CS395T: Pseudorandomness and Combinatorial Constructions — Problem Set No. 1

David Zuckerman — due: Feb. 13

1. (15 points) Give an efficient probabilistic algorithm to test whether $A \times B = C$, where A, B, and C are $n \times n$ matrices with integral entries. Your algorithm should perform $O(n^2)$ additions and multiplications, and should catch an error with probability at least $1/2$.

2. (10 points)
   a) Prove that the definition of BPP remains unchanged if the $2/3$ and $1/3$ are replaced by $1/2 + n^{-c}$ and $1/2 - n^{-c}$, where c is any positive constant.

   b) Prove that the definition of BPP remains unchanged if the $2/3$ and $1/3$ are replaced by $1 - 2^{-n^c}$ and 2^{-n^c}, where c is any positive constant.

3. (25 points) An (N, M, D, K, ϵ)-disperser is a bipartite graph with N nodes on the left side, each with degree D, and M nodes on the right side, such that every subset of K nodes on the left side is connected to more than $1 - \epsilon$ fraction of the nodes on the right.

   a) Show that $(2^s, 2^r, s+2, 2^r, 1/2)$-dispersers exist for all integers $s \geq r > 0$.

   b) Assume all dispersers proved to exist in (a) are also efficiently constructible (define what notion you need), and suppose there exists an RP algorithm that uses $r = r(n)$ random bits to recognize a language. Show how to amplify the success probability to $1 - 2^{-t}$ in polynomial time using only $r + t$ random bits. Compare this to the number of bits used for independent random trials.

   c) Now suppose we wish to amplify the success probability without using any additional random bits. Show that no disperser with left degree D can achieve success probability larger than $1 - 1/(2D)$.

4. (10 points) Find all integral solutions to: $x_1^6 + x_2^6 + x_3^6 + x_4^6 + x_5^6 = 7,777,777,776$.