Varuna zkSNARK protocol specification

August 13, 2024

1 Protocol for a single circuit in R1CS, with Zero-Knowledge

I has input $(\mathbb{F}, H, K, (K_M, M)_{M\in\{A,B,C\}})$

INDEXER I

1. Invoke the indexer for the PIOP for **LINEVAL** to obtain the polynomials $(\mathsf{row}_M, \mathsf{col}_M, \mathsf{rowcol}_M, \mathsf{val}_M)_{M\in\{A,B,C\}}$.
2. Output $(\mathsf{row}_M, \mathsf{col}_M, \mathsf{rowcol}_M, \mathsf{val}_M)_{M\in\{A,B,C\}}$.

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

PIOP 1: ROWCHECK for $\hat{z}_A \cdot \hat{z}_B = \hat{z}_C$ **over** H.
Rounds 1, 2

1. **P** will initialize $A' := \begin{bmatrix} A & 0 \\ 0 & \rho_A \end{bmatrix}$, $B' := \begin{bmatrix} B & 0 \\ 0 & \rho_B \end{bmatrix}$, $C' := \begin{bmatrix} C & 0 \\ 0 & \rho_C \end{bmatrix}$, $w' := (w, \rho_A, \rho_B, \rho_C)$ and $z' := (x, w')$, 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 $\hat{z} \in \mathbb{F}^{|x|+|w'|}[X]$ of z', (2) the LDEs $\hat{z}_A, \hat{z}_B \in \mathbb{F}^{|H|+b}[X]$ 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 $[\hat{w}]$ to **V**.
4. **P** will compute the quotient polynomial $h_0(X) \in \mathbb{F}^{\leq |H|+b}[X]$ such that $\hat{z}_A(X)\hat{z}_B(X) - \hat{z}_C(X) = h_0(X)v_H(X)$.
5. **P** will sample a *masking polynomial* $m(X) \xleftarrow{\$} \mathbb{F}^{2|C|+2b-2}[X]$ such that $\sum_{c\in C} m(c) = 0$.
6. **P** will send the oracles $[h_0], [m]$ to **V**.
7. **V** will sample randomness $\alpha \setminus H \xleftarrow{\$} \mathbb{F}$ and send the challenge to **P**.
8. **P** and **V** will engage in a **UNISUMCHECK** protocol to assert that $\sigma_M \stackrel{?}{=} \hat{z}_M(\alpha)$ for $M \in \{A, B, C\}$.
9. **V** will check that $\sigma_A \cdot \sigma_B - \sigma_C = h_0(\alpha)v_H(\alpha)$.

PIOP 2: UNISUMCHECK for $m(Y) + \frac{\sigma}{|H|} - \sum_M \eta_M \hat{M}(\alpha, Y)\hat{z}(Y) = 0$ **over** H.
Round 3

1. **P** computes the claimed sum $\sigma := \sum_M \eta_M \sigma_M \in \mathbb{F}$ and sends it to **V**.
2. **V** will sample $\eta_A, \eta_B, \eta_C \xleftarrow{\$} \mathbb{F}$ and send the challenges to **P**.
3. **P** finds $h_1(Y), g_1(Y)$ such that $m(Y) + \frac{\sigma}{|H|} - \sum_M \eta_M \hat{M}(\alpha, Y)\hat{z}(Y) = h_1(Y)v_H(Y) + Yg_1(Y)$.
4. **P** sends oracles $[h_1], [g_1]$ to **V** along with claimed sums $\sigma_A := \hat{z}_A(\alpha), \sigma_B := \hat{z}_B(\alpha), \sigma_C := \hat{z}_C(\alpha) \in \mathbb{F}$.
5. **V** sends $\beta \xleftarrow{\$} \mathbb{F} \setminus H$ to **P**.
6. **P** and **V** will engage in **RATSUMCHECK** to assert that $\hat{M}(\alpha, \beta) = \omega_M$ for each $M \in \{A, B, C\}$.
7. **V** checks that $m(\beta) + \frac{\sigma}{|H|} - \sum_M \eta_M \sigma_M \hat{z}(\beta) \stackrel{?}{=} h_1(\beta)v_H(\beta) + \beta g_1(\beta)$.

