Foundations and Frontiers of Probabilistic Proofs (Summer 2021)
Worksheet A.4: Doubly-Efficient IPs
Date: 2021.07.30

Problem 1. (Layered circuits) Prove that any arithmetic circuit of depth d and size S can be transformed into a *layered* arithmetic circuit of depth d and size $O(S^2)$.

Problem 2. (GKR for any set of gates) The GKR protocol that we saw in class applies to layered arithmetic circuits, which by default involve two gates: addition gates and multiplication gates. Now suppose that we instead consider layered circuits where gates are selected from a gate set of bivariate polynomials $\{g_k(X,Y)\}_k$. (The special case of addition and multiplication thus corresponds to the gate set $\{g_1(X,Y) = X + Y, g_2(X,Y) = X \cdot Y\}$.) How would you modify the GKR protocol to support the evaluation of such circuits?

Problem 3. (GKR for formulas) A *formula* is a circuit whose underlying directed acyclic graph is a tree (except for the input layer). Let φ be a layered arithmetic formula of depth d with binary $+$ and $\times$ gates, where even layers consist of $+$ gates and odd layers consist of $\times$ gates. In particular, layer $i \in [d]$ contains 2^{i-1} gates, which we label using the set $\{0,1\}^{i-1}$. (Inputs to the circuit are provided in layer $d+1$.) For even $i \in [d-1]$, let $\mathrm{add}_i \colon \{0,1\}^{i-1} \times \{0,1\}^i \times \{0,1\}^i \to \{0,1\}$ denote the wiring predicate corresponding to φ's gates in layer i; i.e., $\mathrm{add}_i(a,b,c) = 1$ if gate a (in layer i) has the outputs of b, c (in layer $i+1$) as its left and right inputs, respectively. Let $\widehat{\mathrm{add}}_i$ denote the multilinear extension of add_i. Define similarly mul_i and $\widehat{\mathrm{mul}}_i$ for odd $i \in [d-1]$. Show that there is a way to label the gates in φ such that for every $i \in [d-1]$, $\widehat{\mathrm{add}}_i$ or $\widehat{\mathrm{mul}}_i$ can be evaluated at any point in $\mathbb{F}^3$ in $O(i)$ field operations.

Note: it is not possible in general to do this for $\widehat{\mathrm{add}}_d$ (or $\widehat{\mathrm{mul}}_d$) since the wiring between the input layer and the bottom layer of gates can be arbitrary.