Foundations and Frontiers of Probabilistic Proofs (Summer 2021)
Worksheet A.6: Limitations of IPs
Date: 2021.08.03

Problem 1. (IPs with small-space verifier)

1. Prove that if a language $\mathcal{L}$ has a *public-coin* interactive proof where the communication and verifier space complexity are upper bounded by s, then $\mathcal{L}$ can be decided by an algorithm running in space $O(s^2)$.

2. As above, but without the public coin assumption.

(This simple observation has an important consequence: since it is believed that $\mathsf{DTIME}[T] \not\subseteq \mathsf{SPACE}[o(T)]$, we should not expect every language in $\mathsf{DTIME}[T]$ to have a non-trivial interactive proof. This is quite unlike the case for PCPs, where we have good constructions for every language in $\mathsf{NTIME}[T]$.)

Problem 2. (Laconic provers with perfect completeness) Suppose that a language $\mathcal{L}$ has a proof system with perfect completeness in which the prover-to-verifier communication is at most $b(\cdot)$ bits. Show that $\mathcal{L} \in \mathsf{coNTIME}(2^{b(n)} \cdot \mathsf{poly}(n))$.

You may use Zermelo's Theorem: "in every finite, deterministic, perfect-information game between players A and B where the players move alternately, if the game cannot end in a draw, either A or B has a winning strategy."

(*Hint: Use the IP* (P, V) *to define a two-player game:* A *corresponds to* P*, and the goal of* B *is to generate an interaction that makes* V *reject.*)