CS395T: Pseudorandomness | Problem Set No. 1
David Zuckerman | due: October 6, 2009

1. Vadhan, Problem 3.3.

2. The ith coordinate of a code is useless if all codewords have the same value in the ith coordinate. The input to this problem is the generator matrix of a linear binary code of length n with no useless coordinates.

   (a) Show that the expected weight of a random codeword is at least $n/2$.

   (b) Give a randomness-efficient version of the algorithm suggested by (a) which uses just $O(\log n + \log \epsilon^{-1})$ random bits and outputs a codeword with expected weight at least $(1 - \epsilon)n/2$.

3. For your choice of constant c, give an explicit construction of $f(n)$ graphs on n nodes such that at least one of the graphs does not contain a clique or an independent set of size $c \log n$. How small can you make $f(n)$? Note: $f(n) = n^{O(\log n)}$ is possible with what we did in class, and it is an open question to do better.

4. Construct a sample space for $X = (X_1, \ldots, X_n) \in \mathbb{F}_2^n$ such that for any full rank $n \times k$ matrix M over $\mathbb{F}_2$ with $k \leq n$, and any $b \in \mathbb{F}_2^k$,

   $$|\Pr[XM = b] - 2^{-k}| \leq \epsilon.$$

   Your sample space should have size polynomial in n and $1/\epsilon$.

5. Suppose the uniform distribution on the set $T \subseteq \mathbb{F}_2^n$ is ϵ-biased. Use Fourier analysis to show that $|T| \geq 1/\epsilon^2$.