THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

Department of Computing
電子計算學系

Realizing Polynomial Commitment Schemes

GAO Shang

2025/07/8

Univariant PCS - IPA

- Recall the univariant PCS relation:

$$\mathfrak{R} = \left\{ \begin{matrix} \text{witness: } f(X) \\ \text{public input: } F, z, v \end{matrix} \middle| \begin{matrix} F = Com(f) \\ v = f(z) \end{matrix} \right\}.$$

- $f(X) = f_0 + f_1 \cdot X + f_2 \cdot X^2 + \cdots + f_{N-1} \cdot X^{N-1}$.
  - $f(X)$ is determined by $f_0, \cdots, f_{N-1}$. Denoted as $\vec{f}$.
  - Denote $\vec{z} \coloneqq (1, z, z^2, \cdots, z^{N-1})$.

- Now $f(z) = \langle \vec{f}, \vec{z} \rangle$, allowing us to use an inner-product argument for $\langle \vec{f}, \vec{z} \rangle = v$.
  - Bulletproofs-IPA: $2 \log N$ proof size, linear proving/verification time.

[Bulletproofs]: https://eprint.iacr.org/2017/1066.pdf.

Univariant PCS - Quotient

- For $f(z) = v$, we have
$$f(X) - v = q(X) \cdot (X - z).$$
- This gives us a protocol:
  - $\mathcal{P} \to \mathcal{V}$: $q(X)$.
  - $\mathcal{V}$: Check $f(X) - v = q(X) \cdot (X - z)$.

- Improved protocol:
  - $\mathcal{P} \to \mathcal{V}$: $\mathrm{Com}\big(q(X)\big)$.
  - $\mathcal{V}$: Check $\Big(\mathrm{Com}\big(f(X)\big) - \mathrm{Com}(v)\Big) \cdot \mathrm{Com}(1) = \mathrm{Com}\big(q(X)\big) \cdot \mathrm{Com}(X - z)$.
  - KZG: $O(1)$ proof size/verification time, linear proving time (quasi linear when involving FFT).

[KZG]: https://eprint.iacr.org/2017/1066.pdf.

Multilinear PCS

- For a n-variant multilinear polynomial $f(X_0, \cdots, X_{n-1})$:
  - Coefficient form: $f_0 + f_1 X_0 + f_2 X_1 + \cdots + f_{2^n-1} X_0 X_1 \cdots X_{n-1} = \sum_{\vec{i} \in \{0,1\}^n} f_i \cdot \vec{X}^{\vec{i}}$.
  - Evaluation form: $f(0, \cdots 0) = f_0, \cdots, f(1, \cdots 1) = f_{2^n-1}. \sum_{\vec{i} \in \{0,1\}^n} f_i \cdot eq(\vec{i}, \vec{X})$.

Multilinear PCS - IPA

- Both can be regarded as an IPA $\langle \vec{f}, \vec{z} \rangle = v$.
  - Coefficient: $\vec{z} = (1, z_0, z_1, \cdots, z_0 z_1 \cdots z_{n-1})$.
  - Evaluation: $\vec{z} = \left(eq(\vec{0}, \vec{z}), \cdots, eq(\vec{1}, \vec{z}) \right)$.

- Let $m = \frac{n}{2}, N = 2^n, M = 2^m$.

Multilinear PCS - IPA

- Write $\vec{f}$ as a matrix: $\begin{bmatrix} f_0 & f_M & \cdots & f_{(M-1)M} \\ f_1 & f_{M+1} & \cdots & f_{(M-1)M+1} \\ \vdots & \vdots & \ddots & \vdots \\ f_{M-1} & f_{2M-1} & \cdots & f_{M^2-1} \end{bmatrix}$.

- $\langle \vec{f}, \vec{z} \rangle = [1 \quad z_0 \quad z_1 \quad z_0 z_1] \begin{bmatrix} f_0 & f_4 & f_8 & f_{15} \\ f_1 & f_5 & f_9 & f_{13} \\ f_2 & f_6 & f_{10} & f_{14} \\ f_3 & f_7 & f_{11} & f_{15} \end{bmatrix} \begin{bmatrix} 1 \\ z_2 \\ z_3 \\ z_2 z_3 \end{bmatrix}$.

