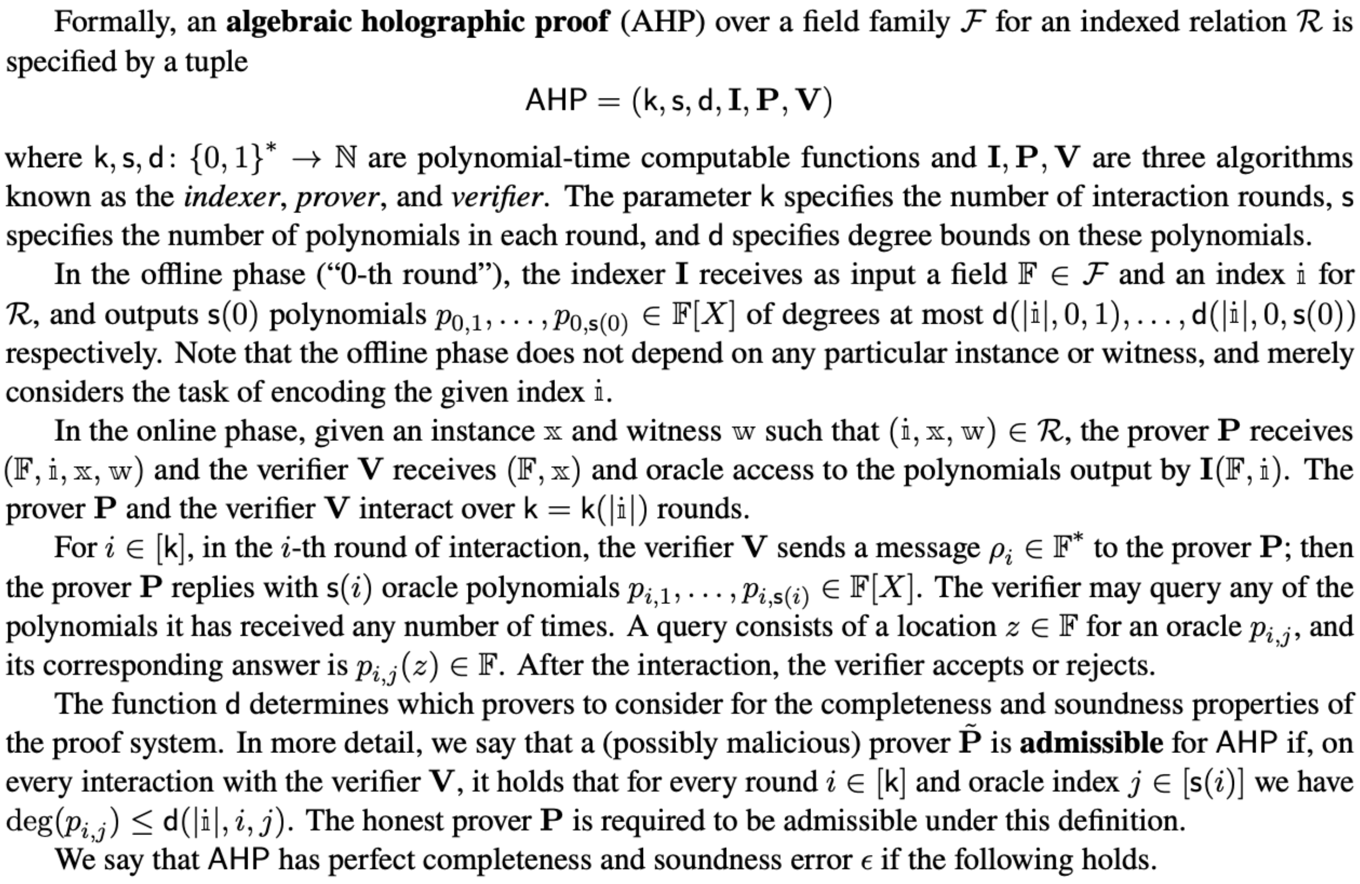
Part III The technical architecture of the Aleo blockchain (AHP)

AHP

AHP (Algebraic Holographic Proof) is essentially evolved from IOP (Interactive Oracle Proof). The distinction between AHP and IOP lies in the division of the verifier's verification process into two phases: offline and online. The offline algorithm is known as the indexer algorithm, which can be understood as involving multiple rounds of interaction between the prover and the verifier. Additionally, the verifier can access the indexer oracle.



Formally, an **algebraic holographic proof** (AHP) over a field family $\mathcal{F}$ for an indexed relation $\mathcal{R}$ is specified by a tuple

$$\mathsf{AHP} = (\mathsf{k}, \mathsf{s}, \mathsf{d}, \mathbf{I}, \mathbf{P}, \mathbf{V})$$

where $\mathsf{k}, \mathsf{s}, \mathsf{d} \colon \{0,1\}^* \to \mathbb{N}$ are polynomial-time computable functions and $\mathbf{I}, \mathbf{P}, \mathbf{V}$ are three algorithms known as the *indexer*, *prover*, and *verifier*. The parameter k specifies the number of interaction rounds, s specifies the number of polynomials in each round, and d specifies degree bounds on these polynomials.

In the offline phase ("0-th round"), the indexer $\mathbf{I}$ receives as input a field $\mathbb{F} \in \mathcal{F}$ and an index $\mathbb{i}$ for $\mathcal{R}$, and outputs $\mathsf{s}(0)$ polynomials $p_{0,1}, \ldots, p_{0,\mathsf{s}(0)} \in \mathbb{F}[X]$ of degrees at most $\mathsf{d}(|\mathbb{i}|, 0, 1), \ldots, \mathsf{d}(|\mathbb{i}|, 0, \mathsf{s}(0))$ respectively. Note that the offline phase does not depend on any particular instance or witness, and merely considers the task of encoding the given index $\mathbb{i}$.

In the online phase, given an instance $\mathbb{x}$ and witness $\mathbb{w}$ such that $(\mathbb{i}, \mathbb{x}, \mathbb{w}) \in \mathcal{R}$, the prover $\mathbf{P}$ receives $(\mathbb{F}, \mathbb{i}, \mathbb{x}, \mathbb{w})$ and the verifier $\mathbf{V}$ receives $(\mathbb{F}, \mathbb{x})$ and oracle access to the polynomials output by $\mathbf{I}(\mathbb{F}, \mathbb{i})$. The prover $\mathbf{P}$ and the verifier $\mathbf{V}$ interact over $\mathsf{k} = \mathsf{k}(|\mathbb{i}|)$ rounds.

For $i \in [\mathsf{k}]$, in the i-th round of interaction, the verifier $\mathbf{V}$ sends a message $\rho_i \in \mathbb{F}^*$ to the prover $\mathbf{P}$; then the prover $\mathbf{P}$ replies with $\mathsf{s}(i)$ oracle polynomials $p_{i,1}, \ldots, p_{i,\mathsf{s}(i)} \in \mathbb{F}[X]$. The verifier may query any of the polynomials it has received any number of times. A query consists of a location $z \in \mathbb{F}$ for an oracle $p_{i,j}$, and its corresponding answer is $p_{i,j}(z) \in \mathbb{F}$. After the interaction, the verifier accepts or rejects.

The function d determines which provers to consider for the completeness and soundness properties of the proof system. In more detail, we say that a (possibly malicious) prover $\tilde{\mathbf{P}}$ is **admissible** for AHP if, on every interaction with the verifier $\mathbf{V}$, it holds that for every round $i \in [\mathsf{k}]$ and oracle index $j \in [\mathsf{s}(i)]$ we have $\deg(p_{i,j}) \leq \mathsf{d}(|\mathbb{i}|, i, j)$. The honest prover $\mathbf{P}$ is required to be admissible under this definition.

