CS6814
Homework 2: PCPs
Date: Nov 25, 2024

Problem 1. (Soundness error lower bound) The *Exponential Time Hypothesis* (ETH) states that 3SAT cannot be decided by any deterministic algorithm running in time $2^{o(n)}$. Prove that, assuming ETH, any (boolean) PCP for 3SAT with randomness complexity r and query complexity q such that $\mathsf{r} + \mathsf{q} = o(n)$ has soundness error at least $2^{-\mathsf{q}}$.

Problem 2. Let $f \colon \mathbb{F}^n \to \mathbb{F}$, and let $\delta(f) = \min_{a \in \mathbb{F}^n} \Pr_{x \leftarrow \mathbb{F}^n}[f(x) \neq \langle a, x \rangle]$. Show that if $\delta(f) < \frac{1}{2}(1 - \frac{1}{|\mathbb{F}|})$ then there is a unique $a^* \in \mathbb{F}^n$ such that $\Pr_{x \leftarrow \mathbb{F}^n}[f(x) \neq \langle a^*, x \rangle] = \delta(f)$.

Problem 3. (LPCP for R1CS) The language R1CS($\mathbb{F}$) (rank-1 constraint satisfiability over the field $\mathbb{F}$) consists of all instances $\mathbb{x} = (A, B, C, v)$, where $A, B, C \in \mathbb{F}^{m \times n}$ and $v \in \mathbb{F}^{n'}$ for $n' \leq n$, such that there exists an assignment $z \in \mathbb{F}^n$ such that $Az \circ Bz = Cz$ and $z = (v, w)$ for some $w \in \mathbb{F}^{n-n'}$; here $\circ$ denotes the entry-wise product.

1. Prove that R1CS($\mathbb{F}$) has a linear PCP over $\mathbb{F}$ with the following parameters: soundness error $\epsilon = O(\frac{m}{|\mathbb{F}|})$, proof size $k = O(n + m)$, query complexity $\mathsf{q} = 4$, and randomness complexity $\mathsf{r} = O(\log |\mathbb{F}|)$. Recall that a linear PCP π of size k answers queries $y \in \mathbb{F}^k$ with the inner product $\langle y, \pi \rangle$.
2. Prove that, for every finite field $\mathbb{F}$, R1CS($\mathbb{F}$) is NP-complete.

Problem 4. (PCPs for NEXP) The NEXP-complete problem *oracle-3SAT* is defined as follows. Let B be an arithmetic formula on $r + 3s + 3$ variables over $\mathbb{F}$. We say that B is *implicitly satisfiable* if there exists an assignment $A \colon \{0,1\}^s \to \{0,1\}$ such that for all $z \in \{0,1\}^r$, $b_1, b_2, b_3 \in \{0,1\}^s$, $B(z, b_1, b_2, b_3, A(b_1), A(b_2), A(b_3)) = 1$. (Think of z as labelling a clause of a 3-SAT formula of size 2^r and b_1, b_2, b_3 as labelling the variables.) Let $\mathsf{Oracle\text{-}3SAT}_{\mathbb{F}}$ be the language consisting of all implicitly-satisfiable arithmetic formulae over $\mathbb{F}$.

Show that $\mathsf{Oracle\text{-}3SAT}_{\mathbb{F}} \in \mathsf{PCP}_{\mathbb{F}}[\mathsf{poly}, \mathsf{poly}]$, provided $\mathbb{F}$ is sufficiently large.