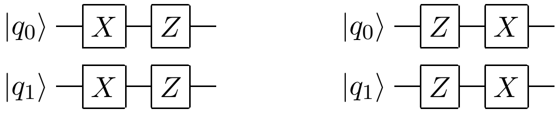
5. [**More practice with 1-qubit gates.**] As before, let $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and let $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

(a) Suppose we have a qubit and we first apply X and then Z. Is this equivalent to first applying Z and then applying X? In other words, are the following two circuits equivalent?



Determine your answer by explicitly computing ZX and XZ.

(b) Suppose we have two qubits; we apply X to both, and then we apply Z to both. Is this equivalent to first applying Z to both and then applying X to both? In other words, are the following two circuits equivalent?



Determine your answer by explicitly computing $X \otimes X$, $Z \otimes Z$, and their products both ways.

6. **[Fun with outer products.]** (Recall the notation $A^\dagger$ for the conjugate transpose of the matrix A.)

   (a) Suppose $A \in \mathbb{C}^{n\times m}$ has columns $|u_1\rangle, \dots, |u_m\rangle$ and $B \in \mathbb{C}^{n\times m}$ has columns $|v_1\rangle, \dots, |v_m\rangle$, i.e.,
   $$A = \begin{bmatrix} | & | & & | \\ u_1 & u_2 & \dots & u_m \\ | & | & & | \end{bmatrix}, \qquad \text{and} \qquad B = \begin{bmatrix} | & | & & | \\ v_1 & v_2 & \dots & v_m \\ | & | & & | \end{bmatrix}.$$
   Show that $AB^\dagger = \sum_{i=1}^m |u_i\rangle\langle v_i|$.

   (b) A *projection matrix* $\Pi \in \mathbb{C}^{n\times n}$ is a matrix such that $\Pi^2 = \Pi$. Supposing Π is Hermitian (i.e., $\Pi^\dagger = \Pi$), show that Π is a projection matrix if and only if $\Pi = \sum_{i=1}^k |v_i\rangle\langle v_i|$ for some orthonormal vectors $|v_1\rangle, \dots, |v_k\rangle \in \mathbb{C}^n$. What is the effect of applying Π to a vector $|w\rangle \in \mathbb{C}^n$?

   (c) Suppose $|v_1\rangle, \dots, |v_n\rangle \in \mathbb{C}^n$ form an orthonormal basis. Show that $\sum_{i=1}^n |v_i\rangle\langle v_i|$ is the identity matrix.

   (d) A matrix M is *norm-preserving* if for every vector $|w\rangle$ it holds that $M|w\rangle$ has the same Euclidean length as $|w\rangle$. Suppose $|v_1\rangle, \dots, |v_n\rangle \in \mathbb{C}^n$ is an orthonormal basis of $\mathbb{C}^n$. Determine with proof what condition(s) on the numbers $a_1, \dots, a_n \in \mathbb{C}$ are necessary and sufficient for
   $$M = \sum_{i=1}^n a_i |v_i\rangle\langle v_i|$$
   to be norm-preserving. Norm-preserving real-valued matrices are known as *orthogonal* matrices, whereas norm-preserving complex-valued matrices are known as *unitary* matrices.

7. **[Dan, Mike, and Tony's game.]** This problem is devoted to a scenario similar to the CHSH Game. Best friends Alice, Bob, and Charlie are several light-seconds apart. Each of them is together with a referee. At the stroke of midnight, the three referees generate uniformly random bits $x, y, z \in \{0,1\}$ subject to the promise that $x \oplus y \oplus z = 0$.[1] Alice is told x, Bob is told y, Charlie is told z. Within less than a millisecond, each of them must reply — Alice with a bit a, Bob with a bit b, and Charlie with a bit c. Then everybody gets together and compares notes: if $a \oplus b \oplus c = x \vee y \vee z$ then Alice, Bob, and Charlie collectively "win"; otherwise, they collectively "lose".

   (a) Assume that Alice, Bob, and Charlie can agree on a strategy beforehand, but during the game they cannot communicate and must act deterministically. Prove that no matter their strategy, they can win with probability at most $\frac{3}{4}$.

   (b) Now suppose that Alice, Bob, and Charlie initially prepare a 3-qubit system in the state $\frac{1}{\sqrt{2}}|000\rangle + \frac{1}{\sqrt{2}}|111\rangle$, and they each take one of the qubits with them before the game starts. Their idea is that upon receiving their "question" (x, y, or z) they will apply a certain unitary gate to their qubit, measure it, and respond with the measurement result. Prove that there is a strategy for Alice, Bob, and Charlie that will allow them to

[1] Since the referees are also light-seconds apart, there's no way they can actually do this for sure: if, say, each referee generates their bit uniformly at random, the probability the promise is satisfied is only $\frac{1}{2}$. So in practice, what the referees will do is the following. They'll play this game a few hundred times, once a millisecond, always generating uniformly random bits, and recording the results. Then once everything is over, the referees meet up, compare notes, and discard all rounds (approximately half of them) in which the promise wasn't satisfied.

win with certainty! (Hint: it's possible for them to all use the same strategy — i.e., use the same gate when seeing a 0 and the same gate when seeing a 1.)