We say that AHP has perfect completeness and soundness error ϵ if the following holds.

1. R1CS

R1CS primarily involves instance-witness pairs $((A,B,C),(x,w))$, where A,B,C are matrices, and $(x,w) \in \mathbb{F}$ satisfy $(Az) \circ (Bz) = cz; z = (1,x,w)$. For a detailed explanation of R1CS, please refer to this example. We will not delve into further details here. If we use Lagrange interpolation to construct three univariate polynomials, $\hat{z}_A(X), \hat{z}_B(X), \hat{z}_C(X)$, on a subgroup H from the three sets of vectors Az, Bz, Cz, then R1CS needs to prove the following:

- entry-wise product： $\forall \kappa \in H, \hat{z}_A(\kappa)\hat{z}_B(\kappa) - \hat{z}_C(\kappa) = 0$
- linear relation： $\forall M \in \{A, B, C\}, \forall \kappa \in H, \hat{z}_M(\kappa) = \sum_{i \in H} M[\kappa, i]\hat{z}(i)$, meaning it needs to be proven that Az, Bz, Cz are indeed derived from the same linear combination z of matrices A, B, C.

The entry-wise product can be easily proven using the aforementioned zeroTest, while the linear relation requires the use of the sumCheck protocol for proof.

2. Lemma

Lemma 1 (Univariate Sumcheck for Subgroups): Given a multiplicative subgroup $S \subset \mathbb{F}$, for a polynomial $f(X)$, the sum $\sum_{\kappa \in S} f(\kappa) = \sigma$. If and only if $f(X)$ can be represented as $f(X) = h(X) \cdot v_S(X) + X \cdot g(X) + \sigma/|S|$, where $v_S(X)$ is the vanish polynomial over subgroup S, and $|S|$ denotes the number of elements in the subgroup S. This lemma is derived from the paper Aurora: Transparent Succinct Arguments for R1CS, and we will not delve into a detailed explanation of this lemma here.

3. AHP for R1CS

3.1. Offline: Index Algorithm

Due to the verification process of zk-SNARKs typically requiring "reading the description of the computation, in order to know what statement is being verified," and the large computational load involved, which means the verification time is proportional to the computational effort, Marlin's approach splits the verification process into two phases:

- Offline phase: Produces a short summary for the given circuit, consisting of coefficient matrices (index).
- Online phase: Uses this short summary to verify the proof, called instance.

The offline algorithm in Marlin is known as the indexer algorithm, which encodes the coefficient matrices.

The indexer $I(\mathbb{F}; (H, K) \subset \mathbb{F}; (A, B, C) \in \mathbb{F}^{H \times H})$, $|K| \geq max\{||A||, ||B||, ||C||\} \rightarrow \{\hat{row}_M(X), \hat{col}_M(X), \hat{val}_M(X)\}_{M \in \{A,B,C\}}$, outputs nine univariate polynomials.

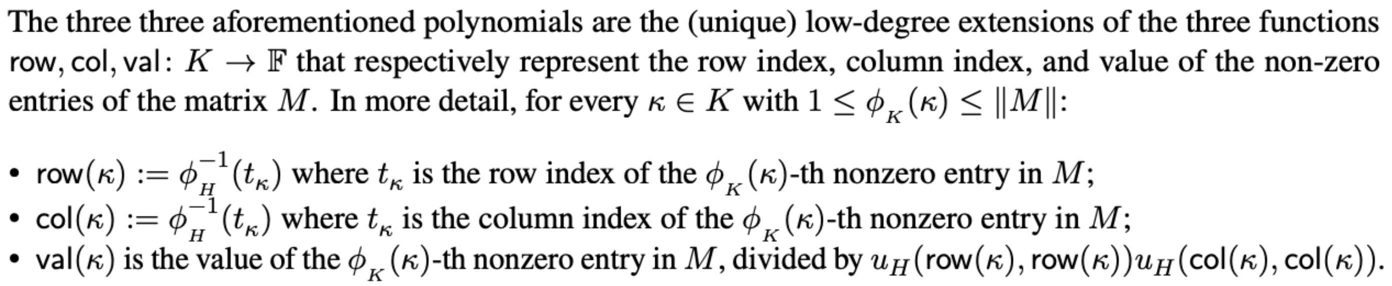
Based on the non-zero elements of matrices A, B, C, these non-zero elements are mapped into three vectors: row, col, val, and then polynomialized on subgroup H using Lagrange interpolation. These nine univariate polynomials have degrees less than | $|K|$ and ensure that the bivariate polynomial $\hat{M}(X,Y)$ is a low-degree extension of M.

$$\hat{M}(X,Y) = \sum_{\kappa \in K} \frac{v_H(X)}{(X - \hat{\mathsf{row}}(\kappa))} \cdot \frac{v_H(Y)}{(Y - \hat{\mathsf{col}}(\kappa))} \cdot \hat{\mathsf{val}}(\kappa) \ .$$

Matrix M corresponds to the row, col, and val matrices of all non-zero elements in matrices A, B, C. For example:

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 5 & 0 \end{bmatrix} B = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} C = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$row_{A,B,C} = \begin{bmatrix} 0 & 1 & 2 & 2 & 3 & 3 \\ 0 & 1 & 2 & 3 & 0 & 0 \\ 0 & 1 & 2 & 3 & 0 & 0 \end{bmatrix} col_{A,B,C} = \begin{bmatrix} 0 & 1 & 2 & 0 & 3 & 4 \\ 0 & 0 & 4 & 4 & 0 & 0 \\ 1 & 2 & 3 & 5 & 0 & 0 \end{bmatrix} val_{A,B,C} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 5 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$



The three three aforementioned polynomials are the (unique) low-degree extensions of the three functions $\mathsf{row}, \mathsf{col}, \mathsf{val} \colon K \to \mathbb{F}$ that respectively represent the row index, column index, and value of the non-zero entries of the matrix M. In more detail, for every $\kappa \in K$ with $1 \leq \phi_K(\kappa) \leq \|M\|$:

- $\mathsf{row}(\kappa) := \phi_H^{-1}(t_\kappa)$ where t_κ is the row index of the $\phi_K(\kappa)$-th nonzero entry in M;
- $\mathsf{col}(\kappa) := \phi_H^{-1}(t_\kappa)$ where t_κ is the column index of the $\phi_K(\kappa)$-th nonzero entry in M;
- $\mathsf{val}(\kappa)$ is the value of the $\phi_K(\kappa)$-th nonzero entry in M, divided by $u_H(\mathsf{row}(\kappa), \mathsf{row}(\kappa)) u_H(\mathsf{col}(\kappa), \mathsf{col}(\kappa))$.

Based on the diagram, let's briefly introduce the calculation process for $row(\kappa)$: Essentially, it involves converting high-degree polynomials over the group K into more low-degree polynomials over the group H through mapping. This means calculating nine low-degree polynomials for $row_{A,B,C}, col_{A,B,C}, val_{A,B,C}$ on H.

- Assume the subgroup $H = \{h_1, h_2, \ldots, h_n\}$ has an order $ord(H) = |H| = n$, which is related to the constraints and the number of instances and witnesses. In the given example, $n = 6$ corresponds to the number of columns in row, col, val, but for ease of FFT transformations, $n = 2^3 = 8$.
- The subgroup $K = \{k_1, k_2, \ldots, k_m\}$ has an order $ord(K) = |K| = m$, which relates to the number of non-zero entries in the matrix M. In the example above, the total number of non-zero entries in matrices A, B and C is 14, but for FFT convenience, $m = 2^4 = 16$.

