Plonk and Poseidon

Dmitry Khovratovich
Ethereum Foundation and Dusk Network

December 27, 2019

Suppose $\mathbb{F}$ has a multiplicative subgroup H of order $n-1$.

Consider an arithmetic circuit of n gates representable in the following form ($i \in [n]$):

$$(\mathbf{q_L})_i \cdot \mathrm{x}_{\mathbf{a}_i} + (\mathbf{q_R})_i \cdot \mathrm{x}_{\mathbf{b}_i} + (\mathbf{q_O})_i \cdot \mathrm{x}_{\mathbf{c}_i} + (\mathbf{q_M})_i \cdot \mathrm{x}_{\mathbf{a}_i} \cdot \mathrm{x}_{\mathbf{b}_i} + \mathbf{q_C}_i \tag{1}$$

where $\mathbf{a}, \mathbf{b}, \mathbf{c} \in [m]^n$ (wire assignment vectors).

Let $\mathfrak{S}$ be partition of $[3n]$ according to $\mathbf{a}, \mathbf{b}, \mathbf{c}$ (i.e. m sets). Let σ be a permutation on $[3n]$ such that it consists of m cycles going over the elements of $\mathfrak{S}$.

1 Protocol

1. Let f_L, f_R, f_O be polynomials interpolating on $\mathrm{x}_\mathbf{a}, \mathrm{x}_\mathbf{b}, \mathrm{x}_\mathbf{c}$:
$$f_L(g^i) = \mathrm{x}_{\mathbf{a}_i}.$$
Prover commits to them. Let $\mathbf{q}_L, \mathbf{q}_R, \mathbf{q}_O, \mathbf{q}_M, \mathbf{q}_C$ interpolate the selector vectors.
2. Prover proves wire consistency using σ and f_L, f_R, f_O. He proves that $\sigma(f_L, f_R, f_O) = (f_L, f_R, f_O)$.
3. Prover proves the circuit polynomials on H^*:
$$\mathbf{q}_L f_L + \mathbf{q}_R f_R + \mathbf{q}_O f_O + \mathbf{q}_M f_L f_R + \mathbf{q}_C + PI = 0$$
This proof is combined with identity proofs from the previous step.

2 Extras

2.1 Permutation check

$\sigma(f_1, f_2, \ldots, f_k) \stackrel{?}{=} (g_1, g_2, \ldots, g_k)$:

1. Define
$$f'_j = f_j + \beta \cdot \underbrace{(j-1)n + \log_\mathbf{g} x}_{S_{ID_j}} + \gamma$$
and
$$g'_j = g_j + \beta \cdot \underbrace{\sigma((j-1)n + \log_\mathbf{g} x)}_{S_{\sigma_j}} + \gamma$$
2. Define multiproduct
$$f' = \prod f'_j; \quad g' = \prod g'_j.$$
3. Define incremental product polynomial:
$$Z(\mathbf{g}^i) = f'(\mathbf{g}) \cdot f'(\mathbf{g}^2) \cdots f'(\mathbf{g}^{i-1});$$
$$Z^*(\mathbf{g}^i) = g'(\mathbf{g}) \cdot g'(\mathbf{g}^2) \cdots g'(\mathbf{g}^{i-1}).$$
4. Prover commits to Z, Z^*.

5. Prover proves the following equations for all $a \in H$, which are sufficient for the permutation check:

$$
\begin{aligned}
[a = \mathbf{g}](Z(a) - Z^*(a)) &= 0; \\
Z(a)f'(a) &= Z(a\mathbf{g}); \\
Z^*(a)g'(a) &= Z^*(a\mathbf{g}); \\
[a = \mathbf{g}^n](Z(a\mathbf{g}) - Z^*(a\mathbf{g})) &= 0.
\end{aligned}
$$

   The correctness as follows. Let $\sigma(i) \neq i$ for some i. Then an elementary proof implies that $f' \neq g'$, which means that the fourth equation can not hold with the other three.

   For such a proof we use the polynomial range check, where we use polynomials $Z, Z^*, f_L, f_R, f_O, T, S_{ID}, S_{\sigma_1}, S_{\sigma_2}, S_{\sigma_3}$; and $t^* = 2$ (since we use a and $a\mathbf{g}$).

