PlonK Proving and Verifying

January 21, 2025

Distributed Lab

zkdl-camp.github.io

github.com/ZKDL-Camp

Plan

1. Gadgets
2. Setup
3. Proving
4. Verifying

Gadgets

Gadgets - Commitments

1. $\text{Commit}(f) \rightarrow com(f) \in G$
2. $\text{Open}(f, \zeta) \rightarrow \pi \in G$
3. $\text{Verify}(com(f), \pi, \zeta, y) \rightarrow Accept$ if $f(\zeta) = y$ w.h.p.

Gadgets - Blindings

Hide the polynomial

Let $a \in \mathbb{F}[X]$ be a polynomial of degree N. Select $M \geq N$. Then polynomial a_{blinded} will be of degree M and is defined as:

$$
\begin{aligned}
z_H &= X^N - 1 \\
k &= M - N \\
b_0, \dots, b_k &\xleftarrow{R} \mathbb{F} \\
a_{\text{blinded}} &= (b_0 + b_1 X + \cdots + b_k X^k) z_H + a
\end{aligned}
$$

Setup

Transcript Setup

Arithmetization $\rightarrow$ 8 polynomials.
Add their commitments to transcript.

1. **Encoding of the copy constraints:**

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

2. **Encoding of the gate constraints:**

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

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:

$$\mathbf{a} := (b_1 X + b_2) Z_\Omega(X) + a'(X)$$
$$\mathbf{b} := (b_3 X + b_4) Z_\Omega(X) + b'(X)$$
$$\mathbf{c} := (b_5 X + b_6) Z_\Omega(X) + c'(X)$$

Add to the transcript commitments of computed above polynomials:

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

Proving: Round 2

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

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

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

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

$$\mathsf{z} := (b_7 X^2 + b_8 X + b_9) Z_H + z'$$

Add to the transcript com(z).

Proving: Round 3

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

$$
\begin{aligned}
p_1 &= aq_L + bq_R + abq_M + cq_o + q_C + \pi \\
p_2 &= (a + \beta X + \gamma)(b + \beta k_1 X + \gamma)(ac + \beta k_2 X + \gamma)z - \\
&\quad - (a + \beta S_{\sigma,1} + \gamma)(b + \beta S_{\sigma,2} + \gamma)(ac + \beta S_{\sigma,3} + \gamma)az(\omega X) \\
p_3 &= (az - 1)L_1
\end{aligned}
$$

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:

$$\hat{p}_{nc1} = \bar{a}q_L + \bar{b}q_R + \bar{a}\bar{b}q_M + \bar{c}q_o + q_C$$
$$\hat{p}_{nc2} = (\bar{a} + \beta\zeta_1 + \gamma)(\bar{b} + \beta k_1\zeta_1 + \gamma)(\bar{c} + \beta k_2\zeta_1 + \gamma)z -$$
$$- (\bar{a} + \beta\bar{S}_{\sigma_1} + \gamma)(\bar{b} + \beta\bar{S}_{\sigma_2} + \gamma)(\bar{c} + \beta\bar{S}_{\sigma_3} + \gamma)z(\omega\zeta_1)$$
$$\hat{p}_{nc3} = L_1(\zeta_1)z$$

Define:

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

Proving: Round 5

Define:

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

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:

$$\begin{aligned} com(a), com(b), com(c), com(z), \\ com(t_{lo}), com(t_{mid}), com(t_{hi}), \\ \bar{a}, \bar{b}, \bar{c}, \bar{S}_{\sigma 1}, \bar{S}_{\sigma 2}, \bar{z}_w, \\ \pi_{batch}, \pi_{single}, \bar{p}_{nc}, \bar{t} \end{aligned}$$

Verifying

Verifier computes all challenges:

1. Add com(a), com(b), com(c) to the transcript.
2. Sample two challenges β, γ.
3. Add com(z) to the transcript.
4. Sample a challenge α.
5. Add com(t_{lo}), com(t_{mid}), 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 υ.

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:

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

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 com($t_{partial}$) and com(p_{nc})

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

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

For the second one, compute those:

$$\begin{aligned}
\hat{p}_{nc1} &= \bar{a} * com(q_L) + \bar{b} * com(q_R) + (\bar{a}\bar{b}) * com(q_M) + \\
&\quad + \bar{c} * com(q_o) + com(q_C) \\
\hat{p}_{nc2} &= (\bar{a} + \beta\zeta_1 + \gamma)(\bar{b} + \beta k_1 \zeta_1 + \gamma)(\bar{c} + \beta k_2 \zeta_1 + \gamma) * com(z) - \\
&\quad - (\bar{a} + \beta\bar{S}_{\sigma_1} + \gamma)(\bar{b} + \beta\bar{S}_{\sigma_2} + \gamma)(\bar{c} + \beta\bar{S}_{\sigma_3} + \gamma) * com(z)(\omega\zeta_1) \\
\hat{p}_{nc3} &= L_1(\zeta_1) * com(z)
\end{aligned}$$

Then:

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

.

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

$$f_{batch}(\zeta) = \bar{t} + \upsilon \bar{p}_{nc} + \upsilon^2 \bar{a} + \upsilon^3 \bar{b} + \upsilon^4 \bar{c} + \upsilon^5 \bar{S}_{o1} + \upsilon^6 \bar{S}_{o2}$$

$$\begin{aligned} com(f_{batch}) = {} & com(t_{partial}) + \upsilon * com(p_{nc}) + \upsilon^2 * com(a) + \\ & + \upsilon^3 * com(b) + \upsilon^4 * com(c) + \\ & + \upsilon^5 * com(S_{o1}) + \upsilon^6 * com(S_{o2}) \end{aligned}$$

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

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

- 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 Verify$(com(z), \pi_{single}, \zeta_w, \bar{z}_w)$ outputs Accept.