The Hong Kong Polytechnic University
香港理工大學

Department of Computing
電子計算學系

Greyhound: Fast Polynomial Commitments from Lattices

GAO Shang

2025/07/15

Inner and Outer Commitments

- To commitment r-many m-size $\mathcal{R}_q$ vectors $\vec{\boldsymbol{f}}_1, \cdots, \vec{\boldsymbol{f}}_r \in \mathcal{R}_q^m$:
  - Decompose each $\mathcal{R}_q$ element in $\vec{\boldsymbol{f}}_i$ to short vectors, resulting $\vec{\boldsymbol{s}}_i \in \mathcal{R}_q^{m\delta}$.
  - Commit each $\vec{\boldsymbol{s}}_i$ as $\vec{\boldsymbol{t}}_i = \boldsymbol{A}\vec{\boldsymbol{s}}_i \in \mathcal{R}_q^n$.
  - Decompose each $\mathcal{R}_q$ element in $\vec{\boldsymbol{t}}_i$ to short vectors, resulting $\vec{\boldsymbol{t}}'_i \in \mathcal{R}_q^{n\delta}$.
  - Commit all $\vec{\boldsymbol{t}}'_i$ as $\vec{\boldsymbol{u}} = \boldsymbol{B}\left(\vec{\boldsymbol{t}}'_1, \cdots, \vec{\boldsymbol{t}}'_n\right) \in \mathcal{R}_q^n$.

Quadratic Relation

- Witness: $\left(\vec{\boldsymbol{s}}_i, \vec{\boldsymbol{t}}_i\right)_{i\in[r]}$.
- Public input: $\vec{\boldsymbol{u}} \in \mathcal{R}_q^n, \vec{\boldsymbol{a}} \in \mathcal{R}_q^m, \vec{\boldsymbol{b}} \in \mathcal{R}_q^r, y \in \mathbb{Z}_q$.
- Relation:

$$[- \ \vec{\boldsymbol{a}} \ -] \cdot \begin{bmatrix} | & & | \\ \vec{\boldsymbol{f}}_1 & \cdots & \vec{\boldsymbol{f}}_r \\ | & & | \end{bmatrix} \cdot \begin{bmatrix} | \\ \vec{\boldsymbol{b}} \\ | \end{bmatrix} = y;$$

$$\vec{\boldsymbol{f}}_i \coloneqq \boldsymbol{G}_m \vec{\boldsymbol{s}}_i; \quad \vec{\boldsymbol{t}}_i = \boldsymbol{A}\vec{\boldsymbol{s}}_i; \quad \vec{\boldsymbol{t}}_i \coloneqq \boldsymbol{G}_n \vec{\boldsymbol{t}}'_i; \quad \vec{\boldsymbol{u}} = \boldsymbol{B}\left(\vec{\boldsymbol{t}}'_1, \cdots, \vec{\boldsymbol{t}}'_n\right).$$

Simple Proof for Quadratic Relation

- Brakedown-like approach [GLS+21].
- $\mathcal{P} \to \mathcal{V}$: $[- \vec{\boldsymbol{w}} \ -] \coloneqq [- \vec{\boldsymbol{a}} \ -] \cdot \begin{bmatrix} | & & | \\ \vec{\boldsymbol{f}}_1 & \cdots & \vec{\boldsymbol{f}}_r \\ | & & | \end{bmatrix} \in \mathcal{R}_q^r$.
- $\mathcal{V} \to \mathcal{P}$: $\vec{c} \coloneqq (c_1, \cdots, c_r) \leftarrow \mathcal{C}^r$ (short challenge).
- $\mathcal{P} \to \mathcal{V}$: $\vec{\boldsymbol{t}}'_i, \vec{\boldsymbol{z}} \coloneqq \begin{bmatrix} | & & | \\ \vec{\boldsymbol{s}}_1 & \cdots & \vec{\boldsymbol{s}}_r \\ | & & | \end{bmatrix} \cdot \begin{bmatrix} | \\ \vec{c} \\ | \end{bmatrix} = \sum_{i=1}^{r} c_i \cdot \vec{\boldsymbol{s}}_i$.