- $row(\kappa)$: Let $\kappa = k_j$, then $\phi_K(\kappa) = j$, and t_κ is the row index of the j th non-zero entry in matrix M, assumed to be i , hence $row(\kappa) = \phi_H^{-1}(i) = h_i$. Using Lagrange interpolation based on $(x = \kappa = k_j, y = row(\kappa) = h_i)$, the polynomial $ro\hat{w}_M(X)$ can be derived.

$$row_{A,B,C} = \begin{bmatrix} 0_{h\_0} & 1_{h\_1} & 2_{h\_2} & 2_{h\_2} & 3_{h\_3} & 3_{h\_3} \\ 0_{h\_0} & 1_{h\_1} & 2_{h\_2} & 3_{h\_3} & 0_{h\_0} & 0_{h\_0} \\ 0_{h\_0} & 1_{h\_1} & 2_{h\_2} & 3_{h\_3} & 0_{h\_0} & 0_{h\_0} \end{bmatrix} col_{A,B,C} = \begin{bmatrix} 0 & 1 & 2 & 0 & 3 & 4 \\ 0 & 0 & 4 & 4 & 0 & 0 \\ 1 & 2 & 3 & 5 & 0 & 0 \end{bmatrix} val_{A,B,C} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 5 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$

3.2. Online: Proving and Verifying Algorithms

Let $pp = [\mathbb{F}; (H, K) \subset \mathbb{F}; (A, B, C) \in \mathbb{F}^{H \times H})$, with $|K| \geq max\{||A||, ||B||, ||C||\}$.

Prover(pp, x, w **):** The prover's inputs are an instance $x \in \mathbb{F}^{H[\leq |x|]}$ and a witness $w \in \mathbb{F}^{H[\geq |x|]}$.

Verifier(pp, x **, indexer)**: The verifier's inputs are an instance $x \in \mathbb{F}^{H[\leq |x|]}$ and access to the indexer oracle.

(1) Round 1 - Prover

- Assume the multiplicative subgroup $H = \{h_1, h_2, \ldots, h_n\}$, define the instance polynomial $\hat{x}(X), x \in H[\leq |X|] = \{h_1, h_1, \ldots, h_{|x|}\}$.
- Define the shifted witness polynomial $\hat{w}(X)$ such that for $X \in H[\geq |X|] = \{h_{|x|+1}, \ldots, h_n\}$, its corresponding value is $\dfrac{w(\gamma) - \hat{x}(\gamma)}{v_{H[\leq |x|]}(\gamma)}, \gamma \in H[\geq |X|]$. This construction is utilized because $z = (x, w)$.
- Let $z = (x; w) \in \mathbb{F}^H$, construct $\hat{z}_A(X), \hat{z}_B(X), \hat{z}_C(X) \in \mathbb{F}^{<|H|+b}[X]$ based on the linear combination $z_A = Az, z_B = Bz, z_C = Cz$ on subgroup H.
- ZeroTest: Calculate the polynomial $h_0(X) s.t. \hat{z}_A(X) \cdot \hat{z}_B(X) - \hat{z}_C(X) = h_0(X) \cdot v_H(X)$.
- Note: $\hat{z}(X) = \hat{w}(X) v_{H[\leq |x|]}(X) + \hat{x}(X)$ can also be directly constructed based on $z = (x; w)$ in group H.
- Construct a random polynomial $s(X) \in \mathbb{F}^{<2|H|+b-1}[X]$ and $\sum_{\kappa \in H} s(\kappa) = \sigma_1$, also known as the mask polynomial, to satisfy the zero-knowledge property of the univariate sumcheck.
- The prover sends $\hat{w}(X), \hat{z}_A(X), \hat{z}_B(X), \hat{z}_C(X), h_0(X), s(X), \sigma_1$.

$z := (x, w) \quad z_A := Az \quad z_B := Bz \quad z_C := Cz$
sample $\hat{w}(X) \in \mathbb{F}^{<|w|+\mathsf{b}}[X]$ and $\hat{z}_A(X), \hat{z}_B(X), \hat{z}_C(X) \in \mathbb{F}^{<|H|+\mathsf{b}}[X]$
find $h_0(X)$ s.t. $\hat{z}_A(X)\hat{z}_B(X) - \hat{z}_C(X) = h_0(X) v_H(X)$
sample $s(X) \in \mathbb{F}^{<2|H|+\mathsf{b}-1}[X]$ and compute sum $\sigma_1 := \sum_{\kappa \in H} s(\kappa)$

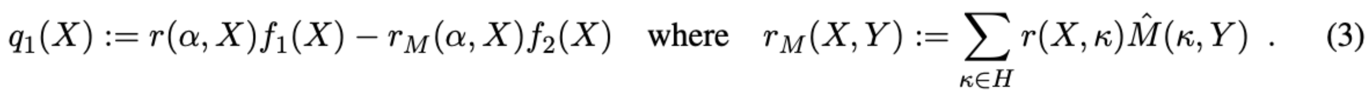
$$\xrightarrow[\quad h_0 \in \mathbb{F}^{<|H|+2\mathsf{b}-1}[X],\, s \in \mathbb{F}^{<2|H|+\mathsf{b}-1}[X] \quad]{\quad \sigma_1 \in \mathbb{F}, \hat{w} \in \mathbb{F}^{<|w|+\mathsf{b}}[X], \hat{z}_A, \hat{z}_B, \hat{z}_C \in \mathbb{F}^{<|H|+\mathsf{b}}[X], \quad}$$

$\alpha, \eta_A, \eta_B, \eta_C \leftarrow \mathbb{F}$

(2) Round 1 - Verifier

Randomly sends $\alpha, \eta_A, \eta_B, \eta_C \in \mathbb{F}$, where α is to reduce the linear check problem to a sumcheck problem, and η_A, η_B, η_C is to bundle three sumcheck problems into one.

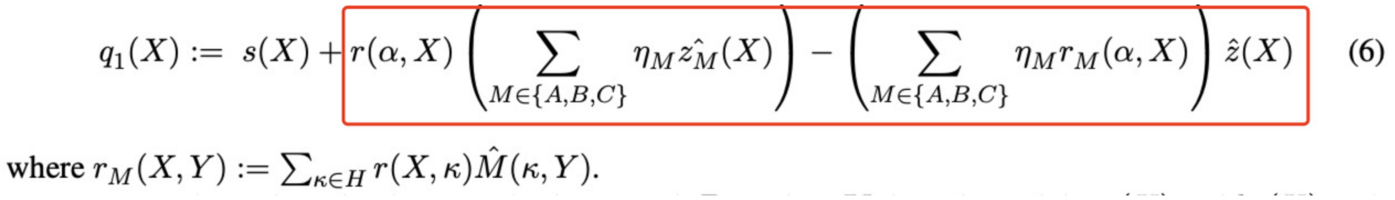
(3)Round2-Prover

> *> reduce lincheck problem to a sumcheck problem: the verifier samples a random element $\alpha \in \mathbb{F}$ and sends it to Prover. Indeed, letting $r(X,Y) = u_H(X,Y)$.*
>
> *> Prover is left to convince Verifier that the following univariate polynomial sums to 0 on H.*
>
> 
>
> $$q_1(X) := r(\alpha, X) f_1(X) - r_M(\alpha, X) f_2(X) \quad \text{where} \quad r_M(X,Y) := \sum_{\kappa \in H} r(X,\kappa)\hat{M}(\kappa, Y) \ . \qquad (3)$$

Following the provided reference, if it can be proven that the sum of polynomial $q_1(X)$ over H equals σ_1, then it demonstrates a linear relation between $f_1(X)$ and $f_2(X)$.

