Assignment 4

COMP 531 Winter 2016

Due March 30th

1. The probabilistic method is a technique to prove the existence of objects with desired combinatorial properties. The idea is to define a suitable probability distribution in which the probability of finding the desired properties is nonzero. As an illustration of the method, consider the following exercise: Let $G = (V, E)$ be any graph that has a matching M (a matching is a collection of edges, no two of which are adjacent to the same vertex). Show that G contains a subgraph H, where H is bipartite and contains at least $|E| + |M|$ edges.

   (Hint: Think of a random bipartition scheme of the set of vertices of G such that you guarantee that each edge of the matching has its endpoints on opposite edges of the partition. Calculate the expected number of edges of G that have their endpoints in opposite partitions.)

2. Consider a problem $\{f_n\}$ such that we have a randomized protocol P with

   $$Pr[P(x, y, r) \neq f_n(x, y)] \leq \frac{1}{3}$$

   Show that there is a randomized protocol $Q(x, y, r)$ which uses only $|r| = O(logn)$ random bits, and still achieves

   $$Pr[P(x, y, r) \neq f_n(x, y)] \leq \frac{1}{3}$$

   Hint: Use the probabilistic method, along with Chernoff bounds, as in the proof that $R^{priv}_{\epsilon+\delta}(f) \leq R_\epsilon(f) + O(log(n) + log(\frac{1}{\delta}))$

3. Let $DISJ : \{0, 1\}^n \times \{0, 1\}^n \to \{0, 1\}$ be defined by

   $$DISJ(x, y) = \begin{cases} 1 \text{ if } x \cap y = \emptyset \\ 0 \text{ otherwise} \end{cases}$$

   In the above we view the inputs as subsets of $\{1, \ldots, n\}$. Show that $D(DISJ) = n + 1$.

4. For any graph G with n vertices, consider the following communication problem: Player 1 receives a clique C in G, and Player 2 receives an independent set I. They have to communicate in order to determine $|C \cap I|$ (note that this number is either 0 or 1). Prove an $O(log^2 n)$ upperbound on the communication complexity.

5. The discrete log problem is as follows: given a prime P, a generator g for the multiplicative group $\mathbb{Z}_p^*$, and a point y chosen at random in $\mathbb{Z}_p^*$, find x such that $g^x = y$. Establish the following claim: Suppose some deterministic poly-time algorithm correctly solves the discrete log problem for a $1/poly(n)$ fraction of $y \in \mathbb{Z}_p^*$ (here n is the length of p, i.e. the size of the input); then there is a randomized poly-time algorithm that solves the discrete log problem at all points with high probability.