Simple Proof for Quadratic Relation

- $\mathcal{V}$: Check

$$[-\ \vec{\boldsymbol{w}}\ -] \cdot \begin{bmatrix} | \\ \vec{\boldsymbol{b}} \\ | \end{bmatrix} = y; \quad [-\ \vec{\boldsymbol{w}}\ -] \cdot \begin{bmatrix} | \\ \vec{c} \\ | \end{bmatrix} = [-\ \vec{\boldsymbol{a}}\ -] \cdot \boldsymbol{G}_m \begin{bmatrix} | \\ \vec{\boldsymbol{z}} \\ | \end{bmatrix};$$

$$\vec{\boldsymbol{t}}_i \coloneqq \boldsymbol{G}_n \vec{\boldsymbol{t}}'_i; \quad \sum_{i=1}^{r} c_i \cdot \vec{\boldsymbol{t}}_i = \boldsymbol{A}\vec{\boldsymbol{z}}; \quad \vec{\boldsymbol{u}} = \boldsymbol{B}\left(\vec{\boldsymbol{t}}'_1, \cdots, \vec{\boldsymbol{t}}'_n\right),$$

$\vec{\boldsymbol{t}}'_i, \vec{\boldsymbol{z}}$ are short.

Reducing Proof Size

- Proof size is dominated by $\vec{\boldsymbol{w}} \in \mathcal{R}_q^r, \vec{\boldsymbol{t}}'_i \in \mathcal{R}_q^{n\delta}, \vec{\boldsymbol{z}} \in \mathcal{R}_q^r$.
- Recall LaBRADOR: $f(\vec{\boldsymbol{s}}_1, \dots, \vec{\boldsymbol{s}}_r) = \sum_{i,j=1}^r \boldsymbol{a}_{i,j} \langle \vec{\boldsymbol{s}}_i, \vec{\boldsymbol{s}}_j \rangle + \sum_{i=1}^r \langle \vec{\boldsymbol{\phi}}_i, \vec{\boldsymbol{s}}_j \rangle - \boldsymbol{b}$.

Reducing Proof Size

- Sending commitment of $\vec{\boldsymbol{w}}' \in \mathcal{R}_q^{r\delta}$ where $\vec{\boldsymbol{w}} \coloneqq \boldsymbol{G}_r \vec{\boldsymbol{w}}'$:
$$\vec{\boldsymbol{v}} = \boldsymbol{D}\vec{\boldsymbol{w}}'.$$
- Revealing $\vec{\boldsymbol{w}}'$ with $\vec{\boldsymbol{t}}'_i, \vec{\boldsymbol{z}}$ at the final step.
- The final inner-product check becomes:

$$\begin{bmatrix} \boldsymbol{D} & \vec{0} & \vec{0} \\ \vec{0} & \boldsymbol{B} & \vec{0} \\ \vec{\boldsymbol{b}}\boldsymbol{G}_r & \vec{0} & \vec{0} \\ \vec{c}\boldsymbol{G}_r & \vec{0} & -\vec{\boldsymbol{a}}\boldsymbol{G}_m \\ \vec{0} & \vec{c}\boldsymbol{G}_n & -\boldsymbol{A} \end{bmatrix} \begin{bmatrix} \vec{\boldsymbol{w}}' \\ \vec{\boldsymbol{t}}'_i \\ \vec{\boldsymbol{z}} \end{bmatrix} = \begin{bmatrix} \vec{\boldsymbol{v}} \\ \vec{\boldsymbol{u}} \\ y \\ \boldsymbol{0} \\ \boldsymbol{0} \end{bmatrix},$$

$\vec{\boldsymbol{w}}', \vec{\boldsymbol{t}}'_i, \vec{\boldsymbol{z}}$ are short.

Polynomial Commitment

- Prove $f(x) = \sum_{i=0}^{mr-1} f_i \cdot x^i = y$ over $\mathbb{Z}_q$.
  - $f(x) = [1, x, x^2, \cdots, x^{m-1}] \cdot \begin{bmatrix} f_0 & f_m & \cdots & f_{(r-1)m} \\ f_1 & f_{m+1} & \cdots & f_{(r-1)m+1} \\ \vdots & \vdots & \ddots & \vdots \\ f_{m-1} & f_{2m-1} & \cdots & f_{mr-1} \end{bmatrix} \cdot \begin{bmatrix} 1 \\ x^m \\ x^{2m} \\ \vdots \\ x^{(r-1)m} \end{bmatrix}$.
- Caveats:
  - f_i's may not be short.
  - The polynomial and evaluation point are in $\mathbb{Z}_q$.

HyperWolf

- The Greyhound's "simple proof for quadratic relation" splits $\vec{f}$ into a 2-dimensional matrix to get $\sim 2\sqrt{N}$ size and verifier complexity (excluding $\vec{\boldsymbol{t}}'_i$).