The polynomial $q_1(x) = s(X) + r(\alpha, X) f_1(X) - r_M(\alpha, X) f_2(X)$ where
$f_1(X) = \eta_A \cdot \hat{z}_A(X) + \eta_B \cdot \hat{z}_B(X) + \eta_C \cdot \hat{z}_C(X)$ $f_2(X) = \hat{z}(X)$

Next, the prover needs to demonstrate to the verifier the following polynomial $\sum_{\kappa \in H} q_1(\kappa) = \sigma_1$, indicating that the value within the red box is zero, which corresponds to the linear relation that needs to be proven.



$$q_1(X) := s(X) + \boxed{r(\alpha, X)\left(\sum_{M \in \{A,B,C\}} \eta_M \hat{z_M}(X)\right) - \left(\sum_{M \in \{A,B,C\}} \eta_M r_M(\alpha, X)\right)\hat{z}(X)} \qquad (6)$$

where $r_M(X,Y) := \sum_{\kappa \in H} r(X,\kappa)\hat{M}(\kappa, Y)$.

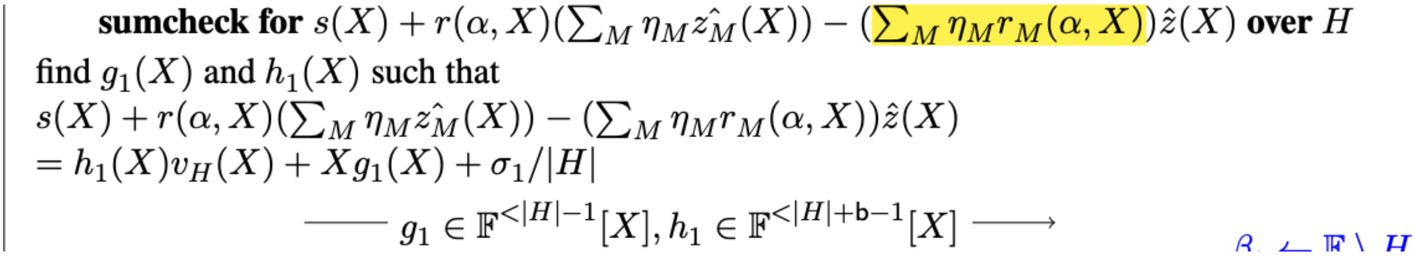
$$r_M(\alpha, X) = \sum_{\kappa \in H} r(\alpha, \kappa)\hat{M}(\kappa, X)$$

$$q_1(X) = s(X) + \frac{v_H(\alpha) - v_H(X)}{\alpha - X} \cdot (\eta_A \cdot \hat{z}_A(X) + \eta_B \cdot \hat{z}_B(X) + \eta_C \cdot \hat{z}_C(X)) - \{\sum_{\kappa \in H} [\eta_A \cdot r(\alpha, \kappa) \cdot \hat{A}(\kappa, X) + \eta_B \cdot r(\alpha, \kappa) \cdot \hat{B}(\kappa, X) + \eta_C \cdot r(\alpha, \kappa) \cdot \hat{C}(\kappa, X)]\} \cdot \hat{z}(X)$$

Note:

- The bivariate polynomial $r(X,Y) = u_H(X,Y) = \frac{v_H(X) - v_H(Y)}{X - Y}$, where $v_H(X)$ is the vanishing polynomial on H.
    - If H is a multiplicative subgroup, then $u_H(X,Y) = \frac{v_H(X) - v_H(Y)}{X - Y} = \frac{X^{|H|} - Y^{|H|}}{X - Y}$; $u_H(X,X) = |H|X^{|H|-1} = nX^{n-1}$.

Next, the prover needs to prove to the verifier the following polynomial $\sum_{\kappa \in H} q_1(\kappa) = \sigma_1$, in accordance with the lemma mentioned in section 5.2.



$$\textbf{sumcheck for } s(X) + r(\alpha, X)(\textstyle\sum_M \eta_M \hat{z_M}(X)) - (\textstyle\sum_M \eta_M r_M(\alpha, X))\hat{z}(X) \textbf{ over } H$$

find $g_1(X)$ and $h_1(X)$ such that

$$s(X) + r(\alpha, X)(\textstyle\sum_M \eta_M \hat{z_M}(X)) - (\textstyle\sum_M \eta_M r_M(\alpha, X))\hat{z}(X)$$
$$= h_1(X) v_H(X) + X g_1(X) + \sigma_1/|H|$$

$$\xrightarrow{\qquad} g_1 \in \mathbb{F}^{<|H|-1}[X], h_1 \in \mathbb{F}^{<|H|+\mathsf{b}-1}[X] \xrightarrow{\qquad}$$

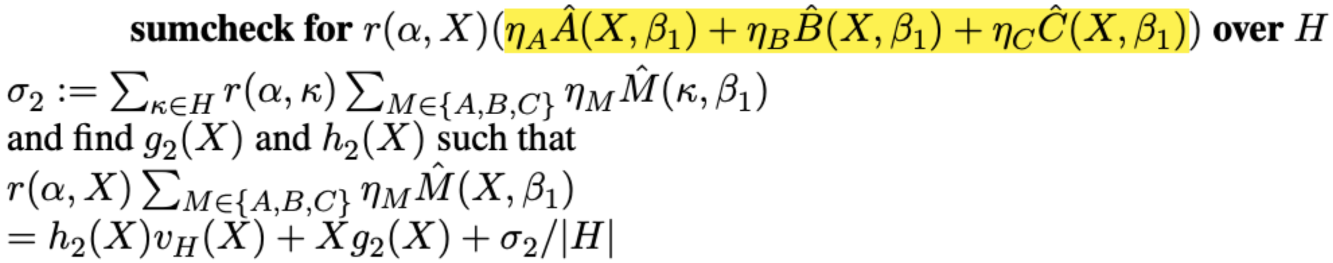
$\beta_1 \leftarrow \mathbb{F} \setminus H$

(4) Round 2 - Verifier

Randomly selects $\beta_1 \in \mathbb{F} \setminus H$.

(5) Round 3 - Prover: Sumcheck

$$\{\sum_{\kappa \in H} [\eta_A \cdot r(\alpha, \kappa) \cdot \hat{A}(\kappa, X) + \eta_B \cdot r(\alpha, \kappa) \cdot \hat{B}(\kappa, X) + \eta_C \cdot r(\alpha, \kappa) \cdot \hat{C}(\kappa, X)]\}$$

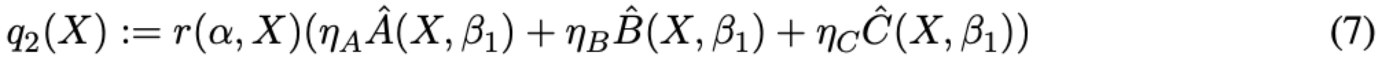


$$\textbf{sumcheck for } r(\alpha, X)(\eta_A \hat{A}(X, \beta_1) + \eta_B \hat{B}(X, \beta_1) + \eta_C \hat{C}(X, \beta_1)) \textbf{ over } H$$

$\sigma_2 := \sum_{\kappa \in H} r(\alpha, \kappa) \sum_{M \in \{A,B,C\}} \eta_M \hat{M}(\kappa, \beta_1)$

and find $g_2(X)$ and $h_2(X)$ such that

$$r(\alpha, X) \textstyle\sum_{M \in \{A,B,C\}} \eta_M \hat{M}(X, \beta_1)$$
$$= h_2(X) v_H(X) + X g_2(X) + \sigma_2/|H|$$



$$q_2(X) := r(\alpha, X)(\eta_A \hat{A}(X, \beta_1) + \eta_B \hat{B}(X, \beta_1) + \eta_C \hat{C}(X, \beta_1)) \tag{7}$$

$\sigma_2 = \sum_{\kappa \in H} q_2(\kappa)$ requires finding polynomials $h_2(X), g_2(X)$.

