PLONK: Permutations over Lagrange-Bases for Oecumenical Noninteractive arguments of Knowledge

Ariel Gabizon   Zachary J. Williamson   Oana Ciobotaru

Protocol Labs   Aztec Protocol

Prelude: Trusted setups for pairing-based SNARKs

- Want to prove statements about circuit satisfiability
- Generate CRS of elements $\mathbf{g}^{\mathbf{P}(s)}$ for secret $s \in \mathbb{F}$ nobody knows, for some polynomials $\mathbf{P}$ (potentially depending on circuit).

Prelude: Trusted setups for pairing-based SNARKs

- Want to prove statements about circuit satisfiability
- Generate CRS of elements $\mathbf{g}^{\mathbf{P}(s)}$ for secret $s \in \mathbb{F}$ nobody knows, for some polynomials $\mathbf{P}$ (potentially depending on circuit).
- If CRS only contains elements $\mathbf{g}^{s^i}$ setup is **universal and updatable**.

Plonk in two sips

1. All you need is a permutation check.
2. Permutations are easier to check on mutliplicative subgroups

Part 1: All you need is a permutation check

Our setting: want short proofs about fan-in 2 unlimited fan-out circuits, trusted setup is updatable depends only on circuit size.

example: Prove knowledge of $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$ with

$$(\mathbf{a} + \mathbf{b}) \cdot \mathbf{c} = 7$$

Left values: $\mathbf{l}_1, \mathbf{l}_2$
Right values: $\mathbf{r}_1, \mathbf{r}_2$
Output values: $\mathbf{o}_1, \mathbf{o}_2$

Left values: $\mathbf{l}_1, \mathbf{l}_2$
Right values: $\mathbf{r}_1, \mathbf{r}_2$
Output values: $\mathbf{o}_1, \mathbf{o}_2$

Gate checks: $\mathbf{l}_1 + \mathbf{r}_1 = \mathbf{o}_1, \mathbf{l}_2 \cdot \mathbf{r}_2 = \mathbf{o}_2$
Wire/copy checks: $\mathbf{o}_1 = \mathbf{l}_2$
Public input checks: $\mathbf{o}_2 = 7$.

Left values: $\mathbf{l}_1, \mathbf{l}_2$
Right values: $\mathbf{r}_1, \mathbf{r}_2$
Output values: $\mathbf{o}_1, \mathbf{o}_2$

Gate checks: $\mathbf{l}_1 + \mathbf{r}_1 = \mathbf{o}_1, \mathbf{l}_2 \cdot \mathbf{r}_2 = \mathbf{o}_2$ **(easy)**
Wire/copy checks: $\mathbf{o}_1 = \mathbf{l}_2$ **(hard)**
Public input checks: $\mathbf{o}_2 = 7$ **(easy)**

Copy checks with permutations

similar to [Groth09,BCGGHJ17]

$$\mathbf{V} = (\mathbf{l}_1, \mathbf{l}_2, \mathbf{r}_1, \mathbf{r}_2, \mathbf{o}_1, \mathbf{o}_2)$$

Copy checks with permutations

similar to [Groth09,BCGGHJ17]

$$\mathbf{V} = (\mathbf{l}_1, \mathbf{l}_2, \mathbf{r}_1, \mathbf{r}_2, \mathbf{o}_1, \mathbf{o}_2)$$

$\mathbf{o}_1 = \mathbf{l}_2$ iff $\mathbf{V} = \boldsymbol{\sigma}(\mathbf{V})$
For permutation $\boldsymbol{\sigma} = (25)$

Part 2: Permutations are easier to check on mutliplicative subgroups

[Bayer-Groth12] - perm checks with products

example: Given $\mathbf{a}, \mathbf{b} \in \mathbb{F}^3$, want to check
$(\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3) = (\mathbf{a}_3, \mathbf{a}_1, \mathbf{a}_2)$

[Bayer-Groth12] - perm checks with products

example: Given $\mathbf{a}, \mathbf{b} \in \mathbb{F}^3$, want to check $(\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3) = (\mathbf{a}_3, \mathbf{a}_1, \mathbf{a}_2)$

step 1: Choose random $\boldsymbol{\beta} \in \mathbb{F}$. Let

$$\mathbf{a}'_1 = \mathbf{a}_1 + \boldsymbol{\beta}, \mathbf{a}'_2 = \mathbf{a}_2 + 2\boldsymbol{\beta}, \mathbf{a}'_3 = \mathbf{a}_3 + 3\boldsymbol{\beta}$$

$$\mathbf{b}'_1 = \mathbf{b}_1 + 3\boldsymbol{\beta}, \mathbf{b}'_2 = \mathbf{b}_2 + \boldsymbol{\beta}, \mathbf{b}'_3 = \mathbf{b}_3 + 2\boldsymbol{\beta}$$

