Foundations and Frontiers of Probabilistic Proofs (Summer 2021)
Worksheet A.8: Linear-Size IOPs for Circuits
Date: 2021.08.05

Problem. (Univariate sumcheck for additive subgroups) We saw how to design a sumcheck protocol for univariate polynomials $g \in \mathbb{F}[X]$ when summing over *multiplicative* subgroups H of $\mathbb{F}$ with $\deg(g) < |H|$, using the identity

$$\sum_{a \in H} g(a) = |H| g(0) \ .$$

In this problem we will design a univariate sumcheck protocol over *additive* subgroups H.

Problem 1. Using the fact that for every univariate polynomial $g \in \mathbb{F}[X]$ with $\deg(g) < |H|$, letting β be the coefficient of $X^{|H|-1}$ in g, it holds that

$$\sum_{a \in H} g(a) = \beta \cdot \sum_{a \in H} a^{|H|-1} \ ,$$

design an efficient univariate sumcheck protocol for additive subgroups. Let $v_H(X)$ be the vanishing polynomial for H. You may assume that $\sum_{a \in H} a^{|H|-1}$, and $v_H(\gamma)$ for any $\gamma \in \mathbb{F}$, can be computed in time $\mathsf{polylog}(|H|)$.

Problem 2. In this question we will prove the identity used above. Let $\mathbb{F}$ be a field of characteristic p (the prime field $\mathbb{F}_p$ is a subfield of $\mathbb{F}$). The *derivative* of a function $f \colon \mathbb{F} \to \mathbb{F}$ in direction $a \in \mathbb{F}$ is $\Delta_a(f)(x) \coloneqq \sum_{b \in \mathbb{F}_p} f(x + ba)$. For $a_1, \ldots, a_k \in \mathbb{F}$ we inductively define $\Delta_{a_1,\ldots,a_k}(f) \coloneqq \Delta_{a_1}(\Delta_{a_2,\ldots,a_k}(f))$.

1. Let $a_1, \ldots, a_k \in \mathbb{F}$ be a basis for H over $\mathbb{F}_p$. Prove that $\Delta_{a_1,\ldots,a_k}(f)(a_0) = \sum_{a \in H} f(a_0 + a)$.
2. Write the p-ary expansion of an integer $c \in \mathbb{N}$ as $\sum_{i \geq 0} c_i p^i$ for $0 \leq c_i < p$. Define the sum of the "p-ary digits" of c as $\mathsf{ds}_p(c) \coloneqq \sum_{i \geq 0} c_i$. For a polynomial $g(X) = \sum_{j \geq 0} \alpha_j X^j$, define $\mathsf{ds}_p(g) \coloneqq \max(\{\mathsf{ds}_p(j) : \alpha_j \neq 0\} \cup \{-1\})$. Prove that for every $a \in \mathbb{F}$ it holds that

   $$\mathsf{ds}_p(\Delta_a(g)) \leq \max\{\mathsf{ds}_p(g) - (p-1), -1\} \ .$$

   You may use the following facts:

   (a) $b^p = b$ for all $b \in \mathbb{F}_p$.
   (b) For $c, d \in \mathbb{N}$, let $c = \sum_i c_i p^i$ and $d = \sum_i d_i p^i$ be their p-ary expansions. If there exists $i \geq 0$ such that $d_i > c_i$ then $\binom{c}{d} \equiv 0 \pmod{p}$.

   Hint: consider a single monomial X^c, and apply the binomial theorem.

3. Prove that for every univariate polynomial $g \in \mathbb{F}[X]$ with $\deg(g) < |H|$, letting β be the coefficient of $X^{|H|-1}$ in g, it holds that

   $$\sum_{a \in H} g(a) = \beta \cdot \sum_{a \in H} a^{|H|-1} \ .$$

Problem 3. (Bonus) Show that $\sum_{a \in H} a^{|H|-1} = \prod_{a \in H \setminus \{0\}} a$. (*Hint: use Newton's identities.*[1]) The right-hand side is equal to the coefficient of the linear term of $v_H(X)$, which can be computed in time $O(\log^2 |H|)$.

[1] `https://en.wikipedia.org/wiki/Newton's_identities`