Foundations and Frontiers of Probabilistic Proofs (Summer 2021)
Worksheet A.2: Sumcheck Protocol
Date: 2021.07.28

Problem 1. **(Sumcheck with tensor weights)** We consider an extension of the sumcheck problem where the summand is multiplied by weights that have a product structure. Specifically, given $n \cdot |H|$ field elements $\{\delta_{i,\alpha} \in \mathbb{F}\}_{i \in [n], \alpha \in H}$, we consider statements of the following form:

$$\sum_{\alpha_1,\ldots,\alpha_n \in H} \delta_{1,\alpha_1} \cdots \delta_{n,\alpha_n} \cdot p(\alpha_1, \ldots, \alpha_n) = \gamma \ .$$

Show that the sumcheck protocol can be extended to support the above statement, with the same completeness and soundness guarantees.

Problem 2. **(Efficient multilinear extension)** The multilinear extension of a boolean function $f \colon \{0,1\}^n \to \{0,1\}$ over a field $\mathbb{F}$ is the unique multilinear polynomial $\mathrm{MLE}_{\mathbb{F}}(f) \in \mathbb{F}[X_1, \ldots, X_n]$ that agrees with f on $\{0,1\}^n$:

$$\mathrm{MLE}_{\mathbb{F}}(f)(X_1, \ldots, X_n) := \sum_{b_1,\ldots,b_n \in \{0,1\}} f(b_1, \ldots, b_n) \prod_{i \in [n] \ b_i = 1} X_i \prod_{i \in [n] \ b_i = 0} (1 - X_i) \ .$$

Prove that evaluating a multilinear extension at a single point is in linear time. Namely, give an algorithm that given a boolean function f (represented as a string of 2^n bits), finite field $\mathbb{F}$, and evaluation point $(\alpha_1, \ldots, \alpha_n) \in \mathbb{F}^n$, computes the evaluation of $\mathrm{MLE}_{\mathbb{F}}(f)$ at $(\alpha_1, \ldots, \alpha_n)$ in $O(2^n)$ field operations. *Hint: The multilinear extension can be evaluated by summing term by term in $O(n \cdot 2^n)$ field operations while maintaining a state of $O(1)$ field elements in memory. How can you use more memory to speed up the computation?*

Problem 3. **(Efficient sumcheck)** We analyze the running time of the honest prover in the sumcheck protocol, when proving statements of the form $\sum_{\alpha_1,\ldots,\alpha_n \in H} p(\alpha_1, \ldots, \alpha_n) = \gamma$.

1. Prove that the honest prover can be realized in $O(d \cdot |H|^n \cdot |p|)$ operations, where d is the individual degree of p and $|p|$ is the number of operations to evaluate p at any point in $\mathbb{F}^n$.
2. Consider the special case where $H = \{0,1\}$ and p is multilinear. Prove that, if p is specified via its evaluations on $\{0,1\}^n$, the honest prover can be realized in $O(2^n)$ field operations.