Multilinear PCS - IPA

- $\mathcal{P} \to \mathcal{V}$: $[w_0 \quad w_1 \quad w_2 \quad w_3] = [1 \quad z_0 \quad z_1 \quad z_0 z_1] \begin{bmatrix} f_0 & f_4 & f_8 & f_{15} \\ f_1 & f_5 & f_9 & f_{13} \\ f_2 & f_6 & f_{10} & f_{14} \\ f_3 & f_7 & f_{11} & f_{15} \end{bmatrix}$.

- Now the verifier needs to check:
  - $[w_0 \quad w_1 \quad w_2 \quad w_3] \begin{bmatrix} 1 \\ z_2 \\ z_3 \\ z_2 z_3 \end{bmatrix} = v$, and
  - $[w_0 \quad w_1 \quad w_2 \quad w_3]$ is correctly computed.

Multilinear PCS - IPA

- $\mathcal{V} \to \mathcal{P}$: $\begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix} \leftarrow \mathbb{F}^4$.
- $\mathcal{P} \to \mathcal{V}$: $\begin{bmatrix} t_0 \\ t_1 \\ t_2 \\ t_3 \end{bmatrix} = \begin{bmatrix} f_0 & f_4 & f_8 & f_{15} \\ f_1 & f_5 & f_9 & f_{13} \\ f_2 & f_6 & f_{10} & f_{14} \\ f_3 & f_7 & f_{11} & f_{15} \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix}$.
- $\mathcal{V}$: Check $\begin{bmatrix} w_0 & w_1 & w_2 & w_3 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} 1 & z_0 & z_1 & z_0 z_1 \end{bmatrix} \begin{bmatrix} t_0 \\ t_1 \\ t_2 \\ t_3 \end{bmatrix}$.

Multilinear PCS - IPA

- The protocol requires the prover to send $\vec{w}, \vec{t}$, resulting $\mathrm{O}(M)$ proof size.

- Replace with IPA:
  - Bulletproofs: $O(\log M) = O(\log N)$ proof size, $O(M) = O(\sqrt{N})$ verification time.
  - KZG: $O(N) + O(N \log N) = O(N \log N)$ proving time $\Longrightarrow O(N) + O(M \log M) = O(N)$ proving time.

Multilinear PCS - IPA

- Bivariant sumcheck + Bulletproofs = Hyrax [2017/1132]
- Bivariant sumcheck + linear code = Brakedown [2021/1043]
- Bivariant sumcheck + KZG = MERCURY [2025/385]
- **Bivariant sumcheck + LaBRADOR = Greyhound [2024/1293]**

Multilinear PCS - IPA

- Sumcheck-based protocols provide a multinear $\rightarrow$ univariant polynomial transfer.

Multilinear PCS - Quotient

- For $f(\vec{z}) = v$, we have

$$f(\vec{X}) - v = \sum_{i=0}^{n-1} q_i(\vec{X}) \cdot (X_i - z_i)\,.$$

- This gives us a protocol:
  - $\mathcal{P} \to \mathcal{V}$: $q_i(X)$.
  - $\mathcal{V}$: Check $f(\vec{X}) - v = \sum_{i=0}^{n-1} q_i(\vec{X}) \cdot (X_i - z_i)$.

- Improved protocol:
  - $\mathcal{P} \to \mathcal{V}$: $\mathrm{Com}(q_i(X))$.
  - $\mathcal{V}$: Check $\left(\mathrm{Com}\left(f(\vec{X})\right) - \mathrm{Com}(v)\right) \cdot \mathrm{Com}(1) = \sum_{i=0}^{n-1} \mathrm{Com}\left(q_i(\vec{X})\right) \cdot \mathrm{Com}(X_i - z_i)$.
  - PST: $O(n) = O(\log N)$ proof size/verification time.

[PST]: https://eprint.iacr.org/2011/587.pdf.

Thanks!

Q&A