Homework #3

Simon Judd

September 26, 2024

1 Layered Circuits

2 GKR for any set of gates

We define the circuit structure as $s-space$ uniform for a circuit family $\{C_n\}_{n \in N}$ with a width W and depth D that is $O(log(W \cdot D))$ uniform.

We define a GKR circuit as $C : F^{n_{in}} -> F^{n_{out}}$, and define $\hat{C}$ as a low degree extension of C. In vanilla GKR our goal is to evaluate C using a public coin IP. We do this by first defining a subset $H \subseteq F$, and then rewriting our computation as summations.

Set $wp_1, .., wp_d$ as the wiring predicates.

The input layer $V_D : H^{m_{in}} -> F$ is defined as $V_d(a) = Z_{in}(a)$:

The intermediate layers as:

$$V_i := \sum_{b,c \in H^m} wp_{i+1}(a, b, c) \cdot g(v_{i+1}(b), v_{i+1}(c))$$

And the output layers as:

$$V_o := \sum_{b,c \in H^m} wp_i(a, b, c) \cdot g(v_i(b), v(c_i))$$

We then low-degree extend each layer.

And then finally check the computation via iterated sumchecks.

The bivariant polynomial $g_k(X, Y)$ has functions of the form $g_k : H^n -> F$, and $p \in F[X, Y]$ extends $g_k : H^n -> F$ if $p|_{H^n} \equiv F$. And we bound it's degree by $deg(g_k) \leq d$.

We need to create a low-degree extension of g_k, we do this by taking a linear combination of the given function and extending it to each layer. We define the low-degree extension of g_k as:

$$\hat{g}_k(X, Y) = \sum_{\alpha \in H^2} g_k(\alpha_1, .., \alpha_n) \cdot L_{H^n(\alpha_1,..,\alpha_n)}(X, Y)$$

Where H^2 is the subset of F^2 containing each component of H. And where $L_\alpha(X, Y)$ is the langrange basis polynomial.

Next we need to replace wp and g_k with there low degree extensions.
Replace $L_{H^m,a}(X)$ with $I_{H^m}(X,a)$ where:

$$I_{H^m}(X,Y) = \prod_{i\in[m]} \sum_{\alpha\in H} L_{H^m,\alpha}(X_i) \cdot L_{H^m,\alpha}(Y_i)$$

Which results in the following low-degree polynomial V_i for each layer:

$$V_i = \sum_{\alpha\in H} (\sum_{b,c\in H} w\hat{p}_i(a,b,c) \cdot g_k(\hat{v}_i(b), \hat{v}_1(c)) \cdot I_{H^m}(X,Y)$$

Now we have obtained our low-degree extension the next step is to perform a multivariate sumcheck on the resulting polynomial.

$$\sum_{\alpha\in H,b,c\in H} w\hat{p}_i(a,b,c) \cdot g_k(\hat{v}_i(b), \hat{v_i(c)}) \cdot I_{H^m}(X,Y) = \gamma$$

To avoid claim blow-up, we need to batch the claims via random linear combination.

$$\sum_{\alpha\in H,b,c\in H} w\hat{p}_i(a,b,c) \cdot g_k(\hat{v}_i(b), \hat{v_i(c)}) \cdot [\rho \cdot I_{H^m}(X,Y) + \beta \cdot I_{H^m}(X,Y)]$$

Soundness
Completeness

3 Problem: 3

4 Problem: 4

5 Problem: 5

6 Problem: 6

7 Problem: 7