

