HyperNova: (Multi-Folding Scheme)

removing of cross-terms.

#1: Revisit R1CS:

$A, B, C \in \mathbb{F}^{m\times m}$,

public inputs

assignment $\vec{z} = (\vec{x}, 1, \vec{w}) \in \mathbb{F}^m$ witness

$$(A\cdot\vec{z})\circ(B\cdot\vec{z}) = C\cdot\vec{z} \Rightarrow \begin{cases} \vec{V}_A = A\cdot\vec{z},\ \vec{V}_B = B\cdot\vec{z},\ \vec{V}_C = C\cdot\vec{z} & \text{(Lin-check)} \\ \vec{V}_A \circ \vec{V}_B = \vec{V}_C & \text{(Row-check)} \end{cases}$$

#2: MLE and Sumcheck.

$\vec{a} \in \mathbb{F}^n$, $\quad \tilde{a}(\vec{x}) = a_i$, $\forall \vec{x} \in \{0,1\}^s$, $\quad s = \log(n)$

$$\tilde{a}(\vec{y}) = \sum_{\vec{x}\in\{0,1\}^s} a_i \cdot \widetilde{eq}(\vec{x},\vec{y})$$ Lagrange Polynomial

$$\widetilde{eq}(\vec{x},\vec{y}) = \prod_i [x_i y_i + (1-x_i)\cdot(1-y_i)]$$

$\tilde{a}(x)$ is the encoding of $\vec{a}$

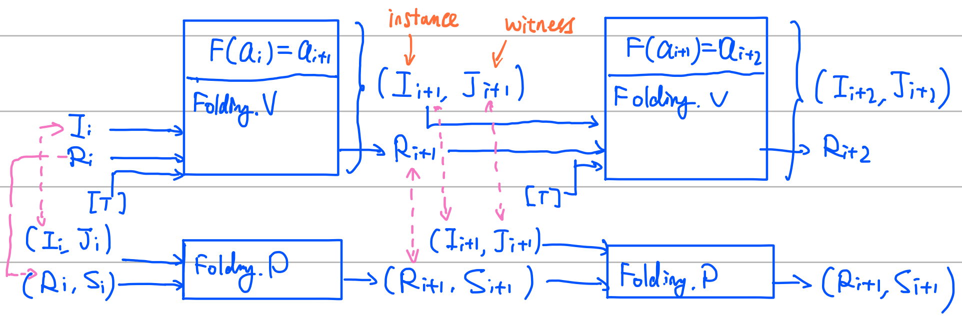
Sumcheck can reduce sumation to polynomial evaluation:

$$\sum_{\vec{x}\in\{0,1\}^s} \tilde{a}(\vec{x}) \stackrel{?}{=} h$$

$$\Uparrow$$

$$\tilde{a}(\vec{r}) \stackrel{?}{=} h'$$

#3: Revisit Nova. (IVC scheme)



#4: Multi-Folding Scheme.

Incremental Instance-Witness: $(\vec{x}_1, [\vec{W}_1]; \vec{W}_1)$ | $\vec{z}_1 = (\vec{x}_1, 1, \vec{W}_1)$

Running Instance-Witness: $(\vec{x}_2, [\vec{W}_2], u, \vec{r}, \bar{V}_A, \bar{V}_B, \bar{V}_C; \vec{W}_2)$ | $\vec{z}_2 = (\vec{x}_2, u, \vec{W}_2)$

Folding. P — Folding. V

$$\xleftarrow{\alpha,\ \vec{\beta} \in \mathbb{F}^s}$$

$$G(\vec{x}) \triangleq Q(\vec{x}) + \alpha \cdot L_A(\vec{x}) + \alpha^2 \cdot L_B(\vec{x}) + \alpha^3 \cdot L_C(\vec{x})$$

$$\bar{V}_A \stackrel{?}{=} L_A(\vec{x}) \triangleq \widetilde{eq}(\vec{r}, \vec{x}) \cdot \widetilde{V}_{A,2}(\vec{x})$$

$$\bar{V}_B \stackrel{?}{=} L_B(\vec{x}) \triangleq \widetilde{eq}(\vec{r}, \vec{x}) \cdot \widetilde{V}_{B,2}(\vec{x})$$

$$\bar{V}_C \stackrel{?}{=} L_C(\vec{x}) \triangleq \widetilde{eq}(\vec{r}, \vec{x}) \cdot \widetilde{V}_{C,2}(\vec{x})$$

