6.842 Randomness and Computation February 12, 2014

Homework 2

Lecturer: Ronitt Rubinfeld *Due Date: February 19, 2014*

Homework guidelines: You may work with other students, as long as (1) they have not yet solved the problem, (2) you write down the names of all other students with which you discussed the problem, and (3) you write up the solution on your own. No points will be deducted, no matter how many people you talk to, as long as you are honest. If you already knew the answer to one of the problems (call these "famous" problems), then let me know that in your solution writeup – it will not affect your score, but will help me in the future. It's ok to look up famous sums and inequalities that help you to solve the problem, but don't look up an entire solution.

The following problems are to be turned in. You should upload your solution to Stellar as a pdf file.

1. Let k, m satisfy $e(m(m-1)+1)k(1-1/k)^m \leq 1$. Let $S \subset \mathcal{Z}$ with $|S| = m$ and $T \subset \mathcal{Z}$ with $|T|$ finite. Show that there exists a k-coloring $\chi : \mathcal{Z} \to [k]$ such that every translate $S+t$ is k-colored. That is, for all $t \in T$ and $1 \leq i \leq k$, there exists $s \in S$ with $\chi(s+t) = i$.

2. **(Moser-Tardos algorithm)** Show that in the Moser-Tardos algorithm, there is a constant c such that the probability that there exists a set that gets resampled more than $c \log m$ times is bounded by $1/10$.

3. **(Directed cycles)** Let $D = (V, E)$ be a simple directed graph (that is, a directed graph with no self-loops and with at most one edge between ever pair of vertices). Assume that D has minimum outdegree δ and maximum indegree Δ. Show that if $e(\Delta\delta+1)(1-\frac{1}{k})^\delta < 1$, then D contains a directed simple cycle whose length is a multiple of k. (A cycle is *simple* if no vertex appears more than once in it.)

4. **(Pairwise independence)** A *pairwise independent* space on n variables is a subset $S \subseteq \{0,1\}^n$ such that for every $i \neq j \in \{1, \ldots, n\}$, if x is uniformly-random element of S then (x_i, x_j) is a pair of independent bits each drawn uniformly from $\{0,1\}$. The size of the pairwise independent space is $|S|$.

   (a) In class, we stated without proof a construction which generates $n = 2^l - 1$ pairwise independent bits from $l = \log(n+1)$ truly random bits (In other words, this is a pairwise independent space of size $2^l = n+1$). Prove that the bits are indeed pairwise independent.

   (b) (extra credit) Show that this construction is optimal in the sense that every pairwise independent space on n variables should have size at least $n+1$.