(6) Round 3 - Verifier

Randomly selects $\beta_2 \in \mathbb{F} \setminus H$.

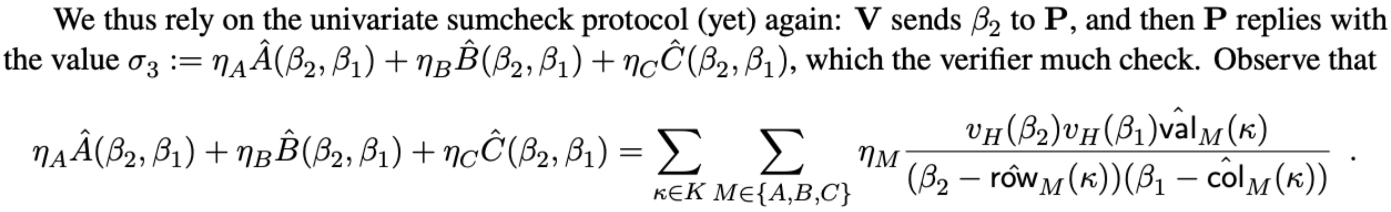
(7) Round 4 - Prover: Sumcheck

Using the calculation formula for $\hat{M}(X, Y)$:

- $f_3(X) = X g_3(X) + \sigma_3/|K|$, this equation proves that f_3 sums to σ_3 over K.

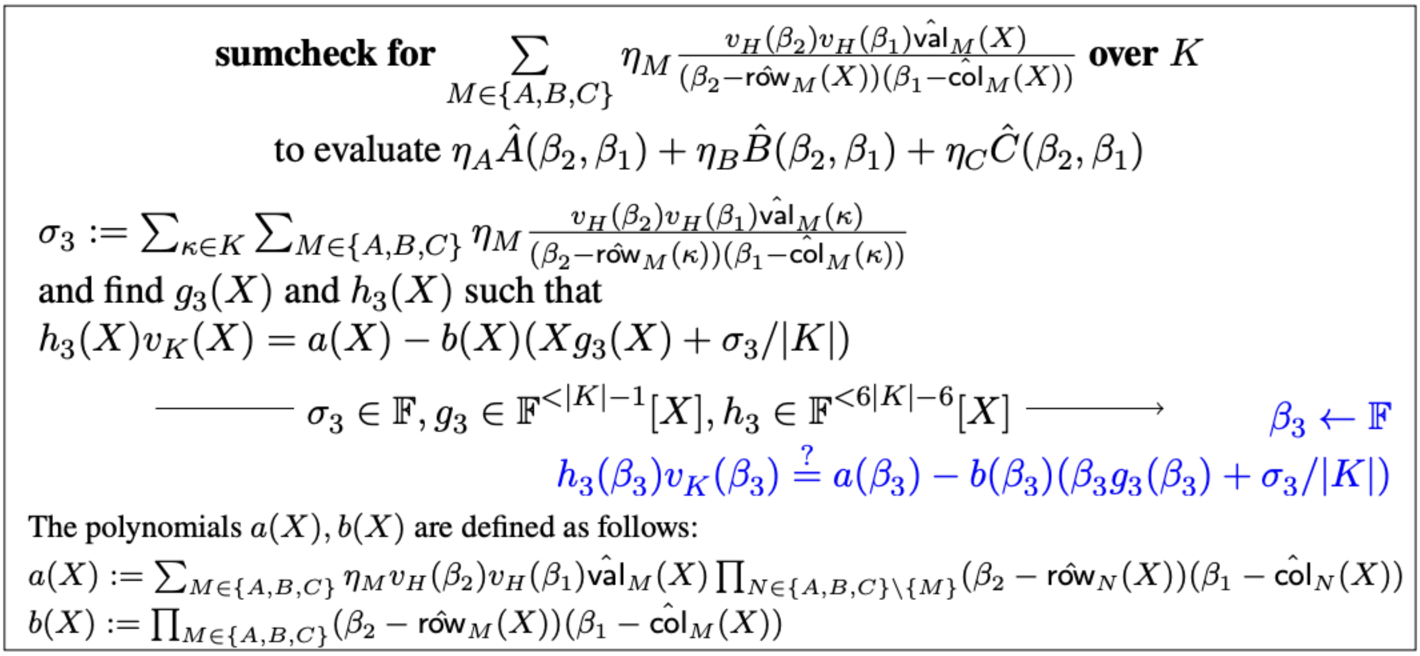
- $a(X)-b(X)f_3(X)=h_3(X)v_K(X)$, this equation demonstrates that f_3 agrees with the correct addends over K .

These two equations can be combined into one:
$h_3(X)v_K(X)=a(X)-b(X)(Xg_3(X)+\sigma_3/|K|)$.



We thus rely on the univariate sumcheck protocol (yet) again: **V** sends β_2 to **P**, and then **P** replies with the value $\sigma_3 := \eta_A\hat{A}(\beta_2,\beta_1)+\eta_B\hat{B}(\beta_2,\beta_1)+\eta_C\hat{C}(\beta_2,\beta_1)$, which the verifier much check. Observe that

$$\eta_A\hat{A}(\beta_2,\beta_1)+\eta_B\hat{B}(\beta_2,\beta_1)+\eta_C\hat{C}(\beta_2,\beta_1)=\sum_{\kappa\in K}\sum_{M\in\{A,B,C\}}\eta_M\frac{v_H(\beta_2)v_H(\beta_1)\hat{\mathsf{val}}_M(\kappa)}{(\beta_2-\hat{\mathsf{row}}_M(\kappa))(\beta_1-\hat{\mathsf{col}}_M(\kappa))}\ .$$



sumcheck for $\sum_{M\in\{A,B,C\}}\eta_M\frac{v_H(\beta_2)v_H(\beta_1)\hat{\mathsf{val}}_M(X)}{(\beta_2-\hat{\mathsf{row}}_M(X))(\beta_1-\hat{\mathsf{col}}_M(X))}$ **over** K

to evaluate $\eta_A\hat{A}(\beta_2,\beta_1)+\eta_B\hat{B}(\beta_2,\beta_1)+\eta_C\hat{C}(\beta_2,\beta_1)$

