

This diagram (on the following page) shows the interaction of the Marlin prover and verifier. It is similar to the diagrams in the paper (Figure 5 in Section 5 and Figure 7 in Appendix E, in the latest ePrint version), but with two changes: it shows not just the AHP but also the use of the polynomial commitments (the cryptography layer); and it aims to be fully up-to-date with the recent optimizations to the codebase. This diagram, together with the diagrams in the paper, can act as a “bridge” between the codebase and the theory that the paper describes.

## 1 Glossary of notation

$\mathbb{F}$	the finite field over which the R1CS instance is defined
$x$	public input
$w$	secret witness
$H$	variable domain
$K_M$	matrix domain for matrix $M$
$K$	$\arg \max_{K_M}  K_M $
$X$	domain sized for input (not including witness)
$v_D(X)$	vanishing polynomial over domain $D$
$s_{D_1, D_2}(X)$	“selector” polynomial over domains $D_1 \supseteq D_2$ , defined as $\frac{ D_2 v_{D_1}}{ D_1 v_{D_2}}$
$u_D(X, Y)$	bivariate derivative of vanishing polynomials over domain $D$
$A, B, C$	R1CS instance matrices
$A^*, B^*, C^*$	shifted transpose of $A, B, C$ matrices given by $M_{a,b}^* := M_{b,a} \cdot u_H(b, b) \forall a, b \in H$ (optimization from Fractal, explained in Claim 6.7 of that paper)
$\text{row}_M, \text{col}_M, \text{val}_M$	LDEs of (respectively) row positions, column positions, and values of non-zero elements of matrix $M^*$
$\text{rowcol}_M$	LDE of the element-wise product of $\text{row}$ and $\text{col}$ , given separately for efficiency (namely to allow this product to be part of a <i>linear</i> combination)
$\mathcal{P}$	prover
$\mathcal{V}$	verifier
$\mathcal{V}^p$	$\mathcal{V}$ with “oracle” access to polynomial $p$ (via commitments provided by the indexer, later opened as necessary by $\mathcal{P}$ )
$b$	bound on the number of queries
$r_M(X, Y)$	an intermediate polynomial defined by $r_M(X, Y) = M^*(Y, X)$

## 2 Diagram

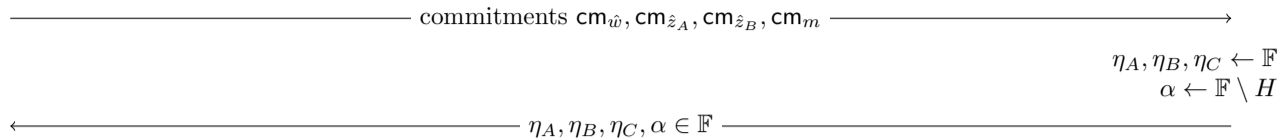
$\mathcal{P}(\mathbb{F}, H, K, A, B, C, x, w)$

$\mathcal{V}^{\text{row}, \text{col}, \text{rowcol}, \text{val}_A^*, \text{val}_B^*, \text{val}_C^*}(\mathbb{F}, H, K, x)$

