The cost of Logup*

1 Introduction

The main bottleneck for the prover in logup* [1] is the GKR used to prove:

$$\sum_{0 \le i < n} \frac{eq_r[i]}{c - I[i]} = \sum_{0 \le j < m} \frac{I_* eq_r[j]}{c - j} \tag{1}$$

Trick 1 (trivial): When used in the context of a zkVM, the memory is often not a perfect power of 2: the final values (up to almost 50%) of $I_* eq_r$ are zeros. In addition to speeding up the GKR, note that this can also help reducing commitment costs.

2 Conventions

- We represent in memory a multilinear polynomial M with "big endian" ordering: $[M(0, \dots, 0)$, $M(0, \dots, 0, 1)$, $M(0, \dots 0, 1, 0)$, $M(0, \dots 0, 1, 1)$, $\dots, M(1, \dots, 1)]$. (This consideration plays a crucial role when it comes to SIMD implementation).
- We denote by D the degree of our extension field. Typically $D = 5$.
- We denote by (ee) (resp. (bb), resp. (be)) the cost of a multiplication between two extension field elements (resp. two base field elements, resp. one extension and one base field element). Typically (ee) $= D^2 \cdot$(bb) $= D \cdot$(be).
- We neglect the cost of all additions.
- GKR is performed from "bottom" (little number of variables) to "top" (big number of variables).

3 Detailled cost analysis of GKR

Proving validity of (1) can be reduced to proving 2 times the value of an expression of the form:

$$\sum_{0 \le i < 2^v} \frac{E[i]}{c - B[i]}$$

where E and B are 2 multilinear polynomials, respectively in the extension and in the base field (both in v variables), and c is in the extension field.

One way to implement GKR for this sums of fractions, which is **SIMD-friendly**, is to define the following polynomial (concatenation of the numerators and denominators):

$$G_1(X_1, \dots, X_{v+1}) = (1 - X_1).E(X_2, \dots, X_{v+1}) + X_1.(c - B(X_2, \dots, X_{v+1}))$$

G_1 is the GKR "top layer".

The next layer is obtained by summing 2-by-2 fractions:

$$
\begin{aligned}
G_2(\alpha_1, \dots, \alpha_v) = \sum_{(X_1,\dots,X_v)\in\{0,1\}^v} & eq((X_1, \dots, X_v), (\alpha_1, \dots, \alpha_v)) \cdot \\
& \Big[(1 - X_1) \cdot \Big(G_1(0, 0, X_2, \dots, X_v) \cdot G_1(1, 1, X_2, \dots, X_v) \\
& \qquad + G_1(0, 1, X_2, \dots, X_v) \cdot G_1(1, 0, X_2, \dots, X_v)\Big) \\
& \quad + X_1 \cdot G_1(1, 0, X_2, \dots, X_v) \cdot G_1(1, 1, X_2, \dots, X_v)\Big]
\end{aligned}
$$

3.1 First sumcheck round (of the top layer)

First, note that we can move out of the sum the "eq" factor containing X_1, as described by section 3.2 of [2].

The sumcheck polynomial we need to compute has degree one in X_1. Using section 3.1 of [2], we need simply need to evaluate it in one point. We suggest 1.

To conclude, the only computation the prover must perform in the first round is:

$$
\sum_{(X_2,\dots,X_v)\in\{0,1\}^{v-1}} eq((X_2, \dots, X_v), (\alpha_2, \dots, \alpha_v)) \cdot G_1(1, 0, X_2, \dots, X_v) \cdot G_1(1, 1, X_2, \dots, X_v)
$$

If we assume $eq((X_2, \dots, X_v), (\alpha_2, \dots, \alpha_v))$ has been previously computed, the prover cost is 2^v (ee) multiplications.

Trick 2: $G_1(1, 0, .)$ and $G_1(1, 1, .)$ correspond to denominator values in our sum of fractions, i.e. $G_1(1, 0, .) = c - i$ and $G_1(1, 1, .) = c - j$ for some values i, j in the **base field**. We can thus expand this part of the product: $(c - i) \cdot (c - j) = c^2 + (-c).(i + j) + ij$. c^2 and $-c$ can be precomputed. We are left with $2.(be) + (bb)$.

As a conclusion, the number of multiplications for the first sumcheck round, of the top GKR layer, is:

$$
2^{v-1} \cdot ((ee) + 2.(be) + (bb)) \approx \frac{1}{2} 2^v \text{ (ee)}
$$

Note that, after receiving the first random challenge, there is no need to "fold" any polynomials.

3.2 Next sumcheck rounds (of the top layer)

It is possible to compute the second sumcheck polynomial (of degree 3) in 5.2^{v-1} (ee) multiplications. (is it optimal?). After receiving the second random challenge, we need to fold 4 multilinear polynomials, each costing 2^{v-2} (ee) multiplications. Overall, the second round costs 7.2^{v-1} (ee) multiplications.

The third round costs 7.2^{v-2} (ee) multiplications, and so on.

Overall, all the consecutive rounds (omitting the first one) cost 7.2^v (ee) multiplications.

3.3 Next layers

The trick 2 (see 3.1) is only available for the first round of the top GKR layer. The cost of the GKR layer just before the top is 8.2^{v-1} (ee) multiplications. Then 8.2^{v-2}, etc.

3.4 Conclusion

$\frac{1}{2} + 7 + 8 = 15, 5$

$\boxed{\text{The total cost of the GKR is } 15, 5 \cdot 2^v \text{ (ee) multiplications}}$

References

[1] L. Soukhanov, "Logup*: faster, cheaper logup argument for small-table indexed lookups," Cryptology ePrint Archive, Paper 2025/946, 2025. [Online]. Available: https://eprint.iacr.org/2025/946

[2] A. Gruen, "Some improvements for the PIOP for ZeroCheck," 2024. [Online]. Available: https://eprint.iacr.org/2024/108