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
$\overline{H}$	variable domain
$K_M$	matrix domain for matrix $M$
K	$rg \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 $A, B, C$ 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)
$row_M, col_M, val_M$	LDEs of (respectively) row positions, column positions, and values of non-zero elements of matrix $M^*$
$rowcol_M$	LDE of the element-wise product of row and col, given separately for efficiency
	(namely to allow this product to be part of a linear combination)
${\cal P}$	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 $r_M(X,Y) = M^*(Y,X)$

```
\begin{array}{l} z:=(x,w), z_A:=Az, z_B:=Bz\\ \text{sample } \hat{w}(X)\in \mathbb{F}^{<|w|+\mathsf{b}}[X] \text{ and } \hat{z}_A(X), \hat{z}_B(X)\in \mathbb{F}^{<|H|+\mathsf{b}}[X]\\ \text{sample mask poly } m(X)\in \mathbb{F}^{<3|H|+2\mathsf{b}-2}[X] \text{ such that } \sum_{\kappa\in H} m(\kappa)=0 \end{array}
                                                                        — commitments \mathsf{cm}_{\hat{w}}, \mathsf{cm}_{\hat{z}_A}, \mathsf{cm}_{\hat{z}_B}, \mathsf{cm}_m —
                                                                                                                                                                                          \eta_A, \eta_B, \eta_C \leftarrow \mathbb{F}
                                                                                                                                                                                                  \alpha \leftarrow \mathbb{F} \setminus H
                                                                              \eta_A, \eta_B, \eta_C, \alpha \in \mathbb{F} —
compute t(X) := \sum_{M} \eta_{M} r_{M}(\alpha, X)
                                          sumcheck for m(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
           m(X) + u_H(\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}_{g_1}, \mathsf{cm}_{h_1} —
                                                                                                                                                                                      \beta \leftarrow \mathbb{F} \setminus H
                                                                                                    -\beta \in \mathbb{F} —
                                         for each M \in \{A, B, C\}, sumcheck for \frac{v_H(\beta)v_H(\alpha)\mathsf{val}_{M^*}(X)}{(\beta - \mathsf{row}(X))(\alpha - \mathsf{col}(X))} over K_M
                                            let a_M(X) := v_H(\beta)v_H(\alpha)\mathsf{val}_{M^*}(X)
                                             let b_M(X) := (\beta - \mathsf{row}_M(X))(\alpha - \mathsf{col}_M(X))
                                                                = \alpha \beta - \alpha \operatorname{row}_{M^*}(X) - \beta \operatorname{col}_{M^*}(X) + \operatorname{rowcol}_{M^*}(X) \text{ (over } K_M)
                          find g_M(X), h_M(X) \in \mathbb{F}^{|K_M|-1}[X] and \sigma_M \in \mathbb{F} s.t.
                          h_M(X)v_{K_M}(X) = a_M(X) - b_M(X)(Xg_M(X) + \sigma_M/|K_M|)
                                                 — commitments \mathsf{cm}_{g_A}, \mathsf{cm}_{g_B}, \mathsf{cm}_{g_C}, and claimed sums \sigma_A, \sigma_B, \sigma_C —
                         let h(X) := \left(\sum_{M \in \{A,B,C\}} r_M h_M s_{K,K_M}\right) \pmod{v_K}
                                                                                --- commitment \mathsf{cm}_h -
                                                                            \mathcal{V} will need to check the following:
                                       v_K(\gamma)h(\gamma) - \sum_{M \in \{A,B,C\}} r_M s_{K,K_M} (a_M(\gamma) - b_M(\gamma)(\gamma g_M(\gamma) + \sigma_M/|K_M|)) \stackrel{?}{=} 0
                                                       \lim_{n\to\infty} \frac{1}{(\gamma)}
                                                                                                                                        Compute \hat{x}(X) \in \mathbb{F}^{<|x|}[X] from input x
                    To verify (*), \mathcal{V} will compute t := \sum_{M \in \{A,B,C\}} \eta_M \sigma_M / |K_M|, and will need to check the following:
                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)) - tv_X(\beta)\hat{w}(\beta) - t\hat{x}(\beta) - v_H(\beta)h_1(\beta) - \beta g_1(\beta) \stackrel{?}{=} 0
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)
                                                                              v_{g_A}, v_{g_B}, v_{g_C}v_{g_1}, v_{\hat{z}_B} =
 use cm_h, and for each M \in \{A, B, C\}, index commitments to row_M, col_M, rowcol_M, val_M, evaluation g_M(\gamma), and sum \sigma_M
                                                                        to construct virtual commitment vcm_{inner}
                           use commitments \mathsf{cm}_m, \mathsf{cm}_{\hat{z}_A}, \mathsf{cm}_{\hat{w}}, \mathsf{cm}_{h_1} and evaluations \hat{z}_B(\beta), g_1(\beta) and sums \sigma_A, \sigma_B, \sigma_C
                                                                       to construct virtual commitment vcm<sub>outer</sub>
                                                                                                                                                                                         \xi_1,\ldots,\xi_5\leftarrow 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:
(\mathsf{cm}_{g_A}, \mathsf{cm}_{g_B}, \mathsf{cm}_{g_C}, \mathsf{vcm}_{\mathsf{inner}}) at \gamma evaluate to (v_{g_A}, v_{g_B}, v_{g_C}, 0)
(\mathsf{cm}_{g_1}, \mathsf{cm}_{\hat{z}_B}, \mathsf{cm}_t, \mathsf{vcm}_{\mathsf{outer}}) at \beta evaluate to (v_{g_1}, v_{\hat{z}_B}, 0)
```