Foundations and Frontiers of Probabilistic Proofs (July 2023)
Worksheet 20: Limitations of PCPs and IOPs
Date: July 28, 2023

Problem 1. (PCP to extremely laconic MA) Consider a language $\mathcal{L} \in \mathsf{PCP}[\epsilon_{\mathsf{c}}, \epsilon_{\mathsf{s}}, \Sigma, \mathsf{l}, \mathsf{q}, \mathsf{r}]$. Let $\mathsf{PCP} = (P, V)$ be a PCP for the language $\mathcal{L}$. Recall the following PCP to laconic one-round MA transformation from lecture:

- $\mathcal{P}_{\mathsf{MA}}(\mathbb{x})$:
  1. Compute $\pi \leftarrow P(\mathbb{x})$.
  2. Sample random $\mathcal{Q} \leftarrow \binom{[\mathsf{l}]}{\mathsf{q}}$.
  3. Send $\Pi \coloneqq (\mathcal{Q}, \pi[\mathcal{Q}])$.
- $\mathcal{V}_{\mathsf{MA}}(\mathbb{x}, \Pi)$:
  1. Sample $\rho \leftarrow \{0,1\}^{\mathsf{r}}$.
  2. Parse Π as $(\mathcal{Q}, a \in \Sigma^{\mathsf{q}})$.
  3. Check that $V(\mathbb{x}; \rho) = 1$ by answering queries $i \in \mathcal{Q}$ with $a[i]$. Reject if V queries anything outside of $\mathcal{Q}$.

The above transformation gives us a MA protocol with completeness error $1 - (1 - \epsilon_{\mathsf{c}}) \cdot 2^{-\mathsf{q} \cdot \log \mathsf{l}}$, soundness error ϵ_{s}, and prover communication $\mathsf{q} \cdot (\log \mathsf{l} + \log |\Sigma|)$.

We are not happy about the prover communication and want to improve the above transformation. Consider the following transformation and argue why the resulting MA protocol has soundness error 1.

- $\mathcal{P}_{\mathsf{MA}}(\mathbb{x})$:
  1. Compute $\pi \leftarrow P(\mathbb{x})$.
  2. Sample random $\mathcal{Q} \leftarrow \binom{[\mathsf{l}]}{\mathsf{q}}$.
  3. Send $\Pi \coloneqq \pi[\mathcal{Q}]$.
- $\mathcal{V}_{\mathsf{MA}}(\mathbb{x}, \Pi)$:
  1. Sample $\rho \leftarrow \{0,1\}^{\mathsf{r}}$.
  2. Check that $V(\mathbb{x}; \rho) = 1$ by answering the i-th query made by V with $\Pi[i]$.

Problem 2. (PCP to laconic MA, a different approach) Consider a language $\mathcal{L} \in \mathsf{PCP}[\epsilon_{\mathsf{c}}, \epsilon_{\mathsf{s}}, \Sigma, \mathsf{l}, \mathsf{q}, \mathsf{r}]$. Design a one-round MA protocol for the language $\mathcal{L}$ with prover communication $\mathsf{r} + \mathsf{q} \cdot \log |\Sigma|$. What is the completeness error and soundness error for your MA protocol?