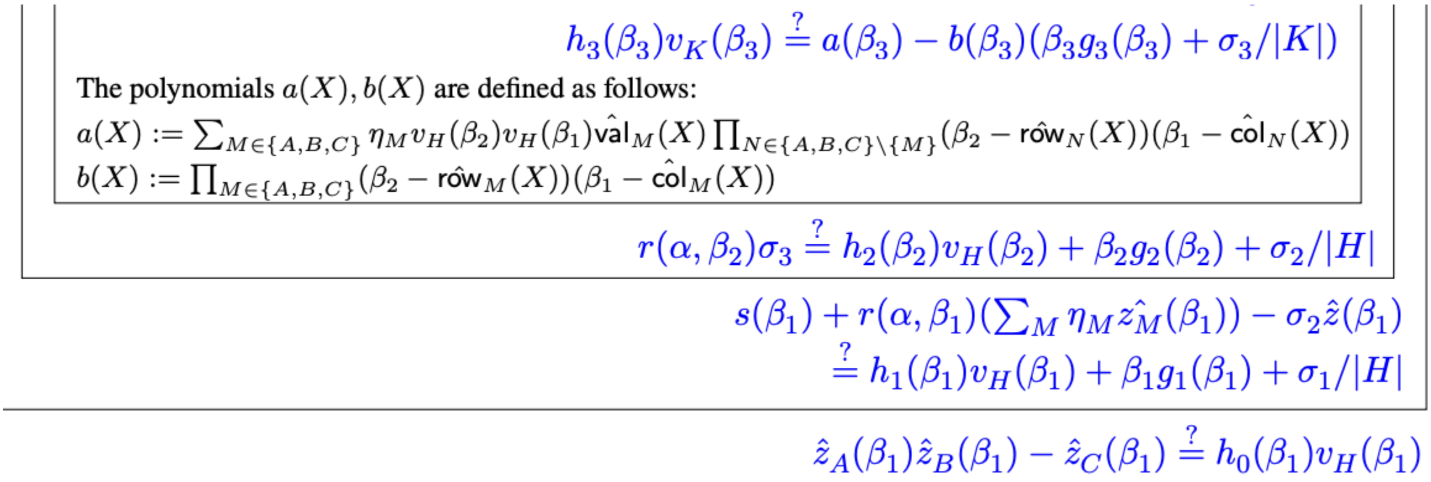
$\sigma_3 := \sum_{\kappa\in K}\sum_{M\in\{A,B,C\}}\eta_M\frac{v_H(\beta_2)v_H(\beta_1)\hat{\mathsf{val}}_M(\kappa)}{(\beta_2-\hat{\mathsf{row}}_M(\kappa))(\beta_1-\hat{\mathsf{col}}_M(\kappa))}$
and find $g_3(X)$ and $h_3(X)$ such that
$h_3(X)v_K(X)=a(X)-b(X)(Xg_3(X)+\sigma_3/|K|)$

$$\xrightarrow{\quad\sigma_3\in\mathbb{F},\ g_3\in\mathbb{F}^{<|K|-1}[X],\ h_3\in\mathbb{F}^{<6|K|-6}[X]\quad}\qquad \beta_3\leftarrow\mathbb{F}$$

$$h_3(\beta_3)v_K(\beta_3)\overset{?}{=}a(\beta_3)-b(\beta_3)(\beta_3g_3(\beta_3)+\sigma_3/|K|)$$

The polynomials $a(X), b(X)$ are defined as follows:
$a(X) := \sum_{M\in\{A,B,C\}}\eta_M v_H(\beta_2)v_H(\beta_1)\hat{\mathsf{val}}_M(X)\prod_{N\in\{A,B,C\}\setminus\{M\}}(\beta_2-\hat{\mathsf{row}}_N(X))(\beta_1-\hat{\mathsf{col}}_N(X))$
$b(X) := \prod_{M\in\{A,B,C\}}(\beta_2-\hat{\mathsf{row}}_M(X))(\beta_1-\hat{\mathsf{col}}_M(X))$

(8)Round4-Verifier



$$h_3(\beta_3)v_K(\beta_3)\overset{?}{=}a(\beta_3)-b(\beta_3)(\beta_3g_3(\beta_3)+\sigma_3/|K|)$$

The polynomials $a(X), b(X)$ are defined as follows:
$a(X) := \sum_{M\in\{A,B,C\}}\eta_M v_H(\beta_2)v_H(\beta_1)\hat{\mathsf{val}}_M(X)\prod_{N\in\{A,B,C\}\setminus\{M\}}(\beta_2-\hat{\mathsf{row}}_N(X))(\beta_1-\hat{\mathsf{col}}_N(X))$
$b(X) := \prod_{M\in\{A,B,C\}}(\beta_2-\hat{\mathsf{row}}_M(X))(\beta_1-\hat{\mathsf{col}}_M(X))$

$$r(\alpha,\beta_2)\sigma_3\overset{?}{=}h_2(\beta_2)v_H(\beta_2)+\beta_2g_2(\beta_2)+\sigma_2/|H|$$

$$s(\beta_1)+r(\alpha,\beta_1)(\textstyle\sum_M\eta_M\hat{z_M}(\beta_1))-\sigma_2\hat{z}(\beta_1)$$
$$\overset{?}{=}h_1(\beta_1)v_H(\beta_1)+\beta_1g_1(\beta_1)+\sigma_1/|H|$$

$$\hat{z}_A(\beta_1)\hat{z}_B(\beta_1)-\hat{z}_C(\beta_1)\overset{?}{=}h_0(\beta_1)v_H(\beta_1)$$

Summary:

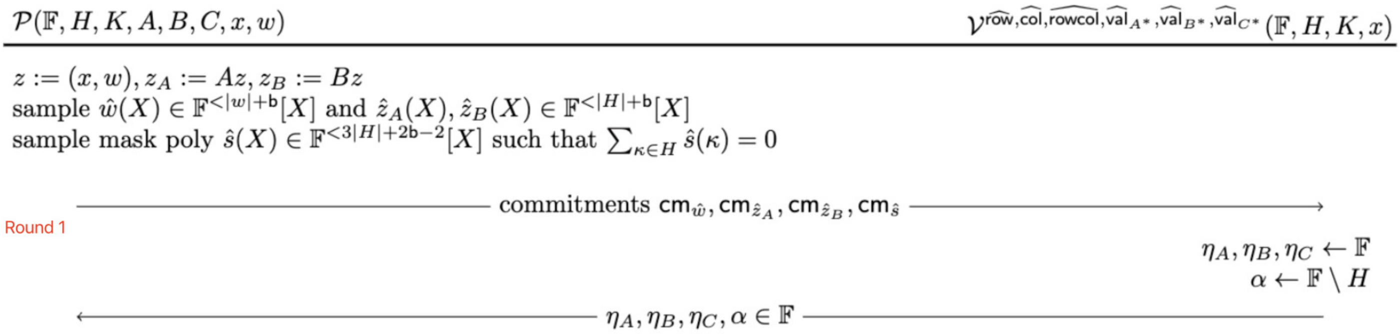
- **Offline**: 9 univariate polynomials define the low-degree extension of matrix M, leading to the output of 9 polynomial commitments.
- **Online**: The verifier queries each of the 9 indexer polynomials and 12 prover polynomials at exactly one location, which amounts to 21 queries.:

  $$\hat{w}(X), \hat{z}_A(X), \hat{z}_B(X), \hat{z}_C(X), h_0(X), s(X), g_1(X), h_1(X), g_2(X), h_2(X), g_3(X), h_3(X)$$

  - The prover outputs 12 commitments, 21 evaluations, and 3 evaluation proofs.
  - 12 commitments: $\hat{w}(X), \hat{z}_A(X), \hat{z}_B(X), \hat{z}_C(X), h_0(X), s(X), g_1(X), h_1(X), g_2(X), h_2(X), g_3(X), h_3(X)$
  - At point β_1 : $\hat{w}, \hat{z_A}, \hat{z_B}, \hat{z_C}, h_0, s, h_1, g_1$.
  - At point β_2 : h_2, g_2 .
  - At point β_3 : $h_3, g_3, r\hat{o}w_M, c\hat{o}l_M, v\hat{a}l_M, M \in \{A, B, C\}$.
- **Overall**: 27 $\mathbb{G}_1 + 24\mathbb{F}_q$.

4. Optimizations for AHP

1. **Elimination of h_0 and $\hat{z_C}$**:
   - Research indicates it's possible to omit proving the zeroTest, simply by replacing $\hat{z_C}(X)$ directly with $\hat{z_A}(X) \cdot \hat{z_B}(X)$ in subsequent proofs.
2. **Minimal Zero Knowledge Query Bound**:
   - Set the coefficient $b = 1$ directly within the mask polynomial.
3. **Eliminating σ_1** :
   - Construct a special mask polynomial that sums to zero over H, rather than σ_1 .
4. **A More Efficient Holographic Lincheck**:
   - Based on existing theoretical proofs, it is possible to reduce one round of interaction, specifically by eliminating one round of the sumcheck.



