Lessons from integrating LogUp-GKR in the Miden VM

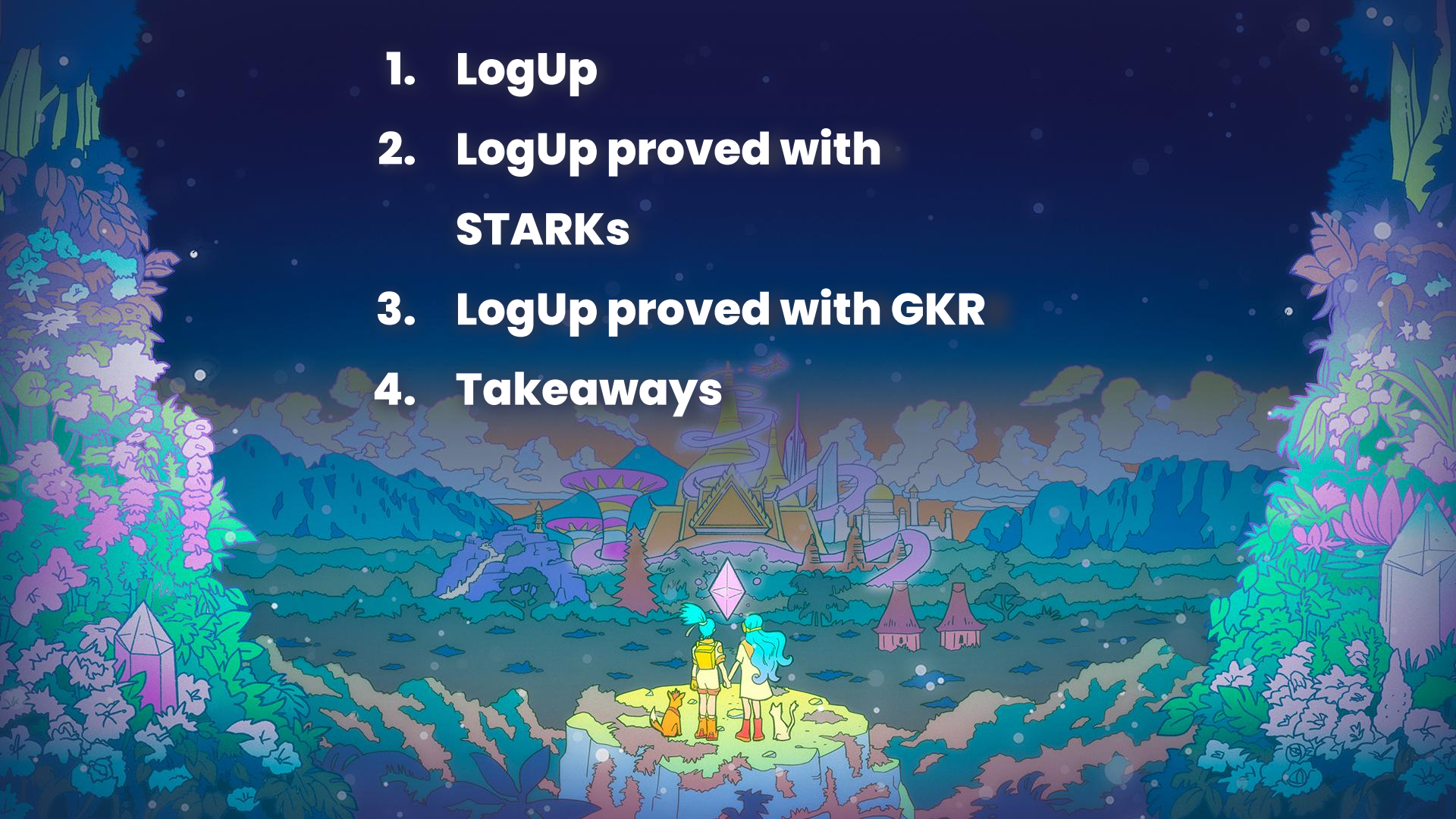
Philippe Laferriere
VM Engineer, Polygon Miden
bit.ly/logup-gkr

