


PlonK Proving and Verifying

January 21, 2025

Distributed Lab

 zkdl-camp.github.io

 github.com/ZKDL-Camp



Plan

1 Setup

2 Proving

3 Verifying

Setup
●○

Proving
○○○○○○○○○

Verifying
○○○○○○○

Setup

Transcript Setup

Arithmetization \rightarrow 8 polynomials.

Add their commitments to transcript.

1. Encoding of the copy constraints:

$$\text{com}(S_{\sigma,1}), \quad \text{com}(S_{\sigma,2}), \quad \text{com}(S_{\sigma,3})$$

2. Encoding of the gate constraints:

$$\text{com}(q_L), \quad \text{com}(q_R), \quad \text{com}(q_M), \quad \text{com}(q_O), \quad \text{com}(q_C)$$

Setup
○○

Proving
●○○○○○○○○

Verifying
○○○○○○○

Proving

Proving: Round 1

Interpolate polynomials a', b', c' over corresponding columns of T .

Sample random $b_1, b_2, b_3, b_4, b_5, b_6 \xleftarrow{R} \mathbb{F}$.

Let the blinded polynomials be:

$$\mathbf{a} := (b_1X + b_2)Z_\Omega(X) + a'(X)$$

$$\mathbf{b} := (b_3X + b_4)Z_\Omega(X) + b'(X)$$

$$\mathbf{c} := (b_5X + b_6)Z_\Omega(X) + c'(X)$$

Add to the transcript commitments of computed above polynomials:

$$\text{com}(a), \quad \text{com}(b), \quad \text{com}(c)$$

Proving: Round 2

Sample random $\beta, \gamma \xleftarrow{R} \mathbb{F}$. Let $z_0 = 1$. $\forall k = 0, \dots, N$:

$$z_{k+1} = z_k \times \frac{(a_k + \beta \omega^k + \gamma)(b_k + \beta \omega^k k_1 + \gamma)(c_k + \beta \omega^k k_2 + \gamma)}{(a_k + \beta S_{\sigma,1}(\omega^k) + \gamma)(b_k + \beta S_{\sigma,2}(\omega^k) + \gamma)(c_k + \beta S_{\sigma,3}(\omega^k) + \gamma)}$$

Interpolate polynomial z' over evaluations (z_0, \dots, z_{N-1}) .

Sample random $b_7, b_8, b_9 \xleftarrow{R} \mathbb{F}$. Compute:

$$z := (b_7 X^2 + b_8 X + b_9) Z_H + z'$$

Add to the transcript $\text{com}(z)$.

Proving: Round 3

Sample random $\alpha \xleftarrow{R} \mathbb{F}$. Interpolate π over Π .

$$p_1 = aq_L + bq_R + abq_M + cq_o + q_C + \pi$$

$$p_2 = (a + \beta X + \gamma)(b + \beta k_1 X + \gamma)(ac + \beta k_2 X + \gamma)z - \\ - (a + \beta S_{\sigma,1} + \gamma)(b + \beta S_{\sigma,2} + \gamma)(ac + \beta S_{\sigma,3} + \gamma)az(\omega X)$$

$$p_3 = (az - 1)L_1$$

Define the composite polynomial:

$$p = p_1 + \alpha p_2 + \alpha^2 p_3$$

Proving: Round 3

For $t'_{\text{lo}}, t'_{\text{mid}}, t'_{\text{hi}} \in \mathbb{F}^{\leq(N+1)}[X]$ polynomials of degree at most $N+1$:

$t = t'_{\text{lo}} + X^{N+2}t'_{\text{mid}} + X^{2(N+2)}t'_{\text{hi}}$. Compute t such that $p = tZ_{\Omega}$.

Sample random $b_{10}, b_{11} \xleftarrow{R} \mathbb{F}$. Define:

$$\begin{aligned}t_{\text{lo}} &= t'_{\text{lo}} + b_{10}X^{N+2} \\t_{\text{mid}} &= t'_{\text{mid}} - b_{10} + b_{11}X^{N+2} \\t_{\text{hi}} &= t'_{\text{hi}} - b_{11}\end{aligned}$$

Add to the transcript commitments:

$$\text{com}(t_{\text{lo}}), \quad \text{com}(t_{\text{mid}}), \quad \text{com}(t_{\text{hi}}).$$

Proving: Round 4

Sample random $\zeta \xleftarrow{R} \mathbb{F}$.

Add to the transcript following evaluations:

$$\bar{a} = a(\zeta), \quad \bar{b} = b(\zeta), \quad \bar{c} = c(\zeta)$$

$$\bar{s}_{\sigma,1} = s_{\sigma,1}(\zeta), \quad \bar{s}_{\sigma,2} = s_{\sigma,2}(\zeta), \quad \bar{z}_{\omega} = z(\zeta\omega)$$

Proving: Round 5

Sample random $v \xleftarrow{R} \mathbb{F}$. Let:

$$\hat{p}_{nc1} = \bar{a}q_L + \bar{b}q_R + \bar{a}\bar{b}q_M + \bar{c}q_o + q_C$$

$$\begin{aligned} \hat{p}_{nc2} = & (\bar{a} + \beta\zeta_1 + \gamma)(\bar{b} + \beta k_1\zeta_1 + \gamma)(\bar{c} + \beta k_2\zeta_1 + \gamma)z - \\ & - (\bar{a} + \beta\bar{S}_{\sigma_1} + \gamma)(\bar{b} + \beta\bar{S}_{\sigma_2} + \gamma)(\bar{c} + \beta\bar{S}_{\sigma_3} + \gamma)z(\omega\zeta_1) \end{aligned}$$

$$\hat{p}_{nc3} = L_1(\zeta_1)z$$

Define:

$$\begin{aligned} p_{nc} &= p_{nc1} + \alpha p_{nc2} + \alpha^2 p_{nc3} \\ t_{\text{partial}} &= t_{lo} + \zeta^{N+2} t_{\text{mid}} + \zeta^{2(N+2)} t_{hi} \end{aligned}$$

Proving: Round 5

Define:

$$f_{batch} = t_{partial} + v p_{nc} + v^2 a + v^3 b + v^4 c + v^5 S_{o1} + v^6 S_{o2}$$

Definition

π_{batch} - opening proof at ζ of f_{batch} .