PIOP 3: RATSUMCHECK for $\sum_{\kappa\in K_M} \frac{v_H(\alpha)v_H(\beta)\mathsf{val}'_M(\kappa)}{(\alpha-\mathsf{row}_M(\kappa))(\beta-\mathsf{col}_M(\kappa))} = \omega_M$ for each $M \in \{A, B, C\}$
Round 4, 5

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

Correctness. 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 choice of randomness $\rho_A\rho_B = \rho_C$, we have $\hat{z}_A\hat{z}_B = \hat{z}_C := [Cz, \rho_C]$, as desired. For correctness of the **LINEVAL** PIOP, recall $\sigma = \sum_M \eta_M \sigma_M$ and $\sum_{\kappa \in H} m(\kappa) = 0$, so $\sum_{Y \in H} m(Y) + \sum_{Y \in H} \frac{\sigma}{|H|} - \sum_{Y \in H} \sum_M \eta_M \hat{M}(\alpha, Y)\hat{z}(Y) = \sigma - \sum_{Y \in H} \sum_M \eta_M \hat{M}(\alpha, Y)\hat{z}(Y)$. Since $\sigma_M \triangleq \hat{z}_M(\alpha) = \sum_{Y \in H} \hat{M}(\alpha, Y)\hat{z}(Y)$, we have $\sigma - \sum_{Y \in H} \sum_M \eta_M \sigma_M = 0$, as desired.

Soundness. The verifier accepts a false claim if either the PIOP for **ROWCHECK**, the PIOP for **UNISUMCHECK**, or the PIOP for **RATSUMCHECK** fail. Each happen with probability $O(\deg(h_0)/|\mathbb{F} \setminus H|), O(|H|/|\mathbb{F}|)$, and $O(|K|/|\mathbb{F} \setminus H|)$, respectively. Hence the soundness error of the protocol is $O(\deg(h_0)/|\mathbb{F} \setminus H| + |H|/|\mathbb{F}| + |K|/|\mathbb{F} \setminus H|)$.

2 Protocol for a single circuit in R1CS, with lookups and Zero-Knowledge

I has input the index $\mathbb{I} = (\mathbb{F}, H, K, (K_M, t_M, M)_{M \in \{A,B,C\}}, f)$.

INDEXER I

1. Find a subgroup $H_T \leq \mathbb{F}^*$ to index the table t_M.
2. Find subgroups $H_R, H_F \leq \mathbb{F}^*$ to index the set of rows $r = \{0, \dots, \mathrm{ord}(H) - 1\} \setminus f$ which adhere to a rowcheck and the rows f which adhere to a table lookup, respectively.
3. Compute the LDEs $\hat{T}_A, \hat{T}_B \in \mathbb{F}^{|t_M|-1}[X]$ of t_A, t_B and set $\hat{T}_C := \hat{T}_A \cdot \hat{T}_B$.
4. Invoke the indexer for the PIOP for polynomial **ROWSAT** to obtain the selector polynomials s_{H,H_R}, s_{H,H_T}, and s_{H,H_F}.
5. Invoke the indexer for the PIOP for **LINEVAL** to obtain the polynomials $(\mathsf{row}_M, \mathsf{col}_M, \mathsf{rowcol}_M, \mathsf{val}_M)_{M \in \{A,B,C\}}$.
6. Output $(H_T, H_R, H_F, s_{H,H_R}, s_{H,H_T}, s_{H,H_F}, (\hat{T}_M, \mathsf{row}_M, \mathsf{col}_M, \mathsf{rowcol}_M, \mathsf{val}_M)_{M \in \{A,B,C\}})$.

P has input $(\mathbb{F}, H, (H_S)_{S \in \{T,R,F\}}, K, (K_M, \hat{T}_M, t_M, M)_{M \in \{A,B,C\}}, f, x, w)$,
V has input $(\mathbb{F}, H, (H_S)_{S \in \{T,R,F\}}, K, (K_M, t_M, M)_{M \in \{A,B,C\}}, x)$ and oracle access to $(\hat{T}_M, \mathsf{row}_M, \mathsf{col}_M, \mathsf{rowcol}_M, \mathsf{val}_M)_{M \in \{A,B,C\}}$.