Improving logarithmic derivative lookups using GKR

Shahar Papini, Ulrich Haböck
spapini@starkware.co, uhaboeck@polygon.technology

September 18*, 2023

1. LogUp
2. LogUp proved with STARKs
3. LogUp proved with GKR
4. Takeaways



Section 1

LogUp

LogUp

LogUp is a protocol to prove the equality of two multisets.

$$\{1, 2, 3, 3\} \equiv \{3, 2, 1, 3\}$$

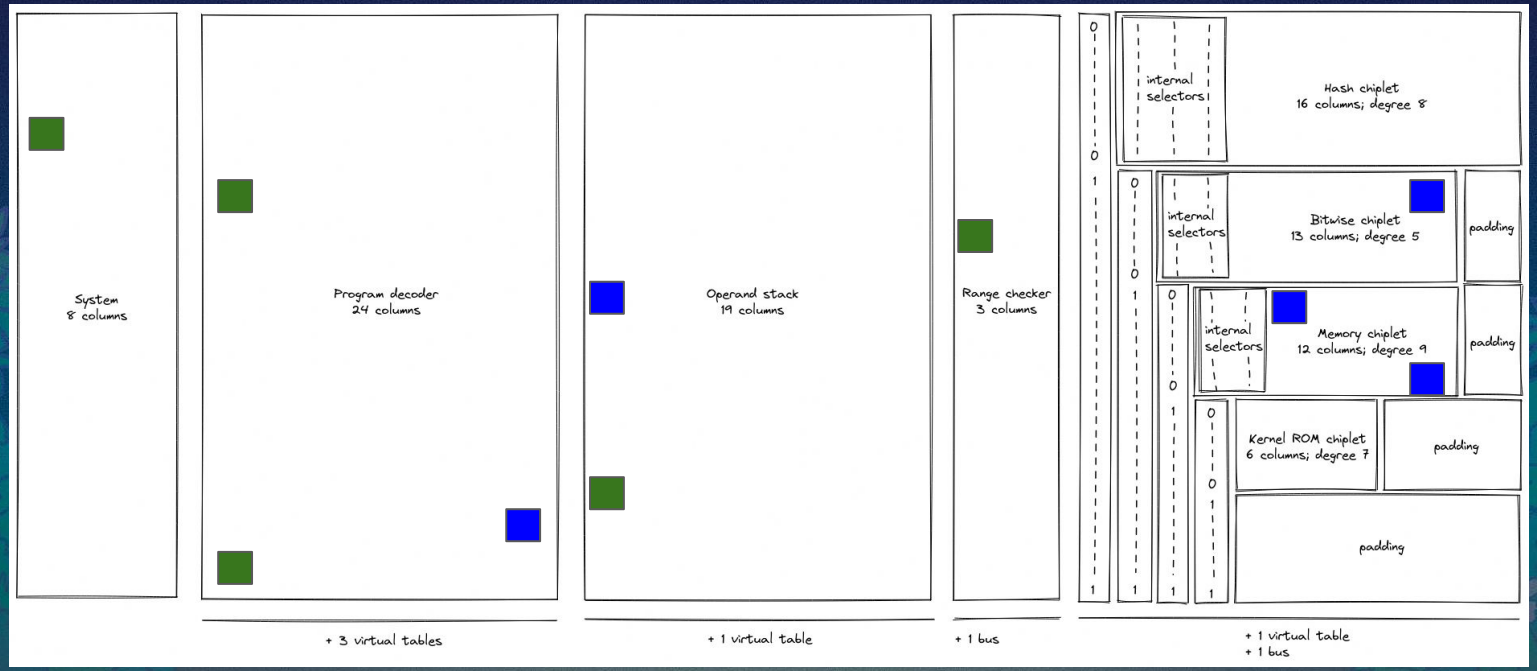
$$\{1, 2, 3, 3\} \not\equiv \{1, 2, 3\}$$