2.2 Polynomial identities on ranges

For $f_1, f_2, \ldots, f_t$ of degree d we test identities of form:

$$
F := G(f_{i_1}(v_1(X)), \ldots, f_{i_M}(v_M(X))) \equiv 0 \tag{2}
$$

where v_i has degree d and the resulting polynomial F has degree D.

From a protocol on range S with k identities we can get a protocol on the full $\mathbb{F}$ by adding random challenges $a_1, a_2, \ldots, a_k$ and verifying that

$$
\sum_i a_i F_i \equiv T \cdot \prod_{x \in S} (X - x)
$$

for a polynomial T, which should be computed by division and also committed.

For given protocol, we define

- d_i be $deg(f_i)$;
- $t^* \leq M$ be the number of distinct v_i in the identity and e_j be the maximum of $(d_i + 1)$ in the partition of M.
- $\mathbf{e}$ be the sum of $(d_i + 1)$ plus sum of e_j

To prove an identity, the prover computes a challenge point x, then shows t^* values $f_{i_j}(v_j(x))$, then proves their correctness in the opening protocol. Verifer checks the identity on this point (t^* communication).

In the generic arithmetic circuit we have $d_i = n - 1$ for polynomials f_L, f_R, f_O, $d = n$ for polynomial Z, $d = 3n - 1$ for polynomial T. We have $t^* = 2$ as there are two evaluation points. We have $e_1 = 3n - 1$ and $e_2 = n - 1$, so $\mathbf{e} = 3(n) + (n + 1) + (3n) + (3n) + (n + 1) = 11n + 2$ (in the paper it is $11n + 2$).

2.3 Polynomial commitment scheme

Let $\{f_i\}$ be polynomials of degree d, which are evaluated at points z, z'.

The commitment is done using universal setup $[x]_1, [x^2]_1, \ldots, [x^d]_1, [x]_2$ and producing $cm_i = [f_i(x)]$ using d multiplications.

Opening with s_i, s_i':

1. γ, γ' are challenges.
2. Compute $h(X) = \sum_i \gamma^i \frac{f_i(X) - f_i(z)}{X - z}$, $\quad h'(X) = \sum_i \gamma'^i \frac{f_i(X) - f_i(z')}{X - z'}$, and $W = [h(X)]_1, W' = [h(X)']$.
3. r, r' are challenges.
4. Compute $F = \sum_i \left(r(\gamma^i cm_i - [\gamma^i s_i]_1) + r'(\gamma'^i cm_i - [\gamma'^i s_i]_1) \right)$.
5. Check if
$$
e(F + rzW + r'z'W\,[1]_2) = e(rW + r'W', [x]_2).
$$

3 Plonk Prover for Poseidon

3.1 Poseidon

Consider a Poseidon permutation $\mathcal{F}$ of width w, which transforms the array of w field elements $I[1\dots w]$ to the array of outputs $O[1\dots w]$. Suppose we want to prove the knowledge of preimage for the hash output H:

$$PoK\{I[2\dots w], O[1, 3\dots w] \mid \mathcal{F}(0_{\mathbb{F}}, I[2\dots w]) = (O[1], H, O[3\dots w])\ \}$$

The array I undergoes the Poseidon permutation as follows:

1. For R_F rounds, $1 \le r \le R_F$:
   (a) $I[j] \leftarrow (I[j])^5$ for all j (exponentiation in the field);
   (b) $I \leftarrow A \cdot I + c(r)$ where A is a field matrix and $c(r)$ is the round constant array.
2. For R_P rounds, $R_F < r \le R_F + R_P$:
   (a) $I[w] \leftarrow (I[w])^5$;
   (b) $I \leftarrow A \cdot I + c(r)$ where $c(r)$ is the round constant array.
3. For R_F rounds, $R_F + R_P < r \le R = 2 * R_F + R_P$:
   (a) $I[j] \leftarrow (I[j])^5$ for all j;
   (b) $I \leftarrow A \cdot I + c(r)$ where $c(r)$ is the round constant array.

Let I_r be the input state for round r and additionally $I_{R+1} = O$.