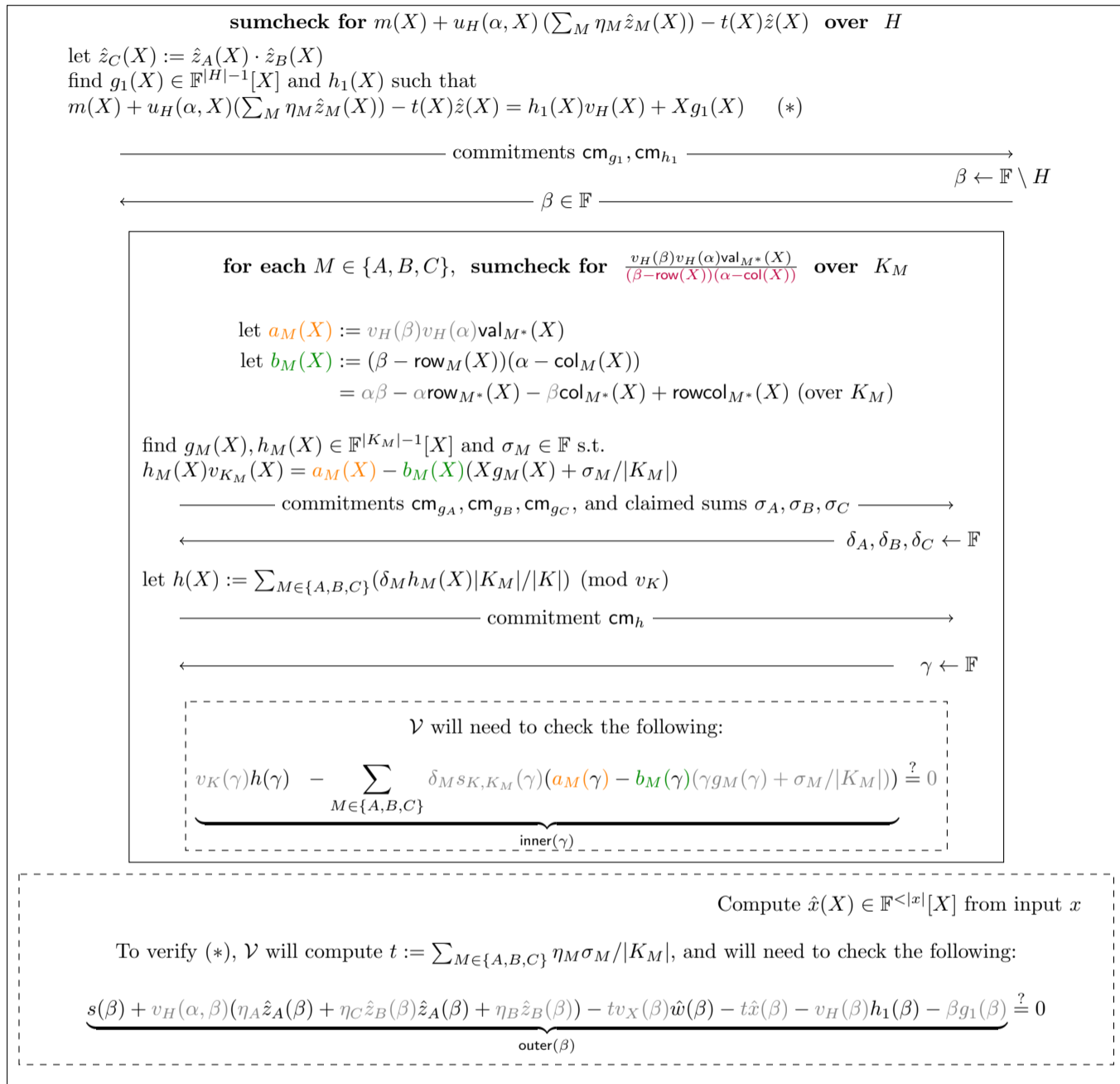
$z := (x, w), z_A := Az, z_B := Bz$

sample  $\hat{w}(X) \in \mathbb{F}^{\langle |w| + b \rangle}[X]$  and  $\hat{z}_A(X), \hat{z}_B(X) \in \mathbb{F}^{\langle |H| + b \rangle}[X]$

sample mask poly  $m(X) \in \mathbb{F}^{\langle 3|H| + 2b - 2 \rangle}[X]$  such that  $\sum_{\kappa \in H} m(\kappa) = 0$

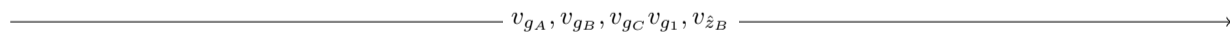


compute  $t(X) := \sum_M \eta_M r_M(\alpha, X)$



$v_{g_A} := g_A(\gamma), v_{g_B} := g_B(\gamma), v_{g_C} := g_C(\gamma)$

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



use  $\text{cm}_h$ , and for each  $M \in \{A, B, C\}$ , index commitments to  $\text{row}_M, \text{col}_M, \text{rowcol}_M, \text{val}_M$ , evaluation  $g_M(\gamma)$ , and sum  $\sigma_M$  to construct virtual commitment  $\text{vcm}_{\text{inner}}$

use commitments  $\text{cm}_m, \text{cm}_{\hat{z}_A}, \text{cm}_{\hat{w}}, \text{cm}_{h_1}$  and evaluations  $\hat{z}_B(\beta), g_1(\beta)$  and sums  $\sigma_A, \sigma_B, \sigma_C$  to construct virtual commitment  $\text{vcm}_{\text{outer}}$

$\xi_1, \dots, \xi_5 \leftarrow F$

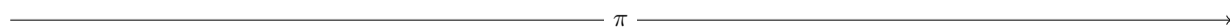


use PC.Prove with randomness  $\xi_1, \dots, \xi_5$  to

construct a batch opening proof  $\pi$  of the following:

$(\text{cm}_{g_A}, \text{cm}_{g_B}, \text{cm}_{g_C}, \text{vcm}_{\text{inner}})$  at  $\gamma$  evaluate to  $(v_{g_A}, v_{g_B}, v_{g_C}, 0)$  (\*\*)

$(\text{cm}_{g_1}, \text{cm}_{\hat{z}_B}, \text{cm}_t, \text{vcm}_{\text{outer}})$  at  $\beta$  evaluate to  $(v_{g_1}, v_{\hat{z}_B}, 0)$  (\*)



verify  $\pi$  with PC.Verify, using randomness  $\xi_1, \dots, \xi_5$ , evaluations  $v_{g_A}, v_{g_B}, v_{g_C}, v_{g_1}, v_{\hat{z}_B}$ , and commitments  $\text{cm}_{g_A}, \text{cm}_{g_B}, \text{cm}_{g_C}, \text{vcm}_{\text{inner}}, \text{cm}_{g_1}, \text{cm}_{\hat{z}_B}, \text{vcm}_{\text{inner}}$