



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 $\overrightarrow{f}_1, \dots, \overrightarrow{f}_r \in \mathcal{R}_q^m$:
 - Decompose each \mathcal{R}_q element in \overrightarrow{f}_i to short vectors, resulting $\overrightarrow{s}_i \in \mathcal{R}_q^{m\delta}$.

• Commit each \vec{s}_i as $\vec{t}_i = A\vec{s}_i \in \mathcal{R}_q^n$.

• Decompose each \mathcal{R}_q element in \vec{t}_i to short vectors, resulting $\vec{t}'_i \in \mathcal{R}_q^{n\delta}$.

• Commit all \vec{t}'_i as $\vec{u} = B(\vec{t}'_1, \dots, \vec{t}'_n) \in \mathcal{R}_q^n$.

Quadratic Relation

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

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

$$\vec{f}_i \coloneqq G_m \vec{s}_i; \quad \vec{t}_i = A \vec{s}_i; \quad \vec{t}_i \coloneqq G_n \vec{t}'_i; \quad \vec{u} = B(\vec{t}'_1, \dots, \vec{t}'_n).$$

Simple Proof for Quadratic Relation

• Brakedown-like approach [GLS+21].

$$\boldsymbol{\cdot} \ \mathcal{P} \to \mathcal{V} \colon [-\overrightarrow{\boldsymbol{w}} \ -] \coloneqq [-\overrightarrow{\boldsymbol{a}} \ -] \cdot \begin{bmatrix} | & & | \\ \overrightarrow{\boldsymbol{f}}_1 & \cdots & \overrightarrow{\boldsymbol{f}}_r \\ | & & | \end{bmatrix} \in \mathcal{R}_q^r.$$

• $\mathcal{V} \to \mathcal{P}$: $\vec{c} \coloneqq (c_1, \dots, c_r) \leftarrow \mathcal{C}^r$ (short challenge).

$$\cdot \mathcal{P} \to \mathcal{V}: \vec{t}'_i, \vec{z} \coloneqq \begin{bmatrix} | & & | \\ \vec{s}_1 & \cdots & \vec{s}_r \\ | & & | \end{bmatrix} \cdot \begin{bmatrix} | \\ \vec{c} \\ | \end{bmatrix} = \sum_{i=1}^r c_i \cdot \vec{s}_i.$$

Simple Proof for Quadratic Relation

• \mathcal{V} : Check

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

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

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

Reducing Proof Size

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

Reducing Proof Size

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

$$\begin{bmatrix} \mathbf{D} & \overrightarrow{0} & \overrightarrow{0} & \overrightarrow{0} \\ \overrightarrow{0} & \mathbf{B} & \overrightarrow{0} \\ \overrightarrow{b} \mathbf{G}_{r} & \overrightarrow{0} & \overrightarrow{0} \\ \overrightarrow{c} \mathbf{G}_{r} & \overrightarrow{0} & -\overrightarrow{a} \mathbf{G}_{m} \\ \overrightarrow{0} & \overrightarrow{c} \mathbf{G}_{n} & -A \end{bmatrix} \begin{bmatrix} \overrightarrow{w}' \\ \overrightarrow{t}'_{i} \\ \overrightarrow{z} \end{bmatrix} = \begin{bmatrix} \overrightarrow{v} \\ \overrightarrow{u} \\ y \\ \mathbf{0} \\ \mathbf{0} \end{bmatrix},$$

$$\overrightarrow{w}', \overrightarrow{t}'_{i}, \overrightarrow{z} \text{ are short.}$$

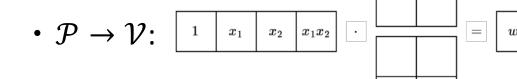
Polynomial Commitment

• Prove $f(x) = \sum_{i=0}^{mr-1} f_i \cdot x^i = y$ over \mathbb{Z}_q .

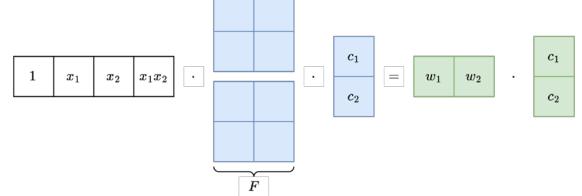
$$f(x) = [1, x, x^{2}, \dots, x^{m-1}] \cdot \begin{bmatrix} f_{0} & f_{m} & \cdots & f_{(r-1)m} \\ f_{1} & f_{m+1} & \cdots & f_{(r-1)m+1} \\ \vdots & \vdots & \ddots & \vdots \\ f_{m-1} & f_{2m-1} & \cdots & f_{mr-1} \end{bmatrix} \cdot \begin{bmatrix} 1 \\ \chi^{m} \\ \chi^{2m} \\ \vdots \\ \chi^{(r-1)m} \end{bmatrix}.$$

- Caveats:
 - f_i 's may not be short.
 - The polynomial and evaluation point are in \mathbb{Z}_q .

- 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{t}'_i).
- Now let's split into a k-dimensional hypercube.
 - Resulting $O(kN^{1/k})$ 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.

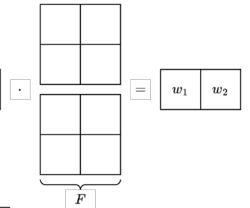


- $\mathcal{V} o \mathcal{P}$: $\frac{c_1}{c_2}$
- Now reduced to:

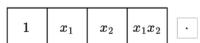


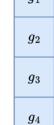
$$f(x_1, x_2, x_3) = f_1 + f_2 x_1 + f_3 x_2 + f_4 x_1 x_2 + f_5 x_3 + f_6 x_1 x_3 + f_7 x_2 x_3 + f_8 x_1 x_2 x_3 = y$$

• $\mathcal{P} o \mathcal{V}$: $\begin{bmatrix} 1 & x_1 & x_2 & x_1x_2 \end{bmatrix}$



- $\mathcal{V}\colon\mathsf{Check}\,\left[\begin{smallmatrix}w_1&w_2\\&&x_3\end{smallmatrix}\right]$ \sqsubseteq $\left[\begin{smallmatrix}y\\&&&\end{matrix}\right]$
- $m{\cdot}\; \mathcal{V} o \mathcal{P} \colon egin{bmatrix} rac{c_1}{c_2} \end{bmatrix}$
- Now reduced to:





11

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



•
$$\mathcal{V}\colon\mathsf{Check}$$
 u_1 u_2 v_3 v_4 v_2

•
$$\mathcal{V} o \mathcal{P}$$
: $\left| \begin{smallmatrix} c_3 \\ c_4 \end{smallmatrix} \right|$

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

Thanks!

