CS6810 - Theory of Computing Due date: February 3rd, 2009

Homework 1

Instructor: Rafael Pass *TA: Muthu Venkitasubramaniam*

You may collaborate with other students on the homework but you must submit your own individually written solution and you must identify your collaborators. If you make use of any other external source, you must acknowledge it. You are not allowed to submit a problem solution which you cannot explain orally to the course staff.

Problem 1 *Expectation and Variance*

Let X and Y be two independent random variables. Prove the following facts.

(a) E[XY] = E[X]E[Y]

(b) Var[X+Y] = Var[X] + Var[Y].

Give examples when X and Y are not independent and equalities (a) and (b) do not hold.

Problem 2 *Pairwise independence*

1. Let $r_1, r_2, \ldots, r_k$ be n-bit strings picked uniformly at random. For any subset S of $\{1, 2, \ldots, k\}$, define a random variable $z_S = \oplus_{i \in S} r_i$. Prove that the set of random variables $\{z_S | S \subset \{1, 2, \ldots, k\}\}$ are pairwise independent.

2. Let $X_1, X_2, \ldots, X_n$ be random variables that are pairwise independent. Further, for all i, let $E[X_i] = \mu$ and $Var[X_i] = \sigma^2$

   (a) Show that,
   $$Pr\left[\left|\frac{\sum X_i}{n} - \mu\right| \geq \epsilon\right] \leq \frac{\sigma^2}{n\epsilon^2}$$
   Note that this is a Chernoff like bound when the random variables are only pairwise independent. (Hint: Use Chebyshev's inequality)

   (b) Suppose, further that the random variables assume the values only 1 and -1. Show that the inequality can be simplified to,
   $$Pr\left[\left|\frac{\sum X_i}{n} - \mu\right| \geq \epsilon\right] \leq \frac{1 - \mu^2}{n\epsilon^2}$$

Problem 3 *Biased Samples*

Let D be a distribution such that $\Pr[D = b] \geq \frac{1}{2} + \epsilon$ for some constant $\epsilon > 0$.

1. Show that using k independent samples from D, b can be computed correctly with high probability.

2. Assuming only k pairwise independent samples from D, calculate the probability b can be computed correctly?

Problem 4 *Taking Complements*

If $\mathsf{NP} \subseteq \mathsf{coNP}$, then show that $\mathsf{NP} = \mathsf{coNP}$

Problem 5 *Diagonalization*

Prove that $\mathsf{NTime}(n^5) \not\subseteq \overline{\mathsf{NTime}(n^2)}$

Problem 6 *NP-completeness*

1. Show that SAT[1] is NP-complete, even if each variable is restricted to occur exactly 3 times. What if it is restricted to occur only 2 times?
2. Consider a system of quadratic equations $\mod 2$ in n variables, i.e. all variables are boolean and every equation has degree at most 2 (eg. $x_1x_2 + x_3 = 1$). Prove that solving such a system is NP-complete. (Hint: Try starting with a 3-SAT formula).

[1] By SAT we mean a general formula in CNF.