CS395T: Polynomials and Computation
David Zuckerman

Problem Set No. 2
due: May 5, 2004

1. Let $RM(r,m)$ denote the binary Reed-Muller code of length $2^m$ where codewords are evaluations of $m$-variate polynomials of degree at most $r$. Show that the dual of $RM(r,m)$ is $RM(m-r-1,m)$.

2. Define the language

$$\text{NONSQUARES} = \{(x,n) | x \text{ is not a square mod } n \text{ and } \gcd(x,n) = 1\}.$$

Give a 2-round interactive proof for NONSQUARES (i.e., the verifier sends bits to the prover, then the prover sends bits to the verifier, and then the verifier accepts or rejects).

3. You are given a black box which, on input $(a_1,\ldots,a_n)$, outputs $p(a_1,\ldots,a_n)$, where $p$ is an unknown multivariate polynomial with at most $t$ terms and integral coefficients. Show how to determine whether $p$ is the zero polynomial by making at most $t$ probes to the black box, and doing $\text{poly}(n,t)$ arithmetic operations. (Hint: the probes should involve several primes raised to consecutive powers.)

4. Let $\mathbb{F}$ denote a finite field and $f : \mathbb{F}^m \to \mathbb{F}$ a function. Show that if the restriction of $f$ to any line in $\mathbb{F}^m$ is a univariate polynomial of degree at most $d$, then $f$ is a multivariate polynomial of total degree at most $d$. You will need to assume a $\text{poly}(d)$ lower bound on the field size; please state what polynomial you need.

5. Let $\mathbb{F}$ be a finite field, $f : \mathbb{F}^2 \to \mathbb{F}$ a function. Suppose that for each $a \in \mathbb{F}$ there are univariate degree $d$ polynomials $C_a, R_a$ such that the following holds. For at least $1 - 1/(200d)$ fraction of $(a,b) \in \mathbb{F}$,

$$f(a,b) = R_a(b) = C_b(a).$$

Show that $f$ is .2-close to a bivariate polynomial with degree at most $d$ in each variable. You may assume a $\text{poly}(d)$ lower bound on the field size, but state what you need.