Foundations and Frontiers of Probabilistic Proofs (Summer 2021)
Worksheet A.0: Warm-Up
Date: 2021.07.26

The goal of this worksheet is to gain familiarity with basic facts about polynomials.

Problem 1. (Restriction to a line) A *line* in $\mathbb{F}^n$ is a function $g\colon \mathbb{F} \to \mathbb{F}^n$ of the form $g(z) = (a_1 z + b_1, \ldots, a_n z + b_n)$ for some choice of coefficients $a_1, b_1, \ldots, a_n, b_n \in \mathbb{F}$. The *restriction* of an n-variate polynomial $f(x_1, \ldots, x_n)$ over $\mathbb{F}$ to the line g is defined as the univariate polynomial $h(z) := f(g(z))$. Prove that for every line g, the degree of h is at most the total degree of f.

Next we prove the *Schwartz–Zippel Lemma*: for every non-zero n-variate polynomial f of total degree at most d over a field $\mathbb{F}$ and every finite set S in $\mathbb{F}$, $\Pr_{a_1,\ldots,a_n \leftarrow S}[f(a_1, \ldots, a_n) = 0] \leq \frac{d}{|S|}$. This fundamental lemma is used numerous times in this course.

Problem 2. (Zeroes of univariate polynomials) Let $\mathbb{F}$ be a field and f a *non-zero* univariate polynomial over $\mathbb{F}$ of degree at most d. Prove that f has at most d roots in $\mathbb{F}$ (you may use without proof the fact that $\mathbb{F}[X]$ is a Euclidean domain). (In particular, for every finite set $S \subseteq \mathbb{F}$, $\Pr_{a \leftarrow S}[f(a) = 0] \leq \frac{d}{|S|}$.) Give an example of a *finite* field $\mathbb{F}$ and polynomial $f \in \mathbb{F}[X]$ that has strictly fewer than $\deg(f)$ roots in $\mathbb{F}$.

Problem 3. (Zeroes of multivariate polynomials) Let $\mathbb{F}$ be a field and f a non-zero n-variate polynomial over $\mathbb{F}$ of degree at most d. Prove that, for every finite set S in $\mathbb{F}$, f has at most $d|S|^{n-1}$ roots in S^n. (*Hint: rely on the prior problem, and use induction.*) Conclude from this the Schwartz–Zippel Lemma.