[Bayer-Groth12] - perm checks with products

example: Given $\mathbf{a}, \mathbf{b} \in \mathbb{F}^3$, want to check $(\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3) = (\mathbf{a}_3, \mathbf{a}_1, \mathbf{a}_2)$

step 1: Choose random $\boldsymbol{\beta} \in \mathbb{F}$. Let

$$\mathbf{a}'_1 = \mathbf{a}_1 + \boldsymbol{\beta}, \mathbf{a}'_2 = \mathbf{a}_2 + 2\boldsymbol{\beta}, \mathbf{a}'_3 = \mathbf{a}_3 + 3\boldsymbol{\beta}$$

$$\mathbf{b}'_1 = \mathbf{b}_1 + 3\boldsymbol{\beta}, \mathbf{b}'_2 = \mathbf{b}_2 + \boldsymbol{\beta}, \mathbf{b}'_3 = \mathbf{b}_3 + 2\boldsymbol{\beta}$$

If claim false - w.h.p as mutliset $\{\mathbf{a}'_1, \mathbf{a}'_2, \mathbf{a}'_3\} \neq \{\mathbf{b}'_1, \mathbf{b}'_2, \mathbf{b}'_3\}$:

[Bayer-Groth12] - reducing permutation checks to products

step 2: Choose random $\gamma \in \mathbb{F}$. Let

$$a_i'' = a_i' + \gamma, b_i'' = b_i + \gamma$$

[Bayer-Groth12] - reducing permutation checks to products

step 2: Choose random $\gamma \in \mathbb{F}$. Let

$$a''_i = a'_i + \gamma, b''_i = b'_i + \gamma$$

If $\{a'_1, a'_2, a'_3\} \neq \{b'_1, b'_2, b'_3\}$ as multiset - w.h.p

$$a''_1 \cdot a''_2 \cdot a''_3 \neq b''_1 \cdot b''_2 \cdot b''_3.$$

Idealized Polynomials Protocols

Preprocessing: $\mathcal{V}$ chooses polynomials $\mathbf{g}_1, \ldots, \mathbf{g}_\mathbf{t} \in \mathbb{F}_{<\mathbf{d}}[\mathbf{X}]$.

Protocol:

1. $\mathcal{P}$'s msgs are to ideal party $\mathbf{I}$. Must be $\mathbf{f}_\mathbf{i} \in \mathbb{F}_{<\mathbf{d}}[\mathbf{X}]$.
2. At protocol end $\mathcal{V}$ asks $\mathbf{I}$ if some identities hold between $\{\mathbf{f}_1, \ldots, \mathbf{f}_\ell, \mathbf{g}_1, \ldots, \mathbf{g}_\mathbf{t}\}$. Outputs $\mathbf{acc}$ iff they do.

Idealized Polynomials Protocols

Preprocessing: $\mathcal{V}$ chooses polynomials $\mathbf{g}_1, \ldots, \mathbf{g}_\mathbf{t} \in \mathbb{F}_{<\mathbf{d}}[\mathbf{X}]$.

Protocol:

1. $\mathcal{P}$'s msgs are to ideal party $\mathbf{I}$. Must be $\mathbf{f}_\mathbf{i} \in \mathbb{F}_{<\mathbf{d}}[\mathbf{X}]$.
2. At end, $\mathcal{V}$ asks $\mathbf{I}$ if some identities hold between $\{\mathbf{f}_1, \ldots, \mathbf{f}_\ell, \mathbf{g}_1, \ldots, \mathbf{g}_\mathbf{t}\}$.

Using [KZG10], can compile to real protocol with each msg of $\mathcal{P}$ being 32-64 bytes according to your NFSPL.

$\mathbb{H}$-ranged Polynomials Protocols

Preprocessing: $\mathcal{V}$ chooses polynomials $\mathbf{g}_1, \ldots, \mathbf{g}_t \in \mathbb{F}_{<\mathbf{d}}[\mathbf{X}]$, $\mathbf{H} \subset \mathbb{F}$.

Protocol:

1. $\mathcal{P}$'s msgs are to ideal party $\mathbf{I}$. Must be $\mathbf{f}_\mathbf{i} \in \mathbb{F}_{<\mathbf{d}}[\mathbf{X}]$.
2. At end, $\mathcal{V}$ asks $\mathbf{I}$ if some identities hold between $\{\mathbf{f}_1, \ldots, \mathbf{f}_\ell, \mathbf{g}_1, \ldots, \mathbf{g}_\mathbf{t}\}$ **on** $\mathbf{H}$.

$\mathbb{H}$-ranged protocol using polynomial protocol:

$\mathcal{V}$ wants to check identities P_1, P_2 on H.

