Foundations and Frontiers of Probabilistic Proofs (Summer 2021)
Worksheet A.5: Zero-Knowledge IPs
Date: 2021.08.02

Problem 1. (ZK requires interaction) Prove that if a language $\mathcal{L}$ has a non-interactive proof that is *zero-knowledge* (even if only against honest verifiers), then $\mathcal{L}$ is in BPP. (In a non-interactive proof, the prover and the verifier receive as input an instance $\mathbb{x}$, the prover sends a message a to the verifier, and then the verifier decides whether to accept or reject based on the instance $\mathbb{x}$, prover message a, and its own internal randomness r.)

Problem 2. (HVZK PCPs for NP) Prove that there exist honest-verifier zero-knowledge PCPs for all of NP by following the steps below.

1. The graph 3-coloring problem (3COL) is defined as follows: given a graph $G = ([n], E)$, decide if there exists a function $\psi\colon [n] \to [3]$ such that for every $(u, v) \in E$ it holds that $\psi(u) \neq \psi(v)$. Prove that 3COL is contained in NP. (You do not have to prove that 3COL is also NP-hard.)

2. The *view* of a PCP verifier is the random variable $(\mathbb{x}, r, a_1, \ldots, a_{\mathsf{q}})$ where $\mathbb{x}$ is its input instance, r is its internal randomness, and $(a_1, \ldots, a_{\mathsf{q}})$ are the answers to its queries to the PCP string π, which itself can be sampled probabilistically by the prover on input $\mathbb{x}$. We denote this view by $\mathrm{view}_V(V^{P(\mathbb{x})}(\mathbb{x}; r))$. A PCP system for a language $\mathcal{L}$ is (perfect) *honest-verifier zero-knowledge* if there exists a polynomial-time probabilistic algorithm S such that, for every $\mathbb{x} \in \mathcal{L}$, $S(\mathbb{x})$ outputs a view that is distributed identically to $\mathrm{view}_V(V^{P(\mathbb{x})}(\mathbb{x}; r))$.

   Design an HVZK PCP for 3COL, with perfect completeness and soundness error $1 - \frac{1}{\mathsf{poly}(n)}$.

   (Hint: how can you randomize the prover's 3-coloring $\psi\colon [n] \to [3]$?)

Discussion question: How would you define a notion of *malicious-verfier* zero-knowledge that is appropriate for superpolynomial-size PCPs? What about for polynomial-size PCPs?

Problem 3. (Auxiliary inputs and sequential repetition) An IP is *auxiliary-input* malicious-verifier zero-knowledge if for every polynomial-time probabilistic verifier $\tilde{V}$ there exists a probabilistic algorithm S that runs in expected polynomial time such that for every instance $\mathbb{x} \in \mathcal{L}$ **and auxiliary input** z, the random variables $S(\mathbb{x}, z)$ and $\mathrm{view}_{\tilde{V}}(\langle P, \tilde{V}(z)\rangle(\mathbb{x}))$ are identical.

Prove that auxiliary-input perfect zero knowledge is preserved under sequential repetition. (See Worksheet A.1 for a definition of sequential repetition of IPs.)

(Hint: Let $X_1, \ldots, X_k$ and $Y_1, \ldots, Y_k$ be $2k$ distributions. In order to show that $(X_1, \ldots, X_k) \equiv (Y_1, \ldots, Y_k)$ it suffices to show that for every $i \in \{0, \ldots, k\}$,

$$(X_1, \ldots, X_i, Y_{i+1}, \ldots, Y_k) \equiv (X_1, \ldots, X_{i+1}, Y_{i+2}, \ldots, Y_k) \ .$$

This proof technique is known as a hybrid argument.*)*

Problem 4. (HVZK and parallel repetition) Let (P_t, V_t) be the *t-wise parallel 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 in parallel, each time with fresh randomness; V_t accepts if and only if V

accepts in all t repetitions. In particular, each prover and verifier message in (P_t, V_t) is a t-tuple of messages corresponding to the t repetitions.

Prove that *honest-verifier* perfect zero knowledge is preserved under parallel repetition of interactive proofs. (An interactive proof for a language $\mathcal{L}$ is *honest-verifier* perfect zero-knowledge if there exists a polynomial-time probabilistic algorithm S such that, for every $\mathtt{x} \in \mathcal{L}$, $S(\mathtt{x})$ is identically distributed as the view of the honest verifier after interacting with the honest prover on common input $\mathtt{x}$.)