

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
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)
$\{\hat{\text{val}}, \hat{\text{row}}, \hat{\text{col}}\}_{\{A^*, B^*, C^*\}}$	preprocessed polynomials from A^*, B^*, C^* matrices containing LDEs of (respectively) row positions, column positions, and values of non-zero matrix elements
$\hat{\text{rowcol}}_{\{A^*, B^*, C^*\}}$	the product polynomial of $\hat{\text{row}}$ and $\hat{\text{col}}$, 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})

2 Diagram

