Foundations and Frontiers of Probabilistic Proofs (Summer 2021)
Worksheet B.3: Low-Degree Testing
Date: 2021.07.29

Problem 1. (Self-correcting polynomials) Prove that low-degree multi-variate polynomials can be self corrected. Namely, prove that there exists a probabilistic oracle algorithm A with query complexity $O(d)$ such that: if $f\colon \mathbb{F}^n \to \mathbb{F}$ is δ-close to a polynomial $p(x_1, \ldots, x_n)$ of total degree d and no other polynomial is that close to f, then for every $a \in \mathbb{F}^n$ it holds that $\Pr_r[A^f(a; r) = p(a)] \geq 1 - O(\delta \cdot d)$.

Problem 2. (From total to individual) In lecture we saw a low-degree test for *total* degree. Here we analyze a test for *individual* degree. That is, our goal is to test if a given function $f\colon \mathbb{F}^m \to \mathbb{F}$ is a polynomial of individual degree at most d or far from any such polynomial with $\mathsf{poly}(dm)$ queries (when the proximity parameter ε is constant).

We assume that we have a low-degree test for functions $g\colon \mathbb{F}^m \to \mathbb{F}$ that accepts with probability 1 if g is a polynomial of total degree d, and accepts with probability at most $\frac{1}{10}$ if g is ϵ-far from all polynomials of total degree d. We also assume that the field size to be large enough so that $\frac{dm}{|\mathbb{F}|}$ is an arbitrarily small constant.

The test for individual degree works as follows.

1. Run the low-degree test for total degree dm on f. If the test fails, reject.
2. For $i \in [m]$:
   (a) Choose uniformly at random $a_1, \ldots, a_m \in \mathbb{F}$.
   (b) Let $g\colon \mathbb{F} \to \mathbb{F}$ be the function defined as $g(z) := f(a_1, \ldots, a_{i-1}, z, a_{i+1}, \ldots, a_m)$. Run the low-degree test for degree d (the same test for total degree with soundness error $\frac{1}{10}$) on the univariate polynomial $g(z)$.
3. If all tests pass, accept. Otherwise reject.

We analyze the properties of this test.

1. Prove that if f has individual degree at most d, then the test accepts with probability 1.
2. Prove that if f is ϵ-far from a polynomial of individual degree at most d, then the test accepts with probability at most $\frac{1}{2}$. *Hint: Consider the two cases where f is ϵ-far from any polynomial of total degree at most dm, and where f is close to one. In the latter, the polynomial h of total degree dm which is close to f contains a variable with individual degree at least $d+1$.*

Problem 3. (Local characterization via derivatives) For $i = 0, 1, \ldots, d+1$, define $c_{d,i} := (-1)^{i+1}\binom{d+1}{i}$. Let p be a prime, d a positive integer with $d + 2 \leq p$, and $f \in \mathbb{F}_p[X]$ a polynomial. (Note that, since any function over $\mathbb{F}_p$ can be represented as a degree-$(p-1)$ polynomial, the problem is trivial for $d + 1 \geq p$.)

1. Prove that f has degree at most d if and only if, for every $a \in \mathbb{F}_p$, $\sum_{i=0}^{d+1} c_{d,i} f(a+i) = 0$. (*Hint: use the "derivative" $f'(x) = f(x) - f(x-1)$ and induction.*)

2. Deduce that f has degree at most d if and only if, for every $a, b \in \mathbb{F}_p$, $\sum_{i=0}^{d+1} c_{d,i} f(a + i \cdot b) = 0$.