Foundations and Frontiers of Probabilistic Proofs (Summer 2021)
Worksheet A.1: Intro to IPs
Date: 2021.07.27

Problem 1. (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 2. (Sequential repetition) Suppose that $\mathcal{L}$ has an interactive proof (P, V) with perfect completeness and soundness error $1/2$. Let (P_t, V_t) be the *t-wise sequential repetition* of (P, V): the new prover P_t and the new verifier V_t respectively simulate the old prover P and old verifier V for t times one after the other, each time with fresh randomness; V_t accepts if and only if V accepts in all t repetitions. Prove that (P_t, V_t) is an interactive proof for $\mathcal{L}$ with perfect completeness and soundness error 2^{-t}.

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

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

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.)