Foundations and Frontiers of Probabilistic Proofs (July 2023)
Worksheet 1: Intro to IPs
Date: July 17, 2023

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

Problem 1. (Schwartz–Zippel Lemma) 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.

- 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 $\mathbb{F}$.
- 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.

Problem 2. (Importance of randomness) Prove that if a language $\mathcal{L}$ has an interactive proof with a deterministic verifier, then $\mathcal{L} \in \mathsf{NP}$.

Problem 3. (Invertible matrices) Let $\mathbb{F}$ be a finite field. Show that the language

$$\mathsf{INV}_{\mathbb{F}} := \{M \in \mathbb{F}^{n \times n} : \exists\, A \in \mathbb{F}^{n \times n} \text{ s.t. } MA = I\}$$

has an interactive proof with perfect completeness, soundness error $1/2$, and $O(n)$ total communication, where the verifier runs in time $O(n^2)$. (Assume that sampling field elements and performing basic field operations have unit cost.)