6.845 Problem Set 1: Quantum Basics

1. **Stochastic and unitary matrices.**

   (a) Show that a matrix $A \in \mathbb{R}^{n\times n}$ maps every nonnegative vector $v \in \mathbb{R}^n_{\geq 0}$ to a nonnegative vector Av with the same L_1-norm, if and only if A is *stochastic* (that is, A is a nonnegative matrix all of whose columns sum to 1).

   (b) Show that a matrix $U \in \mathbb{C}^{n\times n}$ maps every vector $v \in \mathbb{C}^n$ to a vector Uv with the same L_2-norm, if and only if U is *unitary* (that is, $UU^\dagger = I$, where $U^\dagger$ denotes the conjugate transpose of U).

2. **Perfectly-distinguishable quantum states.** Show that there exists a measurement to distinguish the quantum states $|\psi\rangle$ and $|\varphi\rangle$ with certainty, if and only if $\langle\psi|\varphi\rangle = 0$.

3. **GHZ paradox.** Consider the following game: Alice, Bob, and Charlie are given input bits a, b, and c respectively. They are promised that $a \oplus b \oplus c = 0$ (where $\oplus$ denotes addition mod 2). Their goal is to output bits x, y, and z respectively such that $x \oplus y \oplus z = a \vee b \vee c$. They can agree on a strategy in advance but cannot communicate after receiving their inputs.

   (a) Show that in a classical universe, there is no strategy that enables them to win this game with certainty.

   (b) Suppose Alice, Bob, and Charlie share the entangled state

   $$\frac{1}{2}\left(|000\rangle - |011\rangle - |101\rangle - |110\rangle\right).$$

   Show that *now* there exists a strategy by which they can win the game with certainty. [*Hint:* Have each player measure its qubit in the standard basis if its input bit is 0, or the Hadamard basis if its input bit is 1.]

4. **Density matrices.** Suppose we don't know which quantum state we have, and instead just have a probability distribution in which the state $|\psi_i\rangle = \alpha_{i1}|1\rangle + \cdots + \alpha_{in}|n\rangle$ occurs with probability p_i, for all $i \in \{1,\ldots,m\}$. (Here $p_1 + \cdots + p_m = 1$.) Consider the $n \times n$ matrix

   $$\rho = \sum_{i=1}^{m} p_i |\psi_i\rangle\langle\psi_i| = \sum_{i=1}^{m} p_i \begin{pmatrix} \alpha_{i1}\alpha_{i1}^* & \cdots & \alpha_{i1}\alpha_{in}^* \\ \vdots & \ddots & \vdots \\ \alpha_{in}\alpha_{i1}^* & \cdots & \alpha_{in}\alpha_{in}^* \end{pmatrix}$$

   (where * denotes complex conjugate). We call ρ the *density matrix* corresponding to the *ensemble* $\{|\psi_i\rangle, p_i\}$.

   (a) Show that if we measure a quantum system with density matrix ρ in the standard basis, we get outcome $|i\rangle$ with probability $(\rho)_{ii}$ (i.e., the (i,i) entry of ρ).

   (b) Show that if we apply the unitary U to a system with density matrix ρ, then the density matrix of the transformed system is $U\rho U^\dagger$ (where $\dagger$ denotes conjugate transpose).

(c) Conclude that if two ensembles have the same density matrix, then no experiment can distinguish them. And more concretely, that no experiment can distinguish the uniform distribution over the states $|0\rangle$ and $|1\rangle$, from the uniform distribution over the states $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$. [*Note:* Here and throughout this pset, you can assume that "experiment" means a unitary transformation followed by a standard-basis measurement. This assumption turns out to be without loss of generality, so long as we're working in a space of large enough dimension.]

(d) *[Extra credit]* Show that if two ensembles have different density matrices, then there *is* an experiment that can distinguish them.

5. **No-communication theorem.** Quantum mechanics is a *local* theory, in the sense that not even entanglement can be used to communicate information faster than light. However, this is not quite immediate but is a theorem that has to be proved.

(a) Consider a state $|\psi\rangle = \sum_{i,j=1}^{n} \alpha_{ij} |i\rangle |j\rangle$, which involves two registers (possibly entangled with each other). Explain why no operation that we perform on the first register only (including unitaries and measurements), can affect the probability of any outcome of a standard-basis measurement on the second register only. [*Hint:* Write out the α_{ij}'s as an $n \times n$ matrix. What is the effect of an operation on the first register only?]

(b) Show that unitary operations on separate subsystems commute with each other: that is, $(U \otimes I)(I \otimes V) = (I \otimes V)(U \otimes I)$ for all U, V.

(c) Combining parts a. and b. conclude that no unitary transformation or measurement performed on the first register only, can affect the outcome of an experiment on the second register only.

6. "**Uniqueness of quantum mechanics.**" We talked in class about how the 1-norm (the basis for classical probability theory) and the 2-norm (the basis for quantum mechanics) are somehow "special." Here we will try to justify that statement. Call a linear transformation $A \in \mathbb{R}^{n \times n}$ *trivial* if it has the form PD, where P is a permutation matrix and D is a diagonal matrix.

(a) Prove that the only linear transformations on $\mathbb{R}^n$ that preserve the 4-norm (i.e. $\alpha_1^4 + \cdots + \alpha_n^4$) are trivial. [*Hint:* Write out the assumption that a matrix $A \in \mathbb{R}^{n \times n}$ preserves the 4-norm as a set of constraints on the entries of A. Can you find a subset of those constraints that forces A to be trivial?]

(b) Generalize part a. to the k-norm for all even integers $k \geq 4$. (Indeed, the result can even be generalized to the p-norm for all nonnegative reals $p \notin \{1, 2\}$, but you are not being asked to prove that.)

(c) *[Extra credit]* Show that, if we want to preserve the norm of *arbitrary* vectors $v \in \mathbb{R}^n$ (not just nonnegative vectors), then there does not even exist a nontrivial linear transformation $A \in \mathbb{R}^{n \times n}$ that preserves the 1-norm.

6.845 Quantum Complexity Theory
Fall 2010