LogUp

Multiset checks are very useful in virtual machines:

- Enables practically unlimited stack depth
- Enables performing large numbers of range checks efficiently
- Communication between different parts of the trace

LogUp


System
8 columns
Program decoder
24 columns
Operand stack
19 columns
Range checker
3 columns
internal selectors
Hash chiplet
16 columns; degree 8
internal selectors
Bitwise chiplet
13 columns; degree 5
padding
internal selectors
Memory chiplet
12 columns; degree 9
padding
Kernel ROM chiplet
6 columns; degree 7
padding
padding
+ 3 virtual tables
+ 1 virtual table
+ 1 bus
+ 1 virtual table
+ 1 bus

$$\sum_{i=1}^{n-1}\left(\sum_{j=1}^{k}\frac{m_{a_{ij}}}{(\alpha - a_{ij})} - \frac{m_{b_{ij}}}{(\alpha - b_{ij})}\right) = 0$$

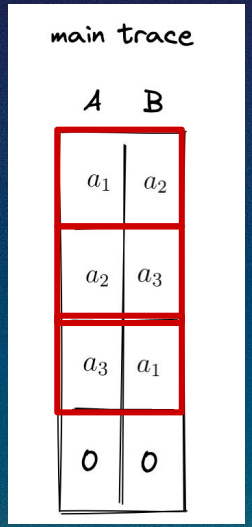
LogUp: the equation

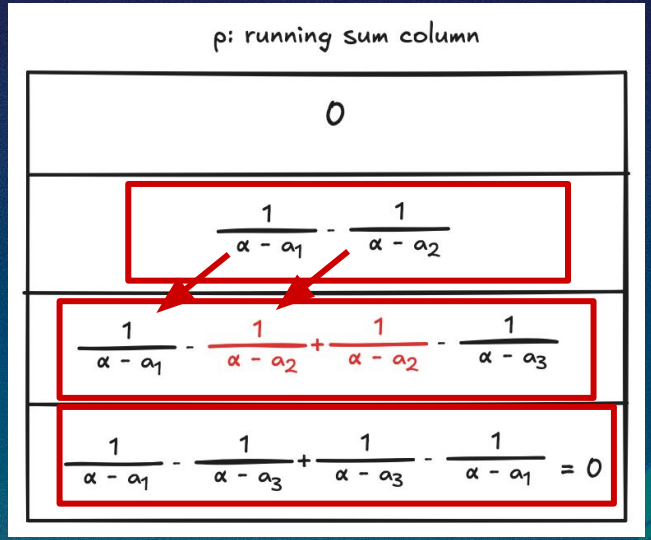
- n is the trace length
- k is the number of elements per trace row
- m_{aij} and m_{bij} are the *multiplicities*
- $\{a_{ij}\}$ is the first multiset
- $\{b_{ij}\}$ is the second multiset

Section 2

LogUp proved with STARKs

LogUp proved with STARKs





$$\sum_{i=1}^{n-1}\left(\sum_{j=1}^{k}\frac{m_{a_{ij}}}{(\alpha - a_{ij})} - \frac{m_{b_{ij}}}{(\alpha - b_{ij})}\right) = 0$$

LogUp proved with STARKs

p: running sum column

0
$\frac{1}{\alpha - a_1} - \frac{1}{\alpha - a_2}$
$\frac{1}{\alpha - a_1} - \frac{1}{\alpha - a_2} + \frac{1}{\alpha - a_2} - \frac{1}{\alpha - a_3}$
$\frac{1}{\alpha - a_1} - \frac{1}{\alpha - a_3} + \frac{1}{\alpha - a_3} - \frac{1}{\alpha - a_1} = 0$

$$p[i+1] = p[i] + \sum_{j=1}^{k} \frac{m_{a_{ij}}}{(\alpha - a_{ij})} - \frac{m_{b_{ij}}}{(\alpha - b_{ij})}$$

