Random discrete structures (MPI, 2014) **Lecturers:** Kunal Dutta and Arijit Ghosh
Topic: Tutorial 2 **Date:** 27/05/2014
Scribe: Kunal Dutta and Arijit Ghosh **Deadline:** 17/06/2014

By *random variables* or *discrete random variables* we mean random variables taking either finitely many values or countably infinite values.

1. Given a positive integer k, describe a non-negative random variable X such that
$$\mathbf{Pr}[X \geq k\mathbb{E}[X]] = \frac{1}{k}.$$

2. Let X be a non-negative integer-valued random variable such that $X \leq m$, and $\mathbb{E}[X] \geq 2m^{1-t\delta/2}$. Prove that
$$\mathbf{Pr}\Big[X \geq m^{1-t\delta/2}\Big] \geq m^{-t\delta/2}.$$

3. Let the random variable X be given by $X = \sum_{i=1}^{n} X_i$. Show that if $\mathbb{E}[X_i X_j] = \mathbb{E}[X_i]\mathbb{E}[X_j]$ for every pair of i and j with $1 \leq i < j \leq n$, then $Var[X] = \sum_{i=1}^{n} Var[X_i]$.

4. Give an example of a random variable with finite expectation, and unbounded variance.

5. (Probability amplification) Let a and b be chosen independently and randomly from $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, where n is a prime. Let $f : \mathbb{Z}_n \to \{0, 1\}$ be an unknown but fixed function, such that $f(x) = 1$ for a random subset $W \subset \mathbb{Z}_n$, which is called the *witness set*.
   (i) Compute the probability that none of a, b belong to the witness set. How many random bits did you need to generate a and b? If you select t random numbers $a_1, \ldots, a_t$, such that the probability that none of the selected numbers lies in the witness set is at most $1/t$, how many random bits do you need (here $0 \leq t < n$)?
   (ii) A set of random variables $X_1, \ldots, X_k$ is said to be *pairwise independent* if for all $i \neq j$, for all $x, y \in \Re$, we have $Pr[X_i = x | X_j = y] = Pr[X_i = x]$.
   Suppose we generate t pseudo-random numbers from $\mathbb{Z}_n$ by choosing $r_i = a.i + b \mod n$, for $1 \leq i \leq t$. Let $|W| = n/2$. Show that (a) the r_i's are pairwise independent. (b) The probability that none of the r_i's belong to the witness set is at most $1/t$. How many random bits were needed using this method?

6. (Chernoff Bounds: Upper Tail) Let X be the sum of n independent indicator random variables, each equal to 1 with probability p, and zero otherwise. Let μ denote $\mathbb{E}[X]$.
   (a) Apply the substitution $Y = e^{tX}$. Given $\delta > 0$, express the event $X > (1 + \delta)\mu$ in terms of Y.
   (b) Obtain an upper bound on the expression obtained in (a), by applying Markov's inequality to Y.
   (c) Obtain an upper bound on the moment generating function of X, i.e. $\mathbb{E}[Y]$, in terms of n, t and p.
   (d) Substitute the bound obtained in (c), to the expression obtained in (b).
   (e) Differentiate the expression obtained in (e) w.r.t. t and optimize to get the tightest possible upper bound.

7. (Chernoff Bounds: Lower Tail) Redo the previous exercise, but with the event $X < (1 - \delta)\mu$, to get an upper bound on its probability of occurence.

8. Let $\mathcal{G}_p(n)$ be the random graph model having vertices $V = 1, 2, \ldots, n$, and each pair of vertices joined by an edge with probability $p = p(n)$ independently of the others.

(a) The degree of a vertex $v \in V$ is the number of edges incident on v. Compute the expected degree of a vertex in $\mathcal{G}_p(n)$ in terms of n, p.

(b) Let $p = n^{-\epsilon}$, where $\epsilon > 0$. Find the maximum degree of the random graph $\mathcal{G}_p(n)$, with probability tending to 1 as $n \to \infty$.

9. Suppose we have n jobs to distribute among m processors. [Assume m divides n]. A job requires one unit of time with probability p, and $k > 1$ units of time with probability $1 - p$. Use Chernoff bounds, to derive upper and lower bounds on the time required (with high probability) for all jobs to be completed, if we randomly assign n/m jobs to each processor. (Notice the indicator variables are not $0 - 1$ variables here!)