CS6814
Homework 1: Interactive Proofs
Date: Oct 31, 2024

Problem 1. (Importance of randomness and error) Prove that if a language $\mathcal{L}$ has an interactive proof with a deterministic verifier, then $\mathcal{L} \in \mathsf{NP}$. Prove that if a language $\mathcal{L}$ has an interactive proof with zero soundness error, 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-fold 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. (Derandomised invertible matrices) Let $\mathbb{F}$ be a prime field such that $10n \leq |\mathbb{F}| \leq \mathsf{poly}(n)$. Give interactive proofs for the language

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

with perfect completeness, soundness error $1/2$, where the verifier runs in time $\tilde{O}(n^2)$, and with each of the following additional properties:

(a) $\tilde{O}(n)$ total communication, or

(b) where the verifier uses $O(\log n)$ random bits.

(Fun challenge problem: can we achieve both simultaneously? I don't know!)

Problem 4. (Multilinear arithmetisation) Prove that if there exists a polynomial-time computable arithmetisation A of 3-CNFs (i.e., a mapping of boolean formulas to arithmetic circuits) such that for all $x_1, \ldots, x_n \in \{0, 1\}$, $A(\phi)(x_1, \ldots, x_n) = 0$ if and only if $\phi(x_1, \ldots, x_n)$ is false, and $A(\phi)$ is multilinear for all ϕ, then $\mathsf{coNP} \subseteq \mathsf{BPP}$. You may assume that the underlying field $\mathbb{F}$ is sufficiently large.

Prove that if, in addition, for all $x_1, \ldots, x_n \in \{0, 1\}$, $A(\phi)(x_1, \ldots, x_n) = 1$ if and only if $\phi(x_1, \ldots, x_n)$ is true, and the characteristic of $\mathbb{F}$ is not 2, then there is a deterministic polynomial-time algorithm for $\#\mathsf{SAT}$.

Problem 5. (Error reduction)

(a) Let $S \subseteq \{0, 1\}^\ell$. Show that if $|S|/2^\ell \leq \frac{1}{3\ell}$, then for all $z_1, \ldots, z_\ell \in \{0, 1\}^\ell$, $|\bigcup_i (S \oplus z_i)| \leq 2^\ell/3$, where $S \oplus z_i = \{s \oplus z_i : s \in S\}$. On the other hand, show that if $|S|/2^\ell \geq 2/3$, then there exist $z_1, \ldots, z_\ell$ such that $\bigcup_i (S \oplus z_i) = \{0, 1\}^\ell$.

(b) Denote by MA_1 the class of languages that have MA protocols with perfect completeness. Show that $\mathsf{BPP} \subseteq \mathsf{MA}_1$.

(c) Show that $\mathsf{MA} = \mathsf{MA}_1$.

(d) Show that $\mathsf{MA} \subseteq \mathsf{AM}$. (Hint: make the soundness error *very* small.)