Degree 3

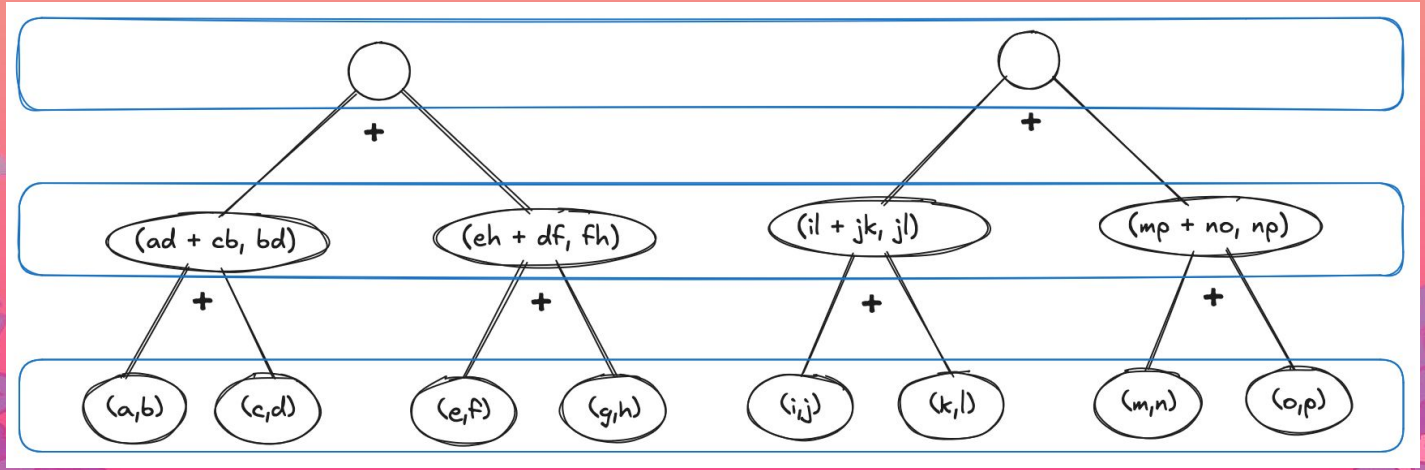
$$p[i+1](\alpha - a_{i0})(\alpha - b_{i0}) = p[i](\alpha - a_{i0})(\alpha - b_{i0}) + m_{a_i 0}(\alpha - b_{i0}) - m_{b_i 0}(\alpha - a_{i0})$$

Section 3

LogUp proved with GKR

LogUp proved with GKR

GKR is a protocol to prove the correct evaluation of a layered circuit



LogUp proved with GKR

$$\frac{f \cdot h(a \cdot d + c \cdot b) + b \cdot d(e \cdot h + g \cdot f)}{b \cdot d \cdot f \cdot h}$$