$\mathcal{P}(\mathbb{F}, H, K, A, B, C, x, w)$

$\mathcal{V}^{\widehat{\mathsf{row}}, \widehat{\mathsf{col}}, \widehat{\mathsf{rowcol}}, \widehat{\mathsf{val}}_{A^*}, \widehat{\mathsf{val}}_{B^*}, \widehat{\mathsf{val}}_{C^*}}(\mathbb{F}, H, K, x)$

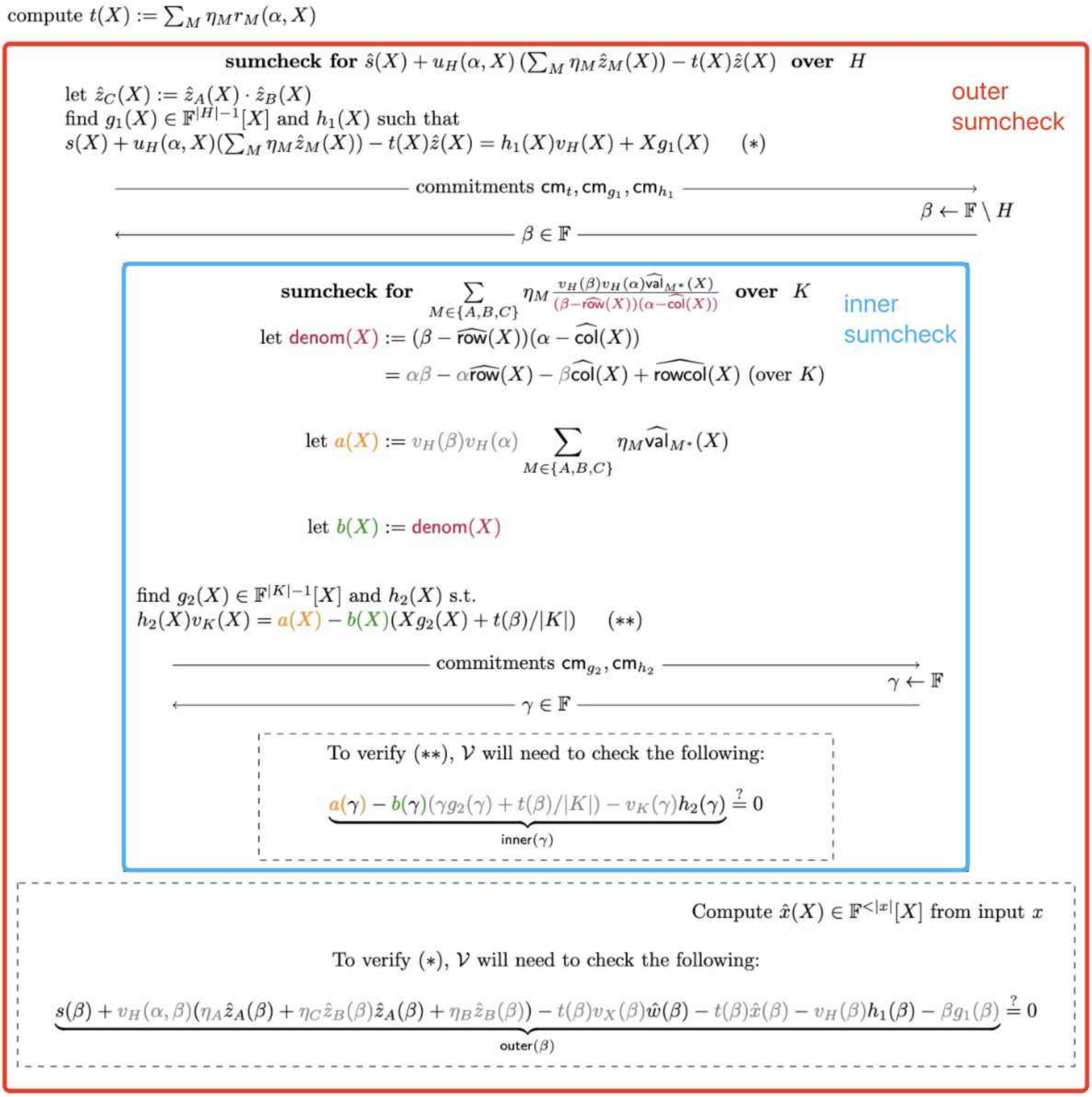
$z := (x, w), z_A := Az, z_B := Bz$
sample $\hat{w}(X) \in \mathbb{F}^{<|w|+\mathsf{b}}[X]$ and $\hat{z}_A(X), \hat{z}_B(X) \in \mathbb{F}^{<|H|+\mathsf{b}}[X]$
sample mask poly $\hat{s}(X) \in \mathbb{F}^{<3|H|+2\mathsf{b}-2}[X]$ such that $\sum_{\kappa \in H} \hat{s}(\kappa) = 0$

Round 1

$\xrightarrow{\text{commitments } \mathsf{cm}_{\hat{w}}, \mathsf{cm}_{\hat{z}_A}, \mathsf{cm}_{\hat{z}_B}, \mathsf{cm}_{\hat{s}}}$

$\eta_A, \eta_B, \eta_C \leftarrow \mathbb{F}$
$\alpha \leftarrow \mathbb{F} \setminus H$

$\xleftarrow{\eta_A, \eta_B, \eta_C, \alpha \in \mathbb{F}}$



compute $t(X) := \sum_M \eta_M r_M(\alpha, X)$

sumcheck for $\hat{s}(X) + u_H(\alpha, X)\left(\sum_M \eta_M \hat{z}_M(X)\right) - t(X)\hat{z}(X)$ **over** H

let $\hat{z}_C(X) := \hat{z}_A(X) \cdot \hat{z}_B(X)$

find $g_1(X) \in \mathbb{F}^{|H|-1}[X]$ and $h_1(X)$ such that

$$s(X) + u_H(\alpha, X)(\textstyle\sum_M \eta_M \hat{z}_M(X)) - t(X)\hat{z}(X) = h_1(X)v_H(X) + Xg_1(X) \qquad (*)$$

$$\xrightarrow{\text{commitments } \mathsf{cm}_t, \mathsf{cm}_{g_1}, \mathsf{cm}_{h_1}}$$

$\beta \leftarrow \mathbb{F} \setminus H$

$$\xleftarrow{\beta \in \mathbb{F}}$$

sumcheck for $\sum_{M \in \{A,B,C\}} \eta_M \frac{v_H(\beta)v_H(\alpha)\widehat{\mathsf{val}}_{M^*}(X)}{(\beta - \widehat{\mathsf{row}}(X))(\alpha - \widehat{\mathsf{col}}(X))}$ **over** K

let $\mathsf{denom}(X) := (\beta - \widehat{\mathsf{row}}(X))(\alpha - \widehat{\mathsf{col}}(X))$

$= \alpha\beta - \alpha\widehat{\mathsf{row}}(X) - \beta\widehat{\mathsf{col}}(X) + \widehat{\mathsf{rowcol}}(X)$ (over K)

let $a(X) := v_H(\beta)v_H(\alpha) \sum_{M \in \{A,B,C\}} \eta_M \widehat{\mathsf{val}}_{M^*}(X)$

let $b(X) := \mathsf{denom}(X)$

find $g_2(X) \in \mathbb{F}^{|K|-1}[X]$ and $h_2(X)$ s.t.

