PLONK Polynomial Interpolation Example

Problem Statement

We have an arithmetic circuit with **3 gates** (constraints) and the following witness assignments:

Gate	Left (L)	Right (R)	Output (O)	Constraint
1	a	b	c	$a \cdot b = c$
2	c	d	e	$c \cdot d = e$
3	e	f	g	$e \cdot f = g$

Witness Assignments

- $a = 2, b = 3 \implies c = 6$
- $d = 2 \implies e = 6 \times 2 = 12$
- $f = 2 \implies g = 12 \times 2 = 24$

Witness vector: $[a, b, c, d, e, f, g] = [2, 3, 6, 2, 12, 2, 24]$

Step 1: Define Gate Positions

We assign each gate to a unique root of unity (for simplicity, $x = 1, 2, 3$):

x	$L(x)$	$R(x)$	$O(x)$
1	$a = 2$	$b = 3$	$c = 6$
2	$c = 6$	$d = 2$	$e = 12$
3	$e = 12$	$f = 2$	$g = 24$

Step 2: Interpolate $L(x), R(x), O(x)$

We use **Lagrange interpolation** to find polynomials that fit these points.

1. Compute $L(x)$

Given points: $(1,2), (2,6), (3,12)$

Lagrange basis polynomials:

$$\ell_1(x) = \frac{(x-2)(x-3)}{(1-2)(1-3)} = \frac{(x-2)(x-3)}{2}$$

$$\ell_2(x) = \frac{(x-1)(x-3)}{(2-1)(2-3)} = \frac{(x-1)(x-3)}{-1}$$

$$\ell_3(x) = \frac{(x-1)(x-2)}{(3-1)(3-2)} = \frac{(x-1)(x-2)}{2}$$

Now, construct $L(x)$:

Now, construct $L(x)$:

$$L(x) = 2 \cdot \ell_1(x) + 6 \cdot \ell_2(x) + 12 \cdot \ell_3(x)$$

$$= 2 \cdot \frac{(x-2)(x-3)}{2} + 6 \cdot \frac{(x-1)(x-3)}{-1} + 12 \cdot \frac{(x-1)(x-2)}{2}$$

$$= (x-2)(x-3) - 6(x-1)(x-3) + 6(x-1)(x-2)$$

$$= x^2 - 5x + 6 - 6x^2 + 24x - 18 + 6x^2 - 18x + 12$$

$$= (x^2 - 6x^2 + 6x^2) + (-5x + 24x - 18x) + (6 - 18 + 12)$$

$$= x^2 + x + 0$$

Final $L(x)$:

$$L(x) = x^2 + x$$

2. Compute $R(x)$

Given points: $(1,3),(2,2),(3,2)$

Following the same method:

$$\begin{aligned}
R(x) &= 3 \cdot \frac{(x-2)(x-3)}{2} + 2 \cdot \frac{(x-1)(x-3)}{-1} + 2 \cdot \frac{(x-1)(x-2)}{2} \\
&= \frac{3}{2}(x^2-5x+6) - 2(x^2-4x+3) + (x^2-3x+2) \\
&= \frac{3}{2}x^2 - \frac{15}{2}x + 9 - 2x^2 + 8x - 6 + x^2 - 3x + 2 \\
&= \left(\frac{3}{2}x^2 - 2x^2 + x^2\right) + \left(-\frac{15}{2}x + 8x - 3x\right) + (9-6+2) \\
&= \frac{1}{2}x^2 - \frac{5}{2}x + 5
\end{aligned}$$

Final $R(x)$:

$$R(x) = \frac{1}{2}x^2 - \frac{5}{2}x + 5$$

3. Compute $O(x)$

Given points: $(1,6),(2,12),(3,24)$

$$\begin{aligned}
O(x) &= 6 \cdot \frac{(x-2)(x-3)}{2} + 12 \cdot \frac{(x-1)(x-3)}{-1} + 24 \cdot \frac{(x-1)(x-2)}{2} \\
&= 3(x^2-5x+6) - 12(x^2-4x+3) + 12(x^2-3x+2) \\
&= 3x^2 - 15x + 18 - 12x^2 + 48x - 36 + 12x^2 - 36x + 24 \\
&= (3x^2 - 12x^2 + 12x^2) + (-15x + 48x - 36x) + (18 - 36 + 24) \\
&= 3x^2 - 3x + 6
\end{aligned}$$

Final $O(x)$:

$$O(x) = 3x^2 - 3x + 6$$

Step 3: Construct $W(x) = L(x) \cdot R(x) - O(x)$

Now, compute $W(x)$:

$$W(x) = (x^2 + x)\left(\frac{1}{2}x^2 - \frac{5}{2}x + 5\right) - (3x^2 - 3x + 6)$$

$$= \frac{1}{2}x^4 - \frac{5}{2}x^3 + 5x^2 + \frac{1}{2}x^3 - \frac{5}{2}x^2 + 5x - 3x^2 + 3x - 6$$

$$= \frac{1}{2}x^4 - 2x^3 + \left(5x^2 - \frac{5}{2}x^2 - 3x^2\right) + (5x + 3x) - 6$$

$$= \frac{1}{2}x^4 - 2x^3 - \frac{1}{2}x^2 + 8x - 6$$

Step 4: Verify Divisibility by $Z(x) = (x-1)(x-2)(x-3)$

Check if $W(x)$ vanishes at $x = 1, 2, 3$:

1. $W(1) = \frac{1}{2}(1)^4 - 2(1)^3 - \frac{1}{2}(1)^2 + 8(1) - 6 = \frac{1}{2} - 2 - \frac{1}{2} + 8 - 6 = 0$
2. $W(2) = \frac{1}{2}(16) - 2(8) - \frac{1}{2}(4) + 16 - 6 = 8 - 16 - 2 + 16 - 6 = 0$
3. $W(3) = \frac{1}{2}(81) - 2(27) - \frac{1}{2}(9) + 24 - 6 = 40.5 - 54 - 4.5 + 24 - 6 = 0$

Since $W(x) = 0$ at all roots, $Z(x)$ divides $W(x)$.

Conclusion

The prover constructs:

- $L(x) = x^2 + x$
- $R(x) = \frac{1}{2}x^2 - \frac{5}{2}x + 5$
- $O(x) = 3x^2 - 3x + 6$
- $W(x) = \frac{1}{2}x^4 - 2x^3 - \frac{1}{2}x^2 + 8x - 6$

Since $W(x)$ is divisible by $Z(x)$, the proof is valid. The verifier confirms correctness **without learning the witness values.**