Foundations and Frontiers of Probabilistic Proofs (Summer 2021)
Worksheet A.9: Linear-Size IOPs for Machines
Date: 2021.08.06

Problem 1. (Permutation testing) We build the *permutation subprotocol* mentioned in lecture.

1. Prove that for every $(a_1, \dots, a_n), (b_1, \dots, b_n) \in \mathbb{F}^n$ there exists a permutation $\pi \colon [n] \to [n]$ such that $\forall\, i \in [n],\ a_i = b_{\pi(i)}$ if and only if
$$\prod_{i=1}^{n}(X - a_i) \equiv \prod_{i=1}^{n}(X - b_i) \ .$$

2. Let ω generate a multiplicative subgroup of $\mathbb{F}$ of size n, and fix $\beta \in \mathbb{F}$. Write two polynomial constraints of the form
$$h_k(X) = \frac{p_k(a(X), f(X), f(\omega^{-1}X))}{v_k(X)}$$
that are jointly satisfied if and only if $f(\omega^j) = \prod_{i=0}^{j}(\beta - a(\omega^i))$ for every $j \in \{0, \dots, n-1\}$.

3. Design an IOP for the language of pairs of polynomials (f, g) of degree d such that $f|_H$ is a permutation of $g|_H$, where $H = \langle \omega \rangle \subseteq \mathbb{F}$. Assume that both the prover and verifier have oracle access to f, g, which are guaranteed to be of degree at most d. You may assume an IOP for algebraic automata as specified in lecture.

Problem 2. (Fibonacci testing) The Fibonacci sequence is given by $a_1 = 1, a_2 = 1, a_n = a_{n-1} + a_{n-2}$ for $n \geq 3$. Let ω generate a subgroup of $\mathbb{F}$ of size n.

1. Write a system of constraints of the form
$$h_k(X) = \frac{p_k(A(X), A(\omega X), A(\omega^2 X))}{v_k(X)}$$
that checks that $A(\omega^{j-1}) = a_j$ for every $j \in [n]$.

2. Write a system of constraints of the form
$$h_k(X) = \frac{p_k(A_1(X), A_1(\omega X), A_2(X), A_2(\omega X))}{v_k(X)}$$
that checks that $A_1(\omega^{j-1}) = a_j$ for every $j \in [n]$.

Problem 3. (Zero-on-domain testing) Let $H, L \subseteq \mathbb{F}$ be domains with $L \cap H = \emptyset$. Prove that if $f \in \mathbb{F}[X]$ has degree d and $f(a) \neq 0$ for some $a \in H$, then the rational function
$$g(X) \coloneqq \frac{f(X)}{\prod_{a \in H}(X - a)}$$
evaluated on L is $(1 - \frac{d}{|L|})$-far from any Reed–Solomon codeword on L of degree $d - |H|$.