Lin-check

$$0 \stackrel{?}{=} Q(\vec{x}) \triangleq \widetilde{eq}(\vec{\beta}, \vec{x}) \cdot [\widetilde{V}_{A,1}(\vec{x}) \cdot \widetilde{V}_{B,1}(\vec{x}) - \widetilde{V}_{C,1}(\vec{x})]$$

Row-check

$$\begin{cases} \widetilde{V}_{A,1}(\vec{x}) = \sum_{\vec{y}} \widetilde{A}(\vec{x}, \vec{y}) \cdot \vec{z}_1(\vec{y}) & (A \cdot \vec{z}_1) \\ \widetilde{V}_{B,1}(\vec{x}) = \sum_{\vec{y}} \widetilde{B}(\vec{x}, \vec{y}) \cdot \vec{z}_1(\vec{y}) & (B \cdot \vec{z}_1) \\ \widetilde{V}_{C,1}(\vec{x}) = \sum_{\vec{y}} \widetilde{C}(\vec{x}, \vec{y}) \cdot \vec{z}(\vec{y}) & (C \cdot \vec{z}_1) \end{cases}$$

$$\begin{cases} \widetilde{V}_{A,2}(\vec{x}) = \sum_{\vec{y}} \widetilde{A}(\vec{x}, \vec{y}) \cdot \vec{z}_2 & (A \cdot \vec{z}_2) \\ \widetilde{V}_{B,2}(\vec{x}) = \sum_{\vec{y}} \widetilde{B}(\vec{x}, \vec{y}) \cdot \vec{z}_1 & (B \cdot \vec{z}_2) \\ \widetilde{V}_{C,2}(\vec{x}) = \sum_{\vec{y}} \widetilde{C}(\vec{x}, \vec{y}) \cdot \vec{z}_2 & (C \cdot \vec{z}_2) \end{cases}$$

sumcheck:

$$\sum_{\vec{x}} G(\vec{x}) \stackrel{?}{=} 0 + \alpha \cdot \bar{V}_A + \alpha^2 \cdot \bar{V}_B + \alpha^3 \cdot \bar{V}_C$$

$$\longleftrightarrow$$

$$G(\vec{r}') \stackrel{?}{=} h'$$

$$V_{A,1} = \widetilde{V}_{A,1}(\vec{r}')$$

$$V_{B,1} = \widetilde{V}_{B,1}(\vec{r}')$$

$$V_{C,1} = \widetilde{V}_{C,1}(\vec{r}')$$

$$V_{A,2} = \widetilde{V}_{A,2}(\vec{r}')$$

$$V_{B,2} = \widetilde{V}_{B,2}(\vec{r}')$$

$$V_{C,2} = \widetilde{V}_{C,2}(\vec{r}')$$

$$\xrightarrow{(V_{A,1},\ V_{B,1},\ V_{C,1},\ V_{A,2},\ V_{B,2},\ V_{C,2})}$$

$$e_1 = \widetilde{eq}(\vec{\beta}, \vec{r}')$$

$$e_2 = \widetilde{eq}(\vec{r}, \vec{r}')$$

$$\begin{cases} \alpha \cdot e_2 \cdot V_{A,2} + \alpha^2 e_2 \cdot V_{B,2} + \alpha^3 \cdot e_2 \cdot V_{C,2} \stackrel{?}{=} h \\ (V_{A,1} \cdot V_{B,1} - V_{C,1}) \cdot e_1 \stackrel{?}{=} 0 \end{cases}$$

$$\xleftarrow{\rho}$$

$$[\vec{W}^*] = [\vec{W}_2] + \rho \cdot [\vec{W}_1]$$

$$\vec{x}^* = \vec{x}_2 + \rho \cdot \vec{x}_1$$

$$u^* = u_2 + \rho \cdot 1$$

$$\vec{W}^* = \vec{W}_2 + \rho \cdot \vec{W}_1$$

$$\vec{r}^* = \vec{r}'$$

$$\bar{V}_A^* = V_{A,2} + \rho \cdot V_{A,1}$$

$$\bar{V}_B^* = V_{B,2} + \rho \cdot V_{B,1}$$

$$\bar{V}_C^* = V_{C,2} + \rho \cdot V_{C,1}$$