$$h_2(X)v_K(X) = a(X) - b(X)(Xg_2(X) + t(\beta)/|K|) \qquad (**)$$

$$\xrightarrow{\text{commitments } \mathsf{cm}_{g_2}, \mathsf{cm}_{h_2}}$$

$\gamma \leftarrow \mathbb{F}$

$$\xleftarrow{\gamma \in \mathbb{F}}$$

To verify $(**)$, $\mathcal{V}$ will need to check the following:

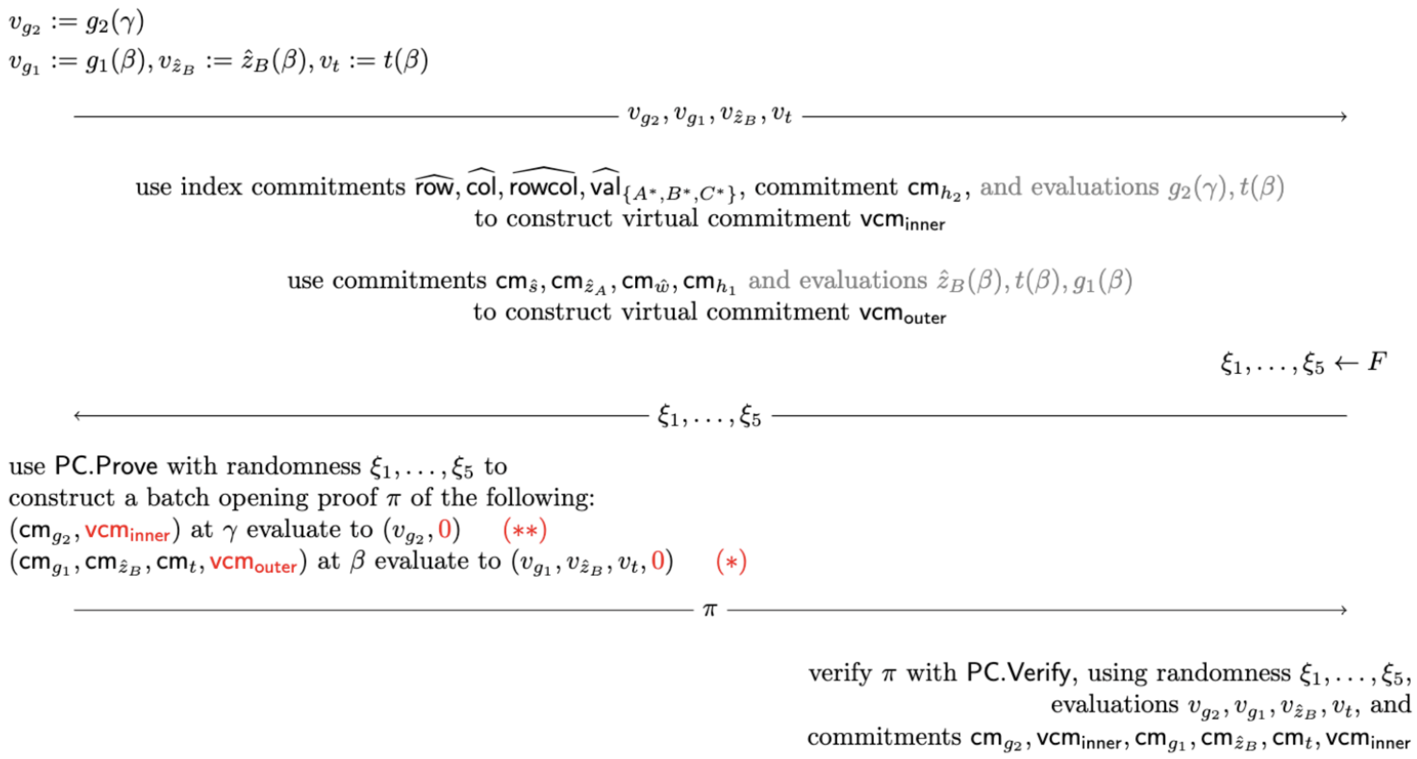
$$\underbrace{a(\gamma) - b(\gamma)(\gamma g_2(\gamma) + t(\beta)/|K|) - v_K(\gamma)h_2(\gamma)}_{\mathsf{inner}(\gamma)} \overset{?}{=} 0$$

Compute $\hat{x}(X) \in \mathbb{F}^{<|x|}[X]$ from input x

To verify $(*)$, $\mathcal{V}$ will need to check the following:

$$\underbrace{s(\beta) + v_H(\alpha, \beta)(\eta_A \hat{z}_A(\beta) + \eta_C \hat{z}_B(\beta)\hat{z}_A(\beta) + \eta_B \hat{z}_B(\beta)) - t(\beta)v_X(\beta)\hat{w}(\beta) - t(\beta)\hat{x}(\beta) - v_H(\beta)h_1(\beta) - \beta g_1(\beta)}_{\mathsf{outer}(\beta)} \overset{?}{=} 0$$

- The use of polynomial commitments to commit and prove the values mentioned above.



$v_{g_2} := g_2(\gamma)$

$v_{g_1} := g_1(\beta), v_{\hat{z}_B} := \hat{z}_B(\beta), v_t := t(\beta)$

$$\xrightarrow{\quad v_{g_2}, v_{g_1}, v_{\hat{z}_B}, v_t \quad}$$

use index commitments $\widehat{\mathsf{row}}, \widehat{\mathsf{col}}, \widehat{\mathsf{rowcol}}, \widehat{\mathsf{val}}_{\{A^*,B^*,C^*\}}$, commitment cm_{h_2}, and evaluations $g_2(\gamma), t(\beta)$
to construct virtual commitment $\mathsf{vcm}_{\mathsf{inner}}$

use commitments $\mathsf{cm}_{\hat{s}}, \mathsf{cm}_{\hat{z}_A}, \mathsf{cm}_{\hat{w}}, \mathsf{cm}_{h_1}$ and evaluations $\hat{z}_B(\beta), t(\beta), g_1(\beta)$
to construct virtual commitment $\mathsf{vcm}_{\mathsf{outer}}$

$\xi_1, \ldots, \xi_5 \leftarrow F$

$$\xleftarrow{\quad \xi_1, \ldots, \xi_5 \quad}$$

use $\mathsf{PC.Prove}$ with randomness $\xi_1, \ldots, \xi_5$ to
construct a batch opening proof π of the following:
$(\mathsf{cm}_{g_2}, \mathsf{vcm}_{\mathsf{inner}})$ at γ evaluate to $(v_{g_2}, 0)$ $(**)$
$(\mathsf{cm}_{g_1}, \mathsf{cm}_{\hat{z}_B}, \mathsf{cm}_t, \mathsf{vcm}_{\mathsf{outer}})$ at β evaluate to $(v_{g_1}, v_{\hat{z}_B}, v_t, 0)$ $(*)$

$$\xrightarrow{\quad \pi \quad}$$

verify π with $\mathsf{PC.Verify}$, using randomness $\xi_1, \ldots, \xi_5$,
evaluations $v_{g_2}, v_{g_1}, v_{\hat{z}_B}, v_t$, and
commitments $\mathsf{cm}_{g_2}, \mathsf{vcm}_{\mathsf{inner}}, \mathsf{cm}_{g_1}, \mathsf{cm}_{\hat{z}_B}, \mathsf{cm}_t, \mathsf{vcm}_{\mathsf{inner}}$

https://github.com/arkworks-rs/marlin/blob/master/diagram/diagram.pdf

5. References

- Preprocessing zkSNARKs with Universal and Updatable SRS
- Aleo Varuna Code
- Marlin Code
- PST13
- The Evolution of Polynomial Commitments
- A Survey of Elliptic Curves for Proof Systems
- Aurora: Transparent Succinct Arguments for R1CS