3.2 Regular Plonk prover

We can convert Poseidon to a regular arithmetic circuit with additions and multiplications of fan-in 2. We would need then 3 multiplication gates per S-box and $w(w-1)$ addition gates for the matrix multiplication, which totals to $w(w-1)R + 3R + 7wR$ assuming 8 full rounds. Thus the prover costs are at least $11(w(w+6)+3)R$ exponentiations, and proof has 7 $\mathbb{G}$ and 7 $\mathbb{F}$ elements.

3.3 Advanced prover

Let us define w polynomials of degree R on $H^* = \{g, g^2, \dots, g^{R+1}\}$:

$$f_i(g^r) = I_r[i].$$

Let us also define indicator polynomials and round constant polynomials:

$$W(g^r) = \begin{cases} 1 \text{ if } R_F < r \le R_F + R_P; \\ 0 \text{ otherwise} \end{cases} . \tag{3}$$

$$\mathbf{C}(g^r) = c(r). \tag{4}$$

Then it suffices to prove the following system of equations:

$$A \cdot \begin{bmatrix} f_1(X)(1-W(X)) + f_1(X)^5 W(X) \\ f_2(X)(1-W(X)) + f_2(X)^5 W(X) \\ \cdots \\ f_{w-1}(X)(1-W(X)) + f_{w-1}(X)^5 W(X) \\ f_w(X)^5 \end{bmatrix} + \mathbf{C}(X) = \begin{bmatrix} f_1(gX) \\ f_2(gX) \\ \cdots f_{w-1}(gX) \\ f_w(gX) \end{bmatrix} \tag{5}$$

$$f_1(g) = 0; \tag{6}$$

$$f_2(g^{R+1}) = H. \tag{7}$$

The last two (boundary) equations are proven by opening the committed polynomials at two points. The first w identities are combined into a single identity F' of degree $6R$ using the challenge vector $[1, y, y^2, \dots, y^{w-1}]$. We also add the residual polynomial T of degree $5R$ which is the division of F' by Z_H. We thus get an identity of form

$$F := G(f_{i_1}(v_1(X)), \dots, f_{i_M}(v_M(X))) \equiv 0$$

with $D = 6R, M = 2w$ with w internal polynomials of degree $d_i = R$ and one of degree $5R$. There are two different $v()$ polynomials, as in Plonk, so we get $t^* = 2$. We also have $e_1 = 5R, e_2 = R$, so $\mathbf{e} = (w + 11)R$.

Lemma 4.7 of the Plonk paper implies that we get a Plonk prover for a Poseidon R-round permutation of width w, which has $(w + 11)R$ prover exponentiations in $\mathbb{G}_1$, prover communication being $w + 3$ $\mathbb{G}_1$ elements and $2w$ $\mathbb{F}$ elements, and verifier complexity being $w + 3$ exponentiations in $\mathbb{G}_1$, two pairings and one evaluation of G of degree 5. For $w = 3$ we get the prover cost being 25 times smaller, and for $w = 5$ the improvement is up to 40x compared to the regular Plonk.

3.4 Not quite an improvement

Instead of exponentiating to the power of 5, we can use $2w$ additional polynomials:

$$f'_i(X) = f_i(X)^2; \quad f''_i(X) = f'_i(X)^2.$$

The resulting identity F' has degree $3R$, and the quotient polynomial T has degree $2R$. We then have $e_1 = 2R$ and $\mathbf{e} = 3wR + 2R + 2R + R = (3w + 5)R$, which is not smaller than $(w + 11)R$.

Using only one additional polynomial which is a cube of f_i, would give the identity F' of degree $4R$, polynomial T of degree $3R$ and $\mathbf{e} = 2wR + 3R + 3R + R = (2w + 7)R$, which is only a slight decrease. However, we expect that it will be mitigated by a more expensive FFT.

3.5 Possible improvement

The Poseidon paper describes another improvement by showing that the inputs and outputs of S-boxes in $2w$ consecutive partial rounds are linked by polynomial equations of degree 5. We can define $2w$ polynomials of degree $R_P/(2w)$ that satisfy these equations, so that a proof about the partial rounds only would involve an identity of degree $5R_P/(2w)$, and the prover costs would be as low as $\mathbf{e} \approx R_P/2$. However, the full rounds would probably add a significant overhead to this number.