CSCI 7000-005 Computational Complexity
Problem Set 5

Alexandra Kolla

Due December 13.

Collaboration Policy: The homework can be worked on in groups of up to 3 students each (2 would be optimal, but 1 and 3 are both accepted).

One submission per team is sufficient. Please write the solution for each of the problems on a separate sheet of paper. Write your team's names and id on each submission and please **staple** all the sheets together.

Submissions should be written in LaTeX, unless your handwriting is indistinguishable from LaTeX.

Homework is due before the end of class. Only one late homework per person will be allowed. If you submit more than one homework late, you will get no grade for the excess late homeworks.

Problem 1 (25 pts)

(GHZ paradox.) Consider the following game: Alice, Bob, and Charlie are given input bits a, b, and c respectively. They are promised that $a \oplus b \oplus c = 0$. 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.

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

2. Suppose Alice, Bob, and Charlie share the entangled state

$$1/2(|000\rangle - |011\rangle - |101\rangle - |110\rangle)$$

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

Problem 2 (25 pts)

(Conjugating CNOT.) Show that if you apply Hadamard gates to qubits A and B, followed by a CNOT gate from A to B, followed by Hadamard gates to A and B again, the end result is the same as if you had applied a CNOT gate from B to A. The above illustrates a principle of quantum mechanics you have heard about: that any physical interaction by which A influences B can also cause B to influence A (so for example, it is impossible to measure a particles state without affecting it).

Problem 3 (25 pts)

Say a problem B is complete for the complexity class $\mathcal{C}$ if (i) B is in $\mathcal{C}$, and (ii) every problem in $\mathcal{C}$ can be reduced to B in deterministic polynomial time.

1. Let PromiseBQP be the class of promise problems efficiently solvable by a quantum computer: that is, the set of all ordered pairs $\Pi_{\text{YES}} \subseteq \{0,1\}^*, \Pi_{\text{NO}} \subseteq \{0,1\}^*$ such that

   - $\Pi_{\text{YES}} \cap \Pi_{\text{NO}} = \emptyset$
   - There exists a uniform family of polynomial-size quantum circuits that decides, given an input x, whether $x \in \Pi_{\text{YES}}$ or $x \in \Pi_{\text{NO}}$ with bounded probability of error, promised that one of these is the case.

   Give an example of a promise problem thats complete for PromiseBQP. [Hint: This problem just requires understanding the definitions; it does not require cleverness.]

2. Explain the basic difficulty in finding a language $L \subseteq \{0,1\}^*$ that is complete for BQP.