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
$\overline{w}$	secret witness
H	variable domain
K	matrix domain
X	domain sized for input (not including witness)
$v_D(X)$	vanishing polynomial over domain $D$
A,B,C	R1CS instance matrices
$A^*, B^*, C^*$	shifted transpose of $A, B, C$ matries 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)
$\{\hat{val}, \hat{row}, \hat{col}\}_{\{A^*, B^*, C^*\}}$	preprocessed polynomials from $A^*, B^*, C^*$ matrices containing LDEs of (respectively)
	row positions, column positions, and values of non-zero matrix elements
$\hat{rowcol}_{\{A^*,B^*,C^*\}}$	the product polynomial of rôw and 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 $\mathcal{P}$ )

```
z:=(x,w), \hat{z}_A:=Az, \hat{z}_B:=Bz sample \hat{w}(X)\in\mathbb{F}^{<|w|+b}[X] and \hat{z}_A(X), \hat{z}_B(X)\in\mathbb{F}^{<|H|+b}[X] sample mask poly \hat{s}(X)\in\mathbb{F}^{<3|H|+2b-2}[X] such that \sum_{\kappa\in H}\hat{s}(\kappa)=0
                                                                           — 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
                                                                                            compute t(X) := \sum_{M} \eta_{M} r_{M}(\alpha, X)
                                               sumcheck for \hat{s}(X) + r(\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) + r(\alpha, X)(\sum_{M} \eta_{M} \hat{z}_{M}(X)) - t(X)\hat{z}(X) = h_{1}(X)v_{H}(X) + Xg_{1}(X) \qquad (*)
                                                                                  — commitments \mathsf{cm}_t, \mathsf{cm}_{g_1}, \mathsf{cm}_{h_1} —
                                                                                                                                                                                               \beta \leftarrow \mathbb{F} \setminus H
                                                    sumcheck for \sum_{M \in \{A,B,C\}} \eta_M \frac{v_H(\beta)v_H(\alpha)\hat{\mathsf{val}}_{M^*}(X)}{(\beta - \hat{\mathsf{row}}_{M^*}(X))(\alpha - \hat{\mathsf{col}}_{M^*}(X))} \ \ \text{over} \ \ K
                                  for M \in \{A, B, C\}, let \underline{M}_{\mathsf{denom}}(X) := (\beta - \mathring{\mathsf{row}}_{M^*}(X))(\alpha - \mathring{\mathsf{col}}_{M^*}(X))
                                                                                                 = \alpha \beta - \alpha \hat{\mathsf{row}}_{M^*}(X) - \beta \hat{\mathsf{col}}_{M^*}(X) + \hat{\mathsf{rowcol}}_{M^*}(X)
                                                   let a(X) := \sum_{M \in \{A,B,C\}} \eta_M v_H(\beta) v_H(\alpha) \hat{\mathsf{val}}_{M^*}(X) \prod_{N \neq M} N_{\mathsf{denom}}(X)
                                                                                let b(X) := \prod_{M \in \{A,B,C\}} M_{\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|) (**)
                                                                                     — commitments \mathsf{cm}_{g_2}, \mathsf{cm}_{h_2} -
                                                                   To verify (**), \mathcal V will need to check the following:
                                                                    \frac{a(\gamma) - b(\gamma)(\gamma g_2(\gamma) + t(\beta)/|K|) - v_K(\gamma)h_2(\gamma) \stackrel{?}{=} 0
                                                                                                  \mathsf{sumcheck}_{\mathsf{inner}}(\gamma)
                                                                                                                                                                         Compute \hat{x}(X) \in \mathbb{F}^{<|x|}[X]
                                                                    To verify (*), \mathcal{V} will need to check the following:
            s(\beta) + r(\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) \stackrel{?}{=} 0
v_{g_2} := g_2(\gamma), v_{A_{\mathsf{denom}}} := A_{\mathsf{denom}}(\gamma), v_{B_{\mathsf{denom}}} := B_{\mathsf{denom}}(\gamma), v_{C_{\mathsf{denom}}} := C_{\mathsf{denom}}(\gamma)
v_{g_1} := g_1(\beta), v_{\hat{z}_B} := \hat{z}_B(\beta), v_t := t(\beta)
                                                                              v_{g_2}, v_{A_{\mathsf{denom}}}, v_{B_{\mathsf{denom}}}, v_{C_{\mathsf{denom}}}, v_{g_1}, v_{\hat{z}_B}, v_t =
                        use index commitments row, col, rowcol to construct virtual commitments vcm_{\{A_{denom}, B_{denom}, C_{denom}\}}
               use index commitments val, commitments \mathsf{vcm}_{A_{\mathsf{denom}}}, \mathsf{vcm}_{B_{\mathsf{denom}}}, \mathsf{cm}_{h_2}, and evaluations g_2(\gamma), t(\beta)
                                                                     to construct virtual commitment vcm<sub>sumchecking</sub>
                                             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 vcm<sub>sumcheckouter</sub>
                                                                                                                                                                                                    \xi_1,\ldots,\xi_5\leftarrow\mathbb{F}
                                                                                                     -\xi_1,\ldots,\xi_5
use PC.
Prove with randomness \xi_1,\ldots,\xi_5 to
construct a batch opening proof \pi of the following:
verify \pi with PC. Verify, using randomness \xi_1, \ldots, \xi_5,
                                                                                                                                 evaluations v_{g_2}, v_{A_{\mathsf{denom}}}, v_{B_{\mathsf{denom}}}, v_{C_{\mathsf{denom}}}, v_{g_1}, v_{\hat{z}_B}, v_t, and
                                                                                                                                             \text{commitments } \mathsf{cm}_{g_2}, \mathsf{cm}_{A_{\mathsf{denom}}}, \mathsf{cm}_{B_{\mathsf{denom}}}, \mathsf{cm}_{C_{\mathsf{denom}}},
                                                                                                                                                \mathsf{vcm}_{\mathsf{sumcheck}_{\mathsf{inner}}}, \mathsf{cm}_{g_1}, \mathsf{cm}_{\hat{z}_B}, \mathsf{cm}_t, \mathsf{vcm}_{\mathsf{sumcheck}_{\mathsf{inner}}}
```