Homework 4
Duke April 13 2009

§1 Suppose a is an unknown m bit vector. Let $r_1, r_2, \ldots, r_m$ be m randomly chosen bit vectors, each of length m, and all of m bit-wise inner products $a \odot r_i$ (where $\odot$ is addition mod 2) revealed to us for all $i = 1, 2, \ldots, m$. Describe a deterministic algorithm to reconstruct a from this information, and show that the probability (over the choice of the r_i's) is at least 1/4 that it works.

Hint : you need to show that this can be done by the use of linear systems over $GF(2)^m$

§2 Suppose somebody holds an unknown n-bit vector a. Whenever you present a randomly chosen subset of indices $S \subseteq \{1, \ldots, n\}$, then with probability at least $1/2 + \epsilon$, she tells you the parity of the all the bits in a indexed by S. Describe a guessing strategy that allows you to guess n bit string a with probability at least $(\epsilon / n)^c$ for some constant $c > 0$.

§3 Suppose $g : \{0, 1\}^n \rightarrow \{0, 1\}^{n+1}$ is any pseudorandom generator. Then use g to describe a pseudorandom generator that stretches n bits to n^k for any constant $k > 1$.

§4 Show the correctness of the pseudorandom function generator in Section 10.4.1 of the Arora Chapter 10 on Cryptography.

Hint: Use a hybrid proof argument (similar to that used by Yao) which replaces the labels of the first k levels of the tree by completely random strings.