PIOP 1: ROWCHECK for $\hat{z}_A \cdot \hat{z}_B = \hat{z}_C$ **over** H.

1. **P** will initialize $A' := \begin{bmatrix} A & 0 \\ 0 & \rho_A \end{bmatrix}$, $B' := \begin{bmatrix} B & 0 \\ 0 & \rho_B \end{bmatrix}$, $C' := \begin{bmatrix} C & 0 \\ 0 & \rho_C \end{bmatrix}$, $w' := (w, \rho_A, \rho_B, \rho_C)$ and $z' := (x, w')$ 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 $\hat{z} \in \mathbb{F}^{|x|+|w'|}[X]$ of z', (2) the LDEs $\hat{z}_A, \hat{z}_B \in \mathbb{F}^{|H|+b}[X]$ of $z_A := A'z', z_B := B'z'$ (resp.), and (3) $\hat{z}_C := \hat{z}_A \cdot \hat{z}_B$.
3. **P** will compute the *compressed table, lookup, and multiplicity polynomials*:
   (a) **P** will compute the compression factor $\zeta \in \mathbb{F}$ to construct the compressed table vector $T = (t_{A,i} + \zeta t_{B,i} + \zeta^2 t_{C,i})_{i \in [|t_M|]}$, and compute its LDE $\hat{T} \in \mathbb{F}^{|T|-1}[X]$ as $\hat{T} := \hat{T}_A + \zeta \hat{T}_B + \zeta^2 \hat{T}_C$.
   (b) **P** will use ζ to construct the compressed lookups vector $F = (z_{A,f(i)} + \zeta z_{B,f(i)} + \zeta^2 z_{C,f(i)})_{i \in [|f|]}$, and compute its LDE $\hat{F} \in \mathbb{F}^{|F|-1}[X]$, where $f(i)$ is the index of the ith lookup.
   (c) **P** will construct the multiplicity vector $m \in \mathbb{F}^{|T|}$ and compute its LDE $\hat{M} \in \mathbb{F}^{|T|-1}[X]$.
4. **P** will send the oracles $[\hat{w}], [\hat{M}], [\hat{F}], [\hat{T}]$ to **V**.
5. **V** will sample $\theta \xleftarrow{\$} \mathbb{F}, \alpha \xleftarrow{\$} \mathbb{F} \setminus H$ and send the challenges to **P**.
6. **P** will compute the sums $\sigma_M := \hat{z}_M(\alpha)$ for $M \in \{A, B, C\}$.
7. **P** and **V** will engage in a **UNISUMCHECK** protocol to assert that $\sigma_M \stackrel{?}{=} \hat{z}_M(\alpha)$ for $M \in \{A, B, C\}$.
8. **P** and **V** will engage in a **BATCHRATSUMCHECK** to assert that (1) $\hat{z}_A(X)\hat{z}_B(X) - \hat{z}_C(X)$ vanishes over H_R and (2) $s_{H,H_T} \frac{\hat{M}(X)}{\theta + \hat{T}(X)} - s_{H,H_F} \frac{1}{\theta + \hat{F}(X)}$ vanishes over H.

PIOP 2: UNISUMCHECK for $m(Y) + \frac{\sigma}{|H|} - \sum_M \eta_M \hat{M}(\alpha, Y)\hat{z}(Y) = 0$ **over** H.

