CS388C: Combinatorics and Graph Theory — Problem Set No. 4

David Zuckerman — due: Oct. 23, 2007

1. Complete the midterm, including the extra credit problem. Your score for any problem will be at least that received on the test; therefore, for example, don't redo problems for which you received full credit. Please remember to hand in your test along with your homework.

2. Suppose you are given a biased coin for which the probability p of heads is unknown. Show how to use this coin to generate a perfectly unbiased random bit. Your algorithm should use an expected number of coin flips which is linear in $\max(1/p, 1/(1-p))$.

   Hint: consider two consecutive flips.

3. $F : [N] \times [D] \to [M]$ is a (K, ϵ)-*extractor* if for every subset $S \subseteq [N]$ of size K, the distribution $F(U_S, U_{[D]})$ is within ϵ of uniform, where U_X denotes the uniform distribution on the set X. A probability distribution P on a set A is within ϵ of uniform if for all $T \subseteq A$, $|P(T) - |T|/|A|| \leq \epsilon$. Show that that there exists a (K, ϵ)-extractor $F : [N = 2^n] \times [D] \to [M]$ with $M = Kn$ and $D = O(n/\epsilon^2)$.

   Hint: compare to the definition of disperser. Use the following Chernoff bound: If X_i, $i \in [\ell]$, are independent 0-1 random variables with $\Pr[X_i = 1] = p$, then

   $$\Pr[X - EX \geq a] \leq \exp(-2a^2/n).$$