- After $\mathcal{P}$ finished sending $\{f_i\}$, $\mathcal{V}$ sends random $a_1, a_2 \in \mathbb{F}$.
- $\mathcal{P}$ sends $T \in \mathbb{F}_{<d}[X]$.
- $\mathcal{V}$ checks identity $a_1 \cdot P_1 + a_2 \cdot P_2 \equiv T \cdot Z_H$.

Checking permutations with $\mathbb{H}$-ranged protocols

Permutation $\sigma : [n] \to [n]$. $H = \{\alpha, \alpha^2, \ldots, \alpha^n\}$.

$\mathcal{P}$ has sent $f \in \mathbb{F}_{<d}[X]$.

Wants to prove $f = \sigma(f)$:

$$\forall i \in [n], f(\alpha^i) = f(\alpha^{\sigma(i)})$$

Using [BG12] reduces to:

$H = \{\alpha, \alpha^2, \ldots, \alpha^n\}$.

$\mathcal{P}$ has sent $f, g \in \mathbb{F}_{<d}[X]$.

Wants to prove:

$$\prod_{i \in [n]} f(\alpha^i) = \prod_{i \in [n]} g(\alpha^i)$$

Checking products with $\mathbf{H}$-ranged protocols

1. $\mathcal{P}$ computes Z with $Z(\alpha) = 1, Z(\alpha^i) = \prod_{j<i} f(\alpha^j)/g(\alpha^j)$, $i = 2..n+1$.
2. Sends Z to $\mathbf{I}$.

Checking products with $\mathbb{H}$-ranged protocols

1. $\mathcal{P}$ computes Z with
   $Z(\alpha) = 1, Z(\alpha^i) = \prod_{j<i} f(\alpha^j)/g(\alpha^j)$.
2. Sends Z to $\mathbf{I}$.
3. $\mathcal{V}$ checks following identities on $\mathbb{H}$.
   3.1 $L_1(X)(Z(X) - 1) = 0$
   3.2 $Z(X)f(X) = Z(\alpha \cdot X)g(X)$
   3.3 $L_n(X)(Z(\alpha \cdot X) - 1) = 0$

The bottom line (on BLS-381 curve)

600 byte proofs with one trusted setup for all fan-in two circuits of $\mathbf{n}$ gates.

Prover does $11\mathbf{n}$ $\mathbf{G}_1$ exp (or $9\mathbf{n}$ $\mathbf{G}_1$ exp with 700 byte proof).

For batch of proofs on same circuit only $3\mathbf{n}$ $\mathbf{G}_1$ exp and 240 bytes for each additional proof.

Bonus material: The KZG polynomial commitment scheme

SRS: $[1]$,$[x]$,..., $\left[x^{d}\right]$, for random $x \in \mathbb{F}$.

$f(X) = \sum_{i=0}^{d} a_i X^i$

$\mathrm{cm}(f) := \sum_{i=0}^{d} a_i \left[x^i\right] = [f(x)]$

SRS: $[1]$,$[x]$,$\ldots$, $\left[x^d\right]$,
for random $x \in \mathbb{F}$.

$\mathrm{cm}(f) := [f(x)]$

$\mathrm{open}(f, i) := [h(x)]$, where $h(X) := \frac{f(X)-f(i)}{X-i}$

$\mathsf{cm}(\mathbf{f}) := [\mathbf{f}(x)]$

$\mathsf{open}(\mathbf{f}, \mathbf{i}) := [\mathbf{h}(x)]$, where $\mathbf{h}(\mathbf{X}) := \frac{\mathbf{f}(\mathbf{X}) - \mathbf{f}(\mathbf{i})}{\mathbf{X} - \mathbf{i}}$

$\mathsf{verify}(\mathsf{cm}, \boldsymbol{\pi}, z, \mathbf{i}) :$

$$e(\mathsf{cm} - [z], [1]) \stackrel{?}{=} e(\boldsymbol{\pi}, [x - \mathbf{i}])$$

$\mathsf{cm}(\mathbf{f}) := [\mathbf{f}(x)]$

$\mathsf{open}(\mathbf{f}, \mathbf{i}) := [\mathbf{h}(x)]$, where $\mathbf{h}(\mathbf{X}) := \frac{\mathbf{f}(\mathbf{X}) - \mathbf{f}(\mathbf{i})}{\mathbf{X} - \mathbf{i}}$

$\mathsf{verify}(\mathsf{cm}, \boldsymbol{\pi}, z, \mathbf{i})$:

$$e(\mathsf{cm} - [z], [1]) \stackrel{?}{=} e(\boldsymbol{\pi}, [x - \mathbf{i}])$$

Thm[KZG,MBKM]: *This works in the Algebraic Group Model.*