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	matrix domain
X	domain sized for input (not including witness)
$v_D(X)$	vanishing polynomial over domain D
$u_D(X,Y)$	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)
$\widehat{\mathsf{row}}, \widehat{\mathsf{col}}$	LDEs of (respectively) row positions and column positions of non-zero elements of any linear combination of A^*, B^*, and C^* (the choice of combination is irrelevant).
$\widehat{\mathsf{rowcol}}$	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)
$\widehat{\mathsf{val}}_{\{A^*,B^*,C^*\}}$	preprocessed polynomials containing LDEs of the values of non-zero elements of any linear combination of A^*, B^*, and C^*. That is, if κ is the k-th element of K, then $(\sum_M \eta_M \widehat{\mathsf{val}}_{M^*})(\kappa)$ is the k-th non-zero entry of $\sum_M \eta_M M^*$, for arbitrary $\eta_{\{A,B,C\}} \in \mathbb{F}$.
$\mathcal{P}$	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

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

$z := (x, w), z_A := Az, z_B := Bz$
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 $\sum_{\kappa \in H} \hat{s}(\kappa) = 0$

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

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

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

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

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

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

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

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:

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

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

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

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

$v_{g_2} := g_2(\gamma)$
$v_{g_1} := g_1(\beta), v_{\hat{z}_B} := \hat{z}_B(\beta), v_t := t(\beta)$

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

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 $\mathsf{vcm}_{\mathsf{outer}}$

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

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

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 $(v_{g_2}, 0) \qquad (**)$
$(\mathsf{cm}_{g_1}, \mathsf{cm}_{\hat{z}_B}, \mathsf{cm}_t, \mathsf{vcm}_{\mathsf{outer}})$ at β evaluate to $(v_{g_1}, v_{\hat{z}_B}, v_t, 0) \qquad (*)$

$\xrightarrow{\pi}$

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 $\mathsf{cm}_{g_2}, \mathsf{vcm}_{\mathsf{inner}}, \mathsf{cm}_{g_1}, \mathsf{cm}_{\hat{z}_B}, \mathsf{cm}_t, \mathsf{vcm}_{\mathsf{inner}}$