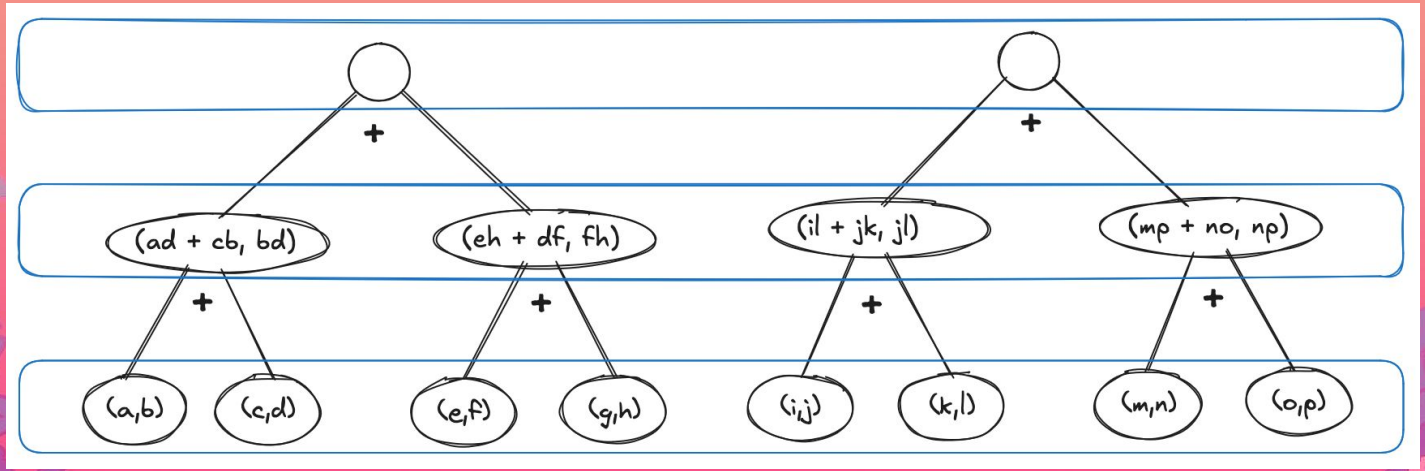
$$\uparrow$$

$$\frac{a \cdot d + c \cdot b}{b \cdot d} + \frac{e \cdot h + g \cdot f}{f \cdot h}$$