- Now let's split into a k-dimensional hypercube.
  - Resulting $O\left(kN^{1/k}\right)$ size and verifier complexity. $O(\log N)$ when $k = \log N$.
  - No need to run LaBRADOR (the protocol itself is recursive).

- Same structure for multilinear polynomials (i.e., sumcheck).

- https://eprint.iacr.org/2025/922.

HyperWolf

- $\mathcal{P} \rightarrow \mathcal{V}$: $\begin{bmatrix} 1 & x_1 & x_2 & x_1x_2 \end{bmatrix} \cdot \underbrace{\begin{bmatrix} & \\ & \\ & \\ & \end{bmatrix}}_{F} = \begin{bmatrix} w_1 & w_2 \end{bmatrix}$
- $\mathcal{V}$: Check $\begin{bmatrix} w_1 & w_2 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ x_3 \end{bmatrix} = \begin{bmatrix} y \end{bmatrix}$
- $\mathcal{V} \rightarrow \mathcal{P}$: $\begin{bmatrix} c_1 \\ c_2 \end{bmatrix}$
- Now reduced to: $\begin{bmatrix} 1 & x_1 & x_2 & x_1x_2 \end{bmatrix} \cdot \underbrace{\begin{bmatrix} & \\ & \\ & \\ & \end{bmatrix}}_{F} \cdot \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} w_1 & w_2 \end{bmatrix} \cdot \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}$

$$f(x_1, x_2, x_3) = f_1 + f_2x_1 + f_3x_2 + f_4x_1x_2 + f_5x_3 + f_6x_1x_3 + f_7x_2x_3 + f_8x_1x_2x_3 = y$$

HyperWolf

- $\mathcal{P} \to \mathcal{V}$: $\begin{bmatrix} 1 & x_1 & x_2 & x_1x_2 \end{bmatrix} \cdot \underbrace{\begin{bmatrix} & \\ & \\ & \\ & \end{bmatrix}}_{F} = \begin{bmatrix} w_1 & w_2 \end{bmatrix}$
- $\mathcal{V}$: Check $\begin{bmatrix} w_1 & w_2 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ x_3 \end{bmatrix} = \begin{bmatrix} y \end{bmatrix}$
- $\mathcal{V} \to \mathcal{P}$: $\begin{bmatrix} c_1 \\ c_2 \end{bmatrix}$
- Now reduced to: $\begin{bmatrix} 1 & x_1 & x_2 & x_1x_2 \end{bmatrix} \cdot \begin{bmatrix} g_1 \\ g_2 \\ g_3 \\ g_4 \end{bmatrix} = \begin{bmatrix} y_g \end{bmatrix}$

$$f(x_1, x_2, x_3) = f_1 + f_2x_1 + f_3x_2 + f_4x_1x_2 + f_5x_3 + f_6x_1x_3 + f_7x_2x_3 + f_8x_1x_2x_3 = y$$

HyperWolf

- $\mathcal{P} \to \mathcal{V}$: $\begin{bmatrix} 1 & x_1 \end{bmatrix} \cdot \begin{bmatrix} g_1 & g_3 \\ g_2 & g_4 \end{bmatrix} = \begin{bmatrix} u_1 & u_2 \end{bmatrix}$
- $\mathcal{V}$: Check $\begin{bmatrix} u_1 & u_2 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ x_2 \end{bmatrix} = \begin{bmatrix} y_g \end{bmatrix}$
- $\mathcal{V} \to \mathcal{P}$: $\begin{bmatrix} c_3 \\ c_4 \end{bmatrix}$
- $\mathcal{P} \to \mathcal{V}$: $\begin{bmatrix} g_1 & g_3 \\ g_2 & g_4 \end{bmatrix} \cdot \begin{bmatrix} c_3 \\ c_4 \end{bmatrix} = \begin{bmatrix} h_1 \\ h_2 \end{bmatrix}$
- $\mathcal{V}$: Check $\begin{bmatrix} 1 & x_1 \end{bmatrix} \cdot \begin{bmatrix} h_1 \\ h_2 \end{bmatrix} = \begin{bmatrix} u_1 & u_2 \end{bmatrix} \cdot \begin{bmatrix} c_3 \\ c_4 \end{bmatrix}$

$$f(x_1, x_2, x_3) = f_1 + f_2 x_1 + f_3 x_2 + f_4 x_1 x_2 + f_5 x_3 + f_6 x_1 x_3 + f_7 x_2 x_3 + f_8 x_1 x_2 x_3 = y$$

Thanks!

Q&A