π_{single} - opening proof at $\zeta\omega$ of z .

Compute:

$$\hat{p}_{nc} := p_{nc} \zeta$$

$$\hat{t} := t \zeta$$

Proof

Definition

PlonK proof consists of the following values:

$$\begin{aligned} &com(a), com(b), com(c), com(z), \\ &com(t_{lo}), com(t_{mid}), com(t_{hi}), \\ &\bar{a}, \bar{b}, \bar{c}, \bar{S}_{o1}, \bar{S}_{o2}, \bar{z}_w, \\ &\pi_{batch}, \pi_{single}, \bar{p}_{nc}, \bar{t} \end{aligned}$$

Setup
○○

Proving
○○○○○○○○○○

Verifying
●○○○○○○

Verifying

Verifier computes all challenges:

1. Add $\text{com}(a)$, $\text{com}(b)$, $\text{com}(c)$ to the transcript.
2. Sample two challenges β, γ .
3. Add $\text{com}(z)$ to the transcript.
4. Sample a challenge α .
5. Add $\text{com}(t_{lo})$, $\text{com}(t_{mid})$, $\text{com}(t_{hi})$ to the transcript.
6. Sample a challenge ζ .
7. Add \bar{a} , \bar{b} , \bar{c} , \bar{S}_{o1} , \bar{S}_{o2} , \bar{z}_w to the transcript.
8. Sample a challenge v .

Compute $pi(\zeta)$

Observation

We don't need to compute whole pi , only one evaluation.

$$pi(\zeta) = \sum_{i=0}^n L_i(\zeta) \Pi_i$$

Where n is the number of public inputs and L_i is the Lagrange basis.

Compute claimed $p(\zeta)$

Compute:

$$\bar{p}_c = p_1(\zeta) + \alpha z_w (\bar{c} + \gamma) (\bar{a} + \beta \bar{S}_{\sigma_1} + \gamma) (\bar{b} + \beta \bar{S}_{\sigma_2} + \gamma) - \alpha^2 L_1(\zeta)$$

This is the constant part of the linearization of p . So, adding it to what the prover claims to be \bar{p}_{nc} , he obtains $p(\zeta) = \bar{p}_c + \bar{p}_{nc}$.

Compute $\text{com}(t_{\text{partial}})$ and $\text{com}(p_{nc})$

He computes these of the commitments in the proof as follows:

$$\text{com}(t_{\text{partial}}) = \text{com}(t_{lo}) + \zeta^{N+2} \text{com}(t_{mid}) + \zeta^{2(N+2)} \text{com}(t_{hi})$$

For the second one, compute those:

$$\begin{aligned} \hat{p}_{nc1} = & \bar{a} * \text{com}(q_L) + \bar{b} * \text{com}(q_R) + (\bar{a}\bar{b}) * \text{com}(q_M) + \\ & + \bar{c} * \text{com}(q_o) + \text{com}(q_C) \end{aligned}$$

$$\begin{aligned} \hat{p}_{nc2} = & (\bar{a} + \beta\zeta_1 + \gamma)(\bar{b} + \beta k_1\zeta_1 + \gamma)(\bar{c} + \beta k_2\zeta_1 + \gamma) * \text{com}(z) - \\ & - (\bar{a} + \beta\bar{S}_{\sigma_1} + \gamma)(\bar{b} + \beta\bar{S}_{\sigma_2} + \gamma)(\bar{c} + \beta\bar{S}_{\sigma_3} + \gamma) * \text{com}(z)(\omega\zeta_1) \end{aligned}$$

$$\hat{p}_{nc3} = L_1(\zeta_1) * \text{com}(z)$$

Then:

$$\text{com}(p_{nc}) = \text{com}(p_{nc1}) + \text{com}(p_{nc2}) + \text{com}(p_{nc3})$$

Compute claimed value $f_{batch}(\zeta)$ and $com(f_{batch})$

$$\begin{aligned} f_{batch}(\zeta) &= \bar{t} + v\bar{p}_{nc} + v^2\bar{a} + v^3\bar{b} + v^4\bar{c} + v^5\bar{S}_{o1} + v^6\bar{S}_{o2} \\ com(f_{batch}) &= com(t_{partial}) + v * com(p_{nc}) + v^2 * com(a) + \\ &\quad + v^3 * com(b) + v^4 * com(c) + \\ &\quad + v^5 * com(S_{o1}) + v^6 * com(S_{o2}) \end{aligned}$$

Proof check

Now the verifier has all the necessary values to proceed with the checks.

- Check that $p(\zeta)$ equals $(\zeta^N - 1)t(\zeta)$.
- Verify the opening of f_{batch} at ζ . That is, check that

$\text{Verify}([f_{batch}], \pi_{batch}, \zeta, f_{batch}(\zeta))$ outputs Accept.

- Verify the opening of z at ζ_w . That is, check the validity of the proof π_{single} using the commitment $com(z)$ and the value \bar{z}_w .

That is, check that $\text{Verify}(com(z), \pi_{single}, \zeta_w, \bar{z}_w)$ outputs Accept.