PLONK Grand Product Polynomial Example

Generated by ChatGPT

Overview

This document illustrates a numeric example of the grand product argument in the PLONK zero-knowledge proof protocol. It highlights the role of the random field elements β and γ in verifying the permutation of wire assignments through a step-by-step computation.

Wire Assignment and Permutation

We consider a simple 2-gate circuit with 6 wire values and a known permutation mapping.

Index	**Value** v_i	**Permutation** $\sigma(i)$	**Result Term (mod 17)**
0	2	0	1
1	3	4	5
2	5	3	6
3	5	2	3
4	3	1	7
5	8	5	1

Mathematical Steps

We compute the term for each index using the formula:

$$\text{Term}_i = \frac{v_i + \beta \cdot \sigma(i) + \gamma}{v_i + \beta \cdot i + \gamma}$$

Let $\beta = 2$, $\gamma = 5$ in the field F_{17}.

$$\begin{aligned}
\text{Term}_0 &= \frac{2 + 2 \cdot 0 + 5}{2 + 2 \cdot 0 + 5} = \frac{7}{7} \equiv 1 \mod 17 \\
\text{Term}_1 &= \frac{3 + 2 \cdot 4 + 5}{3 + 2 \cdot 1 + 5} = \frac{16}{10} \equiv 5 \mod 17 \\
\text{Term}_2 &= \frac{5 + 2 \cdot 3 + 5}{5 + 2 \cdot 2 + 5} = \frac{16}{14} \equiv 6 \mod 17 \\
\text{Term}_3 &= \frac{5 + 2 \cdot 2 + 5}{5 + 2 \cdot 3 + 5} = \frac{14}{16} \equiv 3 \mod 17 \\
\text{Term}_4 &= \frac{3 + 2 \cdot 1 + 5}{3 + 2 \cdot 4 + 5} = \frac{10}{16} \equiv 7 \mod 17 \\
\text{Term}_5 &= \frac{8 + 2 \cdot 5 + 5}{8 + 2 \cdot 5 + 5} = \frac{6}{6} \equiv 1 \mod 17
\end{aligned}$$

Final Verification

Multiplying all terms:

$$1 \cdot 5 \cdot 6 \cdot 3 \cdot 7 \cdot 1 = 630 \equiv 1 \mod 17$$

This confirms that the grand product argument validates the wire value permutation.