Foundations and Frontiers of Probabilistic Proofs (July 2023)
Worksheet 17: Proof Composition and PCP Theorem
Date: July 27, 2023

Problem 1. (PCPs of knowledge) A PCP system (P, V) for a relation $\mathcal{R}$ has knowledge error ϵ if there exists a polynomial-time algorithm E such that for every instance $\mathbb{x}$ and PCP string $\tilde{\pi}$ if $\Pr[V^{\tilde{\pi}}(\mathbb{x}) = 1] > \epsilon$ then $(\mathbb{x}, E(\mathbb{x}, \tilde{\pi})) \in \mathcal{R}$. Show how to construct a PCP system for boolean circuit satisfiability with knowledge error ϵ from these ingredients: (a) a PCPP system for boolean circuit satisfiability with soundness error ϵ and proximity parameter δ; (b) an error-correcting code with efficient-decoding radius $\delta' \geq \delta$.

Problem 2. (Robustification) Let $\mathcal{L}$ be a language with a PCP with soundness error ϵ, alphabet Σ, proof length l, query complexity q, and randomness complexity r. Using an efficiently-decodable error-correcting code $C\colon \Sigma \to \{0,1\}^{O(\log|\Sigma|)}$ with constant rate and relative distance δ, prove that $\mathcal{L}$ has a *robust* PCP with robustness parameter $O(\delta/q)$, soundness error ϵ, alphabet $\{0,1\}$, proof length $O(\mathsf{l} \cdot \log|\Sigma|)$, query complexity $O(\mathsf{q} \cdot \log|\Sigma|)$, and randomness complexity r.

Problem 3. (PCPPs for multi-input circuits) A PCPP system (P, V) for the satisfiability of a 2-input boolean circuit $C\colon \{0,1\}^{n_1} \times \{0,1\}^{n_2} \to \{0,1\}$ has proximity parameter δ and soundness error ϵ if the usual PCPP soundness is replaced by the following one: for every two inputs $(\mathbb{x}_1, \mathbb{x}_2)$ and PCPP string $\tilde{\pi}$, if for every two inputs $(\mathbb{y}_1, \mathbb{y}_2)$ such that $C(\mathbb{y}_1, \mathbb{y}_2) = 1$ there exists $i \in [2]$ such that $\mathbb{x}_i$ is δ-far from $\mathbb{y}_i$ then $\Pr[V^{\mathbb{x}_1, \mathbb{x}_2, \tilde{\pi}}(C) = 1] \leq \epsilon$. Use (standard) PCPPs for circuit satisfiability with soundness error $O(1)$ and proximity parameter $O(1)$ to construct PCPPs for 2-input circuit satisfiability with soundness error $O(1)$ and proximity parameter $O(1)$. You may assume that n_2 divides n_1. (*Hint: For a string $\mathbb{x}$, let $\mathbb{x}^t$ be the t-wise repetition of $\mathbb{x}$. Observe that if $\Delta(\mathbb{x}, \mathbb{y}) = m$ then $\Delta(\mathbb{x}^t, \mathbb{y}^t) = m$.*)