1. **P** computes the claimed sum $\sigma := \sum_M \eta_M \sigma_M \in \mathbb{F}$ and sends it to **V**.
2. **V** will sample $\eta_A, \eta_B, \eta_C \xleftarrow{\$} \mathbb{F}$ and send the challenges to **P**.
3. **P** finds $h_1(Y), g_1(Y)$ such that $m(Y) + \frac{\sigma}{|H|} - \sum_M \eta_M \hat{M}(\alpha, Y)\hat{z}(Y) = h_1(Y)v_H(Y) + Yg_1(Y)$.
4. **P** sends oracles $[h_1], [g_1]$ to **V** along with claimed sums $\sigma_A := \hat{z}_A(\alpha), \sigma_B := \hat{z}_B(\alpha), \sigma_C := \hat{z}_C(\alpha) \in \mathbb{F}$.
5. **V** sends $\beta \xleftarrow{\$} \mathbb{F} \setminus H$ to **P**.
6. **P** and **V** will engage in **RATSUMCHECK** to assert that $\hat{M}(\alpha, \beta) = \sigma_M$ for each $M \in \{A, B, C\}$.
7. **V** checks that $m(\beta) + \frac{\sigma}{|H|} - \sum_M \eta_M \sigma_M \hat{z}(\beta) \stackrel{?}{=} h_1(\beta)v_H(\beta) + \beta g_1(\beta)$.

PIOP 3: RATSUMCHECK for $\sum_{\kappa \in K_M} \frac{v_H(\alpha)v_H(\beta)\mathsf{val}'_M(\kappa)}{(\alpha - \mathsf{row}_M(\kappa))(\beta - \mathsf{col}_M(\kappa))} = \sigma_M$ for each $M \in \{A, B, C\}$

1. **P** finds $h_M, g_M \in \mathbb{F}^{|K_M|-1}[X]$ such that

$$v_H(\alpha)v_H(\beta)\mathsf{val}'_M(X) - (\alpha - \mathsf{row}_M(X))(\beta - \mathsf{col}_M(X))(Xg_M(X) - \sigma_M/|K_M|) = h_M(X)v_{K_M}(X)$$

2. **P** sends oracle $[g_M]$ to **V** along with claimed sum σ_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 $h_2(X) := \frac{1}{v_K(X)} \sum_M \delta_M s_{K \setminus K_M}(X) h_M(X) v_{K_M}(X)$ and sends an oracle for $[h_2]$ to **V**.
5. **V** will sample $\gamma \xleftarrow{\$} \mathbb{F} \setminus K$ and check

$$\sum_M \delta_M s_{K \setminus K_M}(\gamma)(v_H(\alpha) v_H(\beta) \mathsf{val}'_M(\gamma) - (\alpha - \mathsf{row}_M(\gamma))(\beta - \mathsf{col}_M(\gamma)))(\zeta g_M(\gamma) - \sigma_M/|K_M|) \stackrel{?}{=} h_2(\gamma) v_K(\gamma)$$

PIOP 4: BATCHRATSUMCHECK for

$$\hat{z}_A(X)\hat{z}_B(X) - \hat{z}_C(X) \textbf{ over } H_R \text{ and } s_{H,H_T} \frac{\hat{M}(X)}{\theta + T(X)} - s_{H,H_F} \frac{1}{\theta + \hat{F}(X)} \textbf{ over } H$$

1. **V** samples $\phi \xleftarrow{\$} \mathbb{F}$ and sends the challenge to **P**.
2. **P** finds the polynomials polynomial $g_0(X), h_0(X) \in \mathbb{F}^{|H|-1}[X]$ such that

$$\begin{gathered} s_{H,H_R}(X)(\hat{z}_A(X)\hat{z}_B(X) - \hat{z}_C(X)) + \\ \phi \cdot \Big(s_{H,H_T}(X)\hat{M}(X)(\theta + \hat{F}(X)) - s_{H,H_F}(X)(\theta + T(X)) - (\theta + T(X))(\theta + \hat{F}(X)) X g_0(X) \Big) = h_0(X) v_H(X) \end{gathered}$$

3. **P** sends oracles $[g_0], [h_0]$ to **V**.
4. **V** checks that

$$\begin{gathered} s_{H,H_R}(\alpha)(\sigma_A \sigma_B - \sigma_C) + \\ \phi \cdot \Big(s_{H,H_T}(\alpha)\hat{M}(\alpha)(\theta + \hat{F}(X)) - s_{H,H_F}(\alpha)(\theta + T(\alpha)) - (\theta + T(\alpha))(\theta + \hat{F}(\alpha)) \cdot \alpha g_0(\alpha) \Big) = h_0(\alpha) v_H(\alpha) \end{gathered}$$