Marlin with Varuna Updates

Michel Dellepere

July 5, 2023

1 Protocol without multi-circuit batching

P has input $(\mathbb{F}, H, K, A, B, C, x, w)$, **V** has input $(\mathbb{F}, H, K, x)$ and oracle access to $(\mathsf{row}_M, \mathsf{col}_M, \mathsf{rowcol}_M, \mathsf{val}_M)_{M \in \{A,B,C\}}$.

R1-ROWCHECK

1. **P** will initialize $A' := \begin{bmatrix} A & 0 \\ 0 & v_1 \end{bmatrix}$, $B' := \begin{bmatrix} B & 0 \\ 0 & v_2 \end{bmatrix}$, $C' := \begin{bmatrix} C & 0 \\ 0 & v_3 \end{bmatrix}$, $z := (x, w)$, and $z' := [z, \rho_A, \rho_B, \rho_C]$ where $\rho_A, \rho_B, \rho_C \xleftarrow{\$} \mathbb{F}$ satisfy $\rho_A \cdot \rho_B - \rho_C = 0$. Note $v_i = [\delta_{1,i}, \delta_{2,i}, \delta_{3,i}]$ where $\delta_{i,j}$ is the Kronecker delta function.
2. **P** will compute (1) the LDE $\hat{z} \in \mathbb{F}^{|x|+|w|}$ of z', (2) the LDEs $\hat{z}_A, \hat{z}_B \in \mathbb{F}^{|H|+b}$ of $z_A := A'z', z_B := B'z'$ (resp.), and (3) $z_C := z_A \cdot z_B$.
3. **P** will send the oracle $[\hat{z}]$ to **V**.
4. **P** will compute the quotient polynomial $h_0(X) \in \mathbb{F}^{\leq |H|+b}$ such that $\hat{z}_A(X)\hat{z}_B(X) - \hat{z}_C(X) = h_0(X)v_H(X)$ and will send the oracle $[h_0]$ to **V**.
5. **V** will sample randomness $\eta_A, \eta_B, \eta_C, \gamma \xleftarrow{\$} \mathbb{F}$ and send $(\eta_A, \eta_B, \eta_C, \gamma)$ to **P**.
6. **P** will sample a *masking polynomial* $m(X) \xleftarrow{\$} \mathbb{F}^{2|C|+2b-2}$ such that $\sum_{c \in C} m(c) = 0$ and send the oracle $[m]$ to **V**.
7. **P** will send the claimed sums $\sigma_A := \hat{z}_A(\gamma), \sigma_B := \hat{z}_B(\gamma), \sigma_C := \hat{z}_C(\gamma) \in \mathbb{F}$ to **V**.
8. **V** will check that $\sigma_A \cdot \sigma_B - \sigma_C = h_0(\gamma)v_H(\gamma)$.
9. **P** and **V** will engage in a **LINEVAL** protocol to assert that $\sigma_M \stackrel{?}{=} \hat{z}_M(\gamma)$ for $M \in \{A, B, C\}$.

R2-UNISUMCHECK for $m(Y) + \frac{\sigma}{|H|} - \sum_M \eta_M \hat{M}(\gamma, Y)\hat{z}(Y) = 0$ **over** H.

1. **P** computes the claimed sum $\sigma := \sum_M \eta_M \sigma_M \in \mathbb{F}$.
2. **P** finds $h_1(Y), g_1(Y)$ such that $m(Y) + \frac{\sigma}{|H|} - \sum_M \eta_M \hat{M}(\gamma, Y)\hat{z}(Y) = h_1(Y)v_H(Y) + Yg_1(Y)$.
3. **P** sends oracles $[h_1], [g_1]$ to **V** along with claimed sum σ.
4. **V** sends $\beta \xleftarrow{\$} \mathbb{F} \setminus H$ to **P**.
5. **P** and **V** will engage in **R3-RATSUMCHECK** to assert that $\hat{M}(\gamma, \beta) = \omega_M$ for each $M \in \{A, B, C\}$.
6. **V** checks that $m(\beta) + \frac{\sigma}{|H|} - \sum_M \eta_M \omega_M \hat{z}(\beta) \stackrel{?}{=} h_1(\beta)v_H(\beta) + \beta g_1(\beta)$.