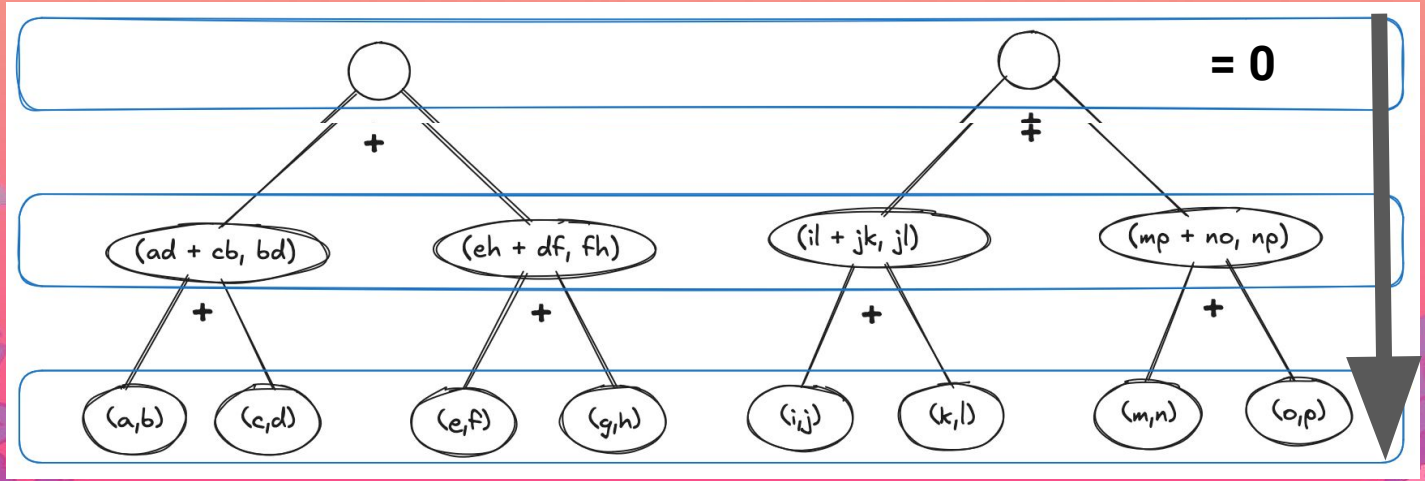
$$\uparrow$$

$$\frac{a}{b} + \frac{c}{d} + \frac{e}{f} + \frac{g}{h}$$

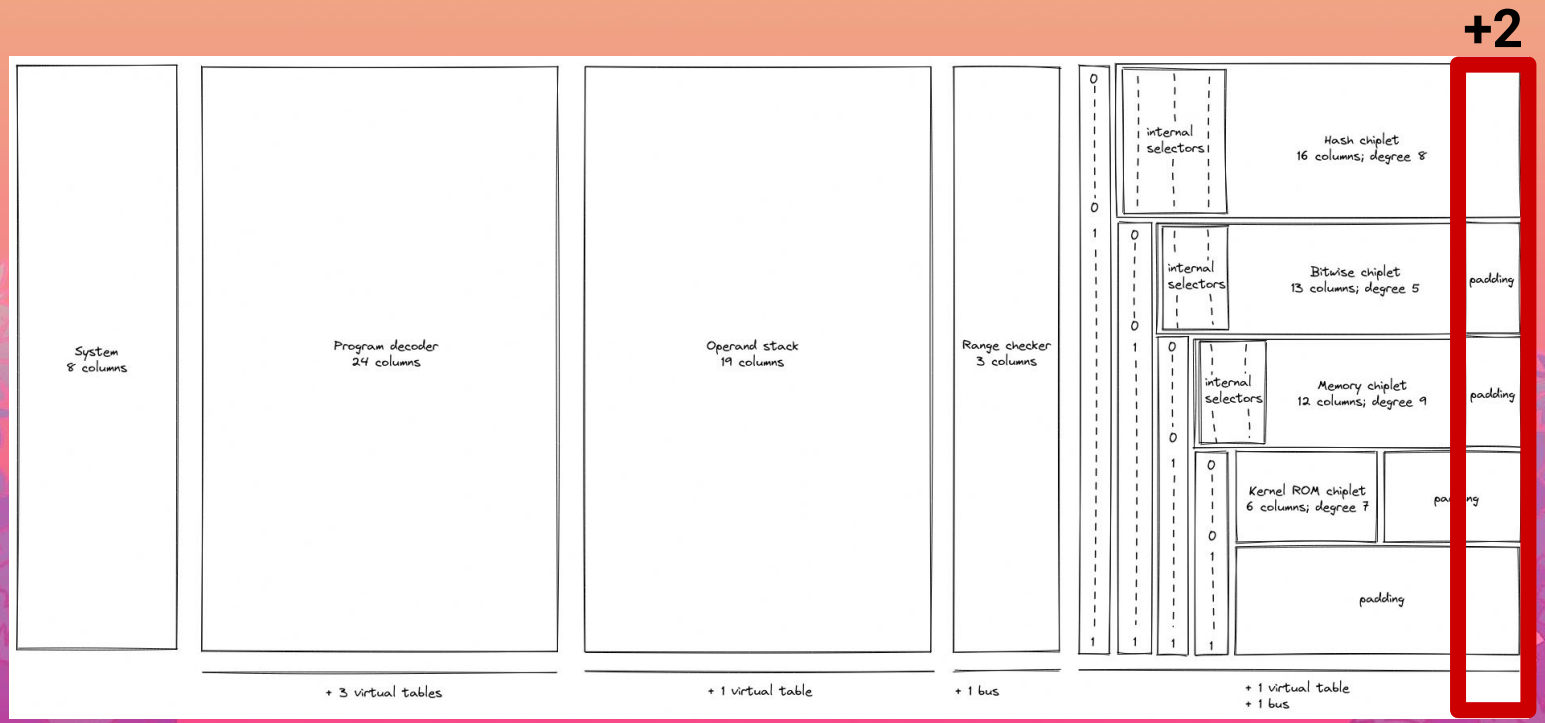
LogUp proved with GKR



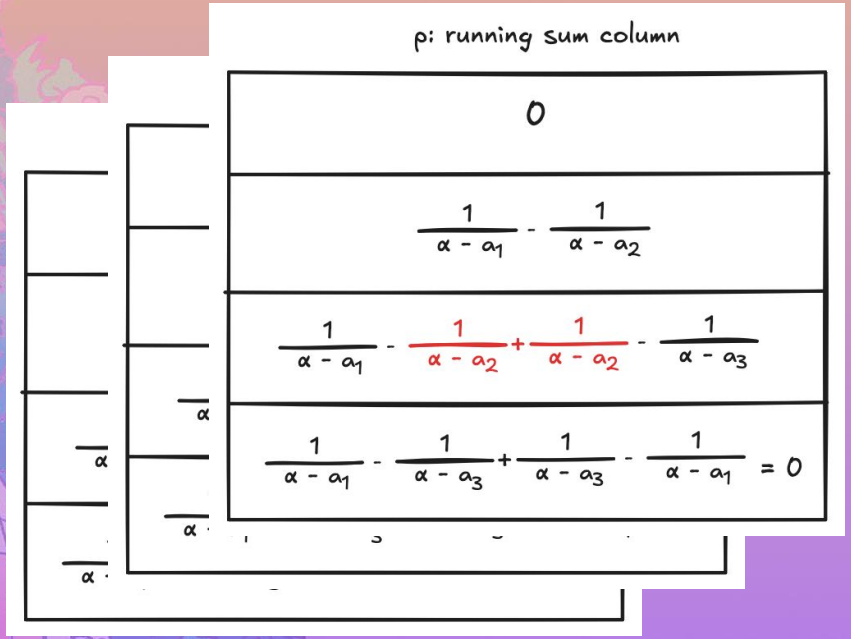
LogUp proved with GKR

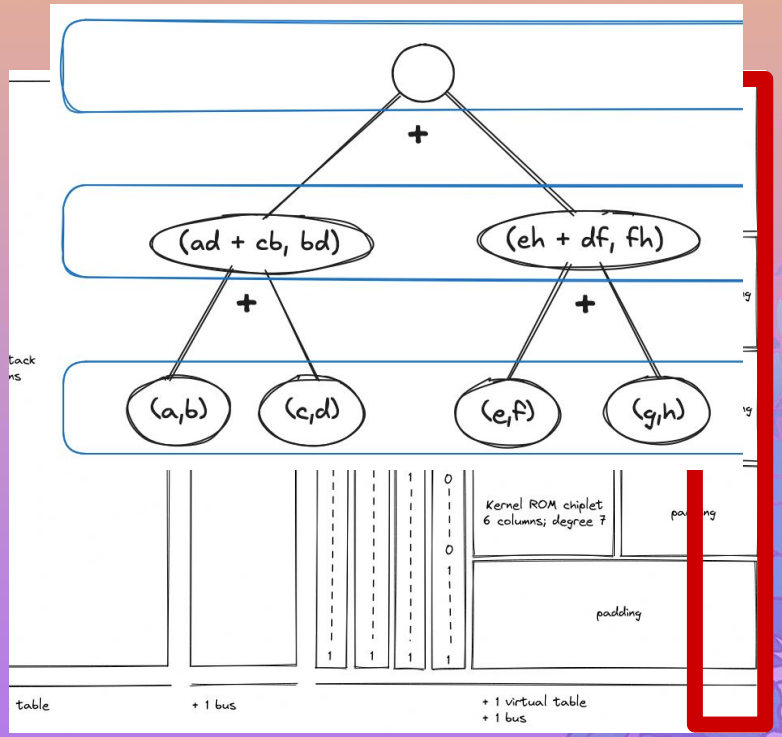


LogUp proved with GKR



STARKs vs GKR





Section 4

Takeaways

	Small	Large
Hash function speed	✓	
Degree of STARK constraints	✓	
Size of the bus		✓

Thank you!

Philippe Laferriere
VM Engineer, Polygon Miden
plafer@proton.me
@plafer2718
bit.ly/logup-gkr