CS395T: Polynomials and Computation — Problem Set No. 1

David Zuckerman — due: March 12, 2004

The last problem is worth twice each of the others.

1. Let $q \geq d+2$ and $f : \mathbb{F}_q \to \mathbb{F}_q$ a function. For $S \subseteq \mathbb{F}_q$, let $\deg_S(f)$ denote the degree of the unique polynomial interpolating $f(s)$ for all $s \in S$. Now choose S to be a uniformly random $(d+2)$-subset of $\mathbb{F}_q$. Show that if $\Pr_S[\deg_S(f) \leq d] \geq 1-\epsilon$, then there is a polynomial of degree at most d which agrees with f on at least $(1-\epsilon)q$ points in $\mathbb{F}_q$.

2. Suppose p is a prime dividing $q-1$ and $a \in \mathbb{F}_q^*$. Show that $x^p - a$ is irreducible if and only if $a^{(q-1)/p} \neq 1$.

3. A mod_m gate takes several Boolean inputs, and outputs 1 if m divides the sum of its inputs and 0 otherwise. Show that for any odd prime p, there is no polynomial size, constant depth circuit family with $\wedge, \vee, \neg$, and mod_p gates which computes PARITY.

4. Suppose f is a polynomial over $\mathbb{F}_q$, and $f = f_1 f_2$ where each f_i is irreducible of degree d. Let $T(x) = x + x^q + x^{q^2} + \ldots x^{q^{d-1}}$, and let $T_i(x) = T(x^i)$ for $i = 0, 1, \ldots, 2d-1$. This problem is to show that some T_i is useful in Berlekamp's algorithm.

   a) Show that T maps $F_q[x]/(f_i)$ surjectively to $\mathbb{F}_q$, and that for all i, $T_i^q \equiv T_i \pmod{f}$.

   b) Show that there is a polynomial g such that:

$$\begin{aligned} T(g(x)) &\not\equiv 0 \pmod{f_1} \\ T(g(x)) &\equiv 0 \pmod{f_2}. \end{aligned}$$

   c) Suppose that for all i each $\gcd(T_i - a, f)$ is a trivial factor of f. Show that there are $c_0, \ldots, c_{2d-1} \in \mathbb{F}_q$ such that if $g(x) = \sum_{i=0}^{2d-1} a_i x^i$, then

$$T(g(x)) \equiv \sum_{i=0}^{2d-1} a_i c_i \pmod{f}.$$

   Observe that this contradicts (b) and hence one of the gcd's must be non-trivial.