ASSIGNMENT 4 CMSC 858K (Fall 2016)

Due in class on Thursday, Nov 3.

1. *Complete problems for* BQP. We say that a language L is *complete* for a complexity class C (or that L is C-complete) if $L \in \mathsf{C}$ and every problem in C can be reduced to L in (classical, deterministic) polynomial time. In class, we discussed the notion of NP-complete problems such as 3SAT. In this problem we explore the notion of complete problems for BQP.

   In a *promise problem*, our goal is to distinguish "yes" from "no" instances subject to a promise about the input. We specify such a problem by a pair of languages $(L_{\text{yes}}, L_{\text{no}}) \subseteq \{0,1\}^* \times \{0,1\}^*$ such that $L_{\text{yes}} \cap L_{\text{no}} = \varnothing$ (but we do not require that $L_{\text{yes}} \cup L_{\text{no}} = \{0,1\}^*$).

   (a) [3 points] Let PromiseBQP be the set of promise problems that can be decided by a BQP machine. More formally, we say $(L_{\text{yes}}, L_{\text{no}}) \in \mathsf{PromiseBQP}$ if there is a polynomial-time quantum algorithm that, on input x, outputs "yes" with probability at least $2/3$ if $x \in L_{\text{yes}}$ and outputs "no" with probability at least $2/3$ if $x \in L_{\text{no}}$. Give an example of a PromiseBQP-complete problem. (It's okay if your problem is trivial, i.e., its PromiseBQP-completeness may follow straightforwadly from the definition, but you should still prove that the problem is PromiseBQP-complete.)

   (b) [1 point] Do you think that there are complete problems for the (non-promise) class BQP? Explain why it might be difficult to find such a problem.

2. *Comparing quantum analogs of* NP. [5 points] In class, we learned that there are several versions of the quantum analog of the complexity class NP. Draw a containment diagram of the complexity classes $\mathsf{QMA}, \mathsf{QCMA}, \mathsf{QMA}_1$, and $\mathsf{QMA}(2)$. Justify your choices of containment. You may use the fact that $\mathsf{QCMA}_1 = \mathsf{QCMA}$.

3. *Improved upper bound on* BQP. In class, we argued that $\mathsf{BQP} \subseteq \mathsf{PSPACE}$. In this problem we will find a stronger bound.

   The class PP of probabilistic polynomial-time computations (with unbounded error, as opposed to BPP which has bounded error) is the set of languages $L \subseteq \{0,1\}^*$ for which there exists a randomized algorithm A satisfying

   - $\forall\, x \in L$, $A(x)$ accepts with probability $> 1/2$ and
   - $\forall\, x \notin L$, $A(x)$ rejects with probability $> 1/2$ (i.e., accepts with probability $\leq 1/2$).

   (a) [2 points] Prove that $\mathsf{PP} \subseteq \mathsf{PSPACE}$.

   (b) [3 points] Prove that $\mathsf{BQP} \subseteq \mathsf{PP}$.

4. *Density matrices.* Consider the ensemble in which the state $|0\rangle$ occurs with probability $3/5$ and the state $(|0\rangle + |1\rangle)/\sqrt{2}$ occurs with probability $2/5$.

   (a) [2 points] What is the density matrix ρ of this ensemble?

   (b) [2 points] Write ρ in the form $\frac{1}{2}(I + r_x X + r_y Y + r_z Z)$, and plot ρ as a point in the Bloch sphere.

   (c) [3 points] Suppose we measure the state in the computational basis. What is the probability of getting the outcome 0? Compute this both by averaging over the ensemble of pure states and by computing $\mathrm{Tr}(\rho |0\rangle\langle 0|)$, and show that the results are consistent.

(d) [3 points] How does the density matrix change if we apply the Hadamard gate? Compute this both by applying the Hadamard gate to each pure state in the ensemble and finding the corresponding density matrix, and by computing $H\rho H^\dagger$.

5. *Local operations and the partial trace.*

   (a) [4 points] Let $|\psi\rangle = \frac{\sqrt{3}}{2}|00\rangle + \frac{1}{2}|11\rangle$. Let ρ denote the density matrix of $|\psi\rangle$ and let ρ' denote the density matrix of $(I \otimes H)|\psi\rangle$. Compute ρ and ρ'.

   (b) [3 points] Compute $\mathrm{Tr}_B(\rho)$ and $\mathrm{Tr}_B(\rho')$, where B refers to the second qubit.

   (c) [4 points] Let ρ be a density matrix for a quantum system with a bipartite state space $A \otimes B$. Let I denote the identity operation on system A, and let U be a unitary operation on system B. Prove that $\mathrm{Tr}_B(\rho) = \mathrm{Tr}_B((I \otimes U)\rho(I \otimes U^\dagger))$.

   (d) [4 points] Show that the converse of part (c) holds for pure states. In other words, show that if $|\psi\rangle$ and $|\phi\rangle$ are bipartite pure states, and $\mathrm{Tr}_B(|\psi\rangle\langle\psi|) = \mathrm{Tr}_B(|\phi\rangle\langle\phi|)$, then there is a unitary operation U acting on system B such that $|\phi\rangle = (I \otimes U)|\psi\rangle$.

   (e) [2 points] Does the converse of part (c) hold for general density matrices? Prove or provide a counterexample.

6. *Unambiguous state discrimination.* In this problem, we will explore a task for which POVMs outperform orthogonal measurement. As in problem 4 of Assignment 1, fix some angle θ, and suppose someone flips a fair coin and, depending on the outcome, gives you the state

$$|0\rangle \qquad \text{or} \qquad \cos\theta|0\rangle + \sin\theta|1\rangle$$

   (but does not tell you which).

   (a) [2 points] Show that if $\theta \in [0, \pi/2)$, no orthogonal measurement can distinguish between the states perfectly.

   (b) [3 points] Show that there is an orthogonal measurement that *unambiguously discriminates* the states for any $\theta \in (0, \pi/2)$, meaning that if it reports an answer, it is guaranteed to be correct, but it is allowed to sometimes report that the measurement was inconclusive. What is the probability of obtaining an inconclusive result with an unambiguous discrimination procedure using orthogonal measurement?

   (c) [3 points] Now suppose we try to unambiguously discriminate the states using a POVM. What is the best possible success probability? Compare your answer to that of the previous part.

   (d) [3 bonus points] Describe how to implement the optimal POVM of the previous part using a unitary interaction with an ancilla followed by an orthogonal measurement.