Algebraic Geometry for Theoretical Computer Science

Assignment 1

Lecturer: Gil Cohen *Hand in date: November 6, 2014*

Instructions: Please write your solutions in LaTeX, Word or exquisite handwriting. Submission can be done individually or in pairs.

1. Let $S \subseteq \{0,1\}^n$ be an ε-biased set. Show how to obtain a binary linear code from S. What are the parameters of your code in terms of $n, |S|$ and ε ?

2. Give an efficient construction of an ε-biased set $S \subseteq \{0,1\}^n$ with size $O((n/\varepsilon^3) \cdot \log^c(n/\varepsilon))$, where c is some fixed constant. *Guidance: in the powering construction, instead of sampling y in $\langle x^i, y\rangle$ uniformly at random, try to sample it from someplace else (hint: look right under you nose!).*