CPSC 421/501 Intro to Theory of Computing (Term 1, 2013-14)
Assignment 7

Due: Wednesday November 27th, in class.

Question 1: [10 marks] Let $DUMBPP$ be the complexity class for with $L \in DUMBPP$ if and only if there is a TM for which

$$x \in L \implies \Pr[\, M \text{ accepts } x\,] < 1/3$$
$$x \notin L \implies \Pr[\, M \text{ rejects } x\,] < 1/3$$

What complexity class does $DUMBPP$ equal? Briefly explain your answer.

Question 2: [10 marks] Consider the following purported proof that $BPP \cap NP = RP$.

Proof. We already saw in class that $RP \subseteq BPP$ and $RP \subseteq NP$, so $RP \subseteq BPP \cap NP$.

Now consider any $L \in BPP \cap NP$. Every string $x \in L$ can be accepted with probability at least 2/3 since $L \in BPP$. Every string $x \notin L$ can be rejected with probability 1 since $L \in NP$. These acceptance/rejection probabilities are the same as in definition of RP, so $L \in RP$. So $BPP \cap NP \subseteq RP$. $\square$

Is this a valid proof? If so, explain how it can be made precise. If not, explain what the flaw is. In either case, ensure that your answer is explained carefully.

Question 3: [10 marks] Let $G = (V, E)$ and $H = (W, F)$ be two undirected graphs with $|V| = |W| = n$. We say that G and H are isomorphic if there is a bijection $\pi : V \to W$ such that

$$\{u, v\} \in E \quad \Leftrightarrow \quad \{\pi(u), \pi(v)\} \in F.$$

Consider the communication complexity problem ISO_n, where Alice is given a graph G, Bob is given the graph H, and they must decide if G and H are isomorphic.

- **(a):** Prove that $D(ISO_n) \le O(n^2)$.
- **(b):** Prove that $D(ISO_n) \ge \Omega(n^2)$.
  Hint: Isomorphism is an equivalence relation on the set of n-vertex graphs. Every equivalence class has size at most $n!$, so the number of equivalence classes is at least $2^{\binom{n}{2}}/n!$.

Question 4: Recall the "combinatorial auction" problem. The items for auction are $U = \{1, \ldots, n\}$. There are two bidders, and bidder i has valuation function $v_i : 2^U \to \mathbb{R}$. (For simplicity, let us even assume $v_i : 2^U \to \{0, 1\}$.) The goal is to compute $\max_{S \subseteq U}(v_1(S) + v_2(U \setminus S))$.

- **(a):** [10 marks] In this question, we will prove that the bidders must exchange $2^{\Omega(n)}$ bits in order to solve the combinatorial auction problem. To do so, perform a reduction from the Disjointness problem. (Specifically, consider $DISJ_\ell$ with $\ell = 2^n$. Alice receives $A \subseteq \{1, \ldots, \ell\}$ and Bob receives $B \subseteq \{1, \ldots, \ell\}$. They must decide whether $A \cap B = \emptyset$.)
  Hint: Let $\pi : 2^U \to \{1, \ldots, \ell\}$ be an arbitrary bijection. Define a valuation function for Alice using A and π, and define a valuation function for Bob using B and π.
- **(b):** **OPTIONAL** [5 marks]
  It is a natural assumption in auctions that valuation functions are **monotone** (i.e., $v_i(A) \le v_i(B)$ if $A \subseteq B$). Intuitively, one should place more value on owning more items. Prove that the $2^{\Omega(n)}$ lower bound still holds, even under the restriction that v_1 and v_2 are both monotone.
  Hint: Let $\ell = \binom{n}{n/2}$. Consider only subsets A and B with $|A| = |B| = n/2$.

OPTIONAL BONUS QUESTIONS:

Question 5: [20 marks]

Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be given by $f(x,y) = 1$ iff $\sum_i x_i y_i \equiv 0 \pmod{2011}$. Prove that f has no fooling set larger than n^c, for some constant c.

Relevant ideas are contained in Sherstov's lecture 3.
`http://www.cs.ucla.edu/~sherstov/teaching/2012-winter/docs/lecture03.pdf`.

Question 6: [20 marks]

Let us briefly define randomized communication complexity of a function $f : X \times Y \to \{0,1\}$. Alice receives her input $x \in X$ and Bob receives his input $y \in Y$. In a randomized protocol for deciding f, Alice also receives a string $r_A \in \{0,1\}^k$ and Bob also receives a string $r_B \in \{0,1\}^k$, for some integer k. So Alice's combined input is (x, r_A) and Bob's combined input is (y, r_B). We assume that r_A and r_B are chosen independently and uniformly at random from $\{0,1\}^k$.

A randomized protocol P decides f with two-sided error ϵ if, for all $x \in X$ and $y \in Y$,

$$\Pr[\,\text{protocol } P \text{ on input } (x,y) \text{ fails to output } f(x,y)\,] \;\leq\; \epsilon.$$

Here the probability is over the random choice of r_A and r_B. The **cost of** P is the maximum number of bits sent by P over all $x \in X$, $y \in Y$, $r_A \in \{0,1\}^k$ and $r_B \in \{0,1\}^k$. The **ϵ-error randomized communication complexity** of f is the minimum cost of P, over all protocols P that decide f with two-sided error ϵ. This quantity is denoted $R_\epsilon^{\text{two}}(f)$.

Let ϵ and ϵ' satisfy $0 < \epsilon \leq \epsilon' < 1/2$. Set $T = 4\log(1/\epsilon) \cdot (1/2 - \epsilon')^{-2}$. Prove that $R_\epsilon^{\text{two}}(f) \leq T \cdot R_{\epsilon'}^{\text{two}}(f)$.

Hint: Execute the best ϵ'-error protocol T times and take the majority vote.