R3-RATSUMCHECK for $\hat{M}(\gamma, \beta) = \sum_{\kappa \in K_M} \frac{v_H(\gamma)v_H(\beta)\mathsf{val}'_M(\kappa)}{(\gamma - \mathsf{row}_M(\kappa))(\beta - \mathsf{col}_M(\kappa))} = \omega_M$ for each $M \in \{A, B, C\}$

1. **P** finds $h_M, g_M \in \mathbb{F}^{|K_M|-1}[X]$ and $\omega_M \in \mathbb{F}$ such that
$$v_H(\gamma)v_H(\beta)\mathsf{val}'_M(X) - (\gamma - \mathsf{row}_M(X))(\beta - \mathsf{col}_M(X))(Xg_M(X) - \omega_M/|K_M|) = h_M(X)v_{K_M}(X)$$
2. **P** sends oracle $[g_M]$ to **V** along with claimed sum ω_M for $M \in \{A, B, C\}$.
3. **V** samples $\delta_M \xleftarrow{\$} \mathbb{F}$ and sends to **P** for $M \in \{A, B, C\}$.
4. **P** computes the polynomial $h_2(X) := \sum_M \delta_M s_{K \setminus K_M}(X)h_M(X)\frac{|K_M|}{|K|}$ mod v_K and sends an oracle for $[h_2]$ to **V**.
5. **V** will sample $\zeta \xleftarrow{\$} \mathbb{F}$ and check
$$\sum_M \delta_M s_{K \setminus K_M}(\zeta)(v_H(\gamma)v_H(\beta)\mathsf{val}'_M(\zeta) - (\gamma - \mathsf{row}_M(\zeta))(\beta - \mathsf{col}_M(\zeta)))(\zeta g_M(\zeta) - \omega_M/|K_M|) \stackrel{?}{=} h_2(\zeta)v_K(\zeta)$$

R4-BATCHCOMMITS

1. **P** will compute and set:
   - $v_{g_A} := g_A(\zeta), v_{g_B} := g_B(\zeta), v_{g_C} := g_C(\zeta)$
   - $v_m := m(\beta), v_{\hat{z}}(\beta) := \hat{z}(\beta), v_{g_1}(\beta) := g_1(\beta), v_{h_1} := h_1(\beta)$
   - $v_{h_0} := h_0(\gamma)$
   - $v_{h_2}(\zeta) := h_2(\zeta)$

   and send these values to **V**.
2. **P** will construct a batch opening proof π of the following:
   - $([g_A], [g_B], [g_C])$ at ζ evaluate to $(v_{g_A}, v_{g_B}, v_{g_C})$
   - $([\hat{z}], [g_1], [h_1])$ at β evaluate to $(v_{\hat{z}}, v_{g_1}, v_{h_1})$
   - $([m], [h_0])$ at γ evaluate to (v_m, v_{h_0})
   - $[h_2]$ at ζ evaluates to v_{h_2}

3. **V** will verify proof π.

Completeness. For the **ROWCHECK** PIOP, note that $\hat{z}_M = [Mz, \rho_M]$ so we have $\hat{z}_A \circ \hat{z}_B = [Az, \rho_A] \circ [Bz, \rho_B] = [Az \circ Bz, \rho_A \rho_B]$. By the R1CS constraint $Az \circ Bz = Cz$ and by construction $\rho_A \rho_B = \rho_C$, which shows $\hat{z}_A \hat{z}_B = \hat{z}_C := [Cz, \rho_C]$, as desired. For the **LINEVAL** PIOP, we would like to prove $\sum_{Y \in H} \left(m(Y) + \frac{\sigma}{|H|} - \sum_M \eta_M \hat{M}(\gamma, Y) \hat{z}(Y) \right) = 0$. Recall $\sigma = \sum_M \eta_M \sigma_M$ and $\sum_{\kappa \in H} m(\kappa) = 0$ and hence $\sum_M \eta_M \sigma_M - \sum_{Y \in H} \sum_M \eta_M \hat{M}(\gamma, Y) \hat{z}(Y) = 0$. Note $\sigma_M \triangleq \hat{z}_M(\gamma) = \sum_{Y \in H} \hat{M}(\gamma, Y) \hat{z}(Y)$, as desired.