Foundations and Frontiers of Probabilistic Proofs (Summer 2021)
Worksheet B.8: PCPs with Sublinear Verification
Date: 2021.08.05

Problem 1. (Polynomial consistency test) Let $f_1, f_2, g \colon \mathbb{F}^n \to \mathbb{F}$ be polynomials of individual degree at most d. Let $S_1, S_2 \subseteq \mathbb{F}^n$ and $H \subseteq \mathbb{F}$ be such that $S_1 \cup S_2 = H^n$. Design a PCP system for proving that for every $i \in \{1, 2\}$ and $a \in S_i$ it holds that $g(a) = f_i(a)$, when the PCP verifier is given oracle access to f_1, f_2, g. (*Hint: reduce the problem to a zero-on-subcube problem. The reduction need not be time-efficient, i.e., it may perform* $\mathsf{poly}(|H|^n, d)$ *field oprations.*)

Below we develop an alternative approach to a zero-on-subcube test to the one described in class. Rather than using sumcheck, we build on properties of multi-variate polynomials.

Problem 2. (Characterization of vanishing on subcube) Let $\mathbb{F}$ be a finite field, H a subset of $\mathbb{F}$, and $V_H(X) := \prod_{a \in H}(X - a)$ be the vanishing polynomial of H. Prove that a polynomial $f \in \mathbb{F}[X_1, \ldots, X_n]$ vanishes everywhere on H^n if and only if there exist polynomials $Q_1, \ldots, Q_n \in \mathbb{F}[X_1, \ldots, X_n]$ of individual degree less than that of f satisfying

$$f(X_1, \ldots, X_n) \equiv \sum_{i \in [n]} Q_i(X_1, \ldots, X_n) V_H(X_i) \ .$$

(*Hint: Any polynomial* $f(X)$ *can be written as* $Q(X) \cdot V_H(X) + R(X)$, *where* R *has degree less than* $|H|$. *Apply this fact to the monomials of* f.)

Problem 3. (Alternative zero-on-subcube test) Use the fact in the prior problem to design a zero-on-subcube test proving that f vanishes everywhere on H^n with constant soundness and $\mathsf{poly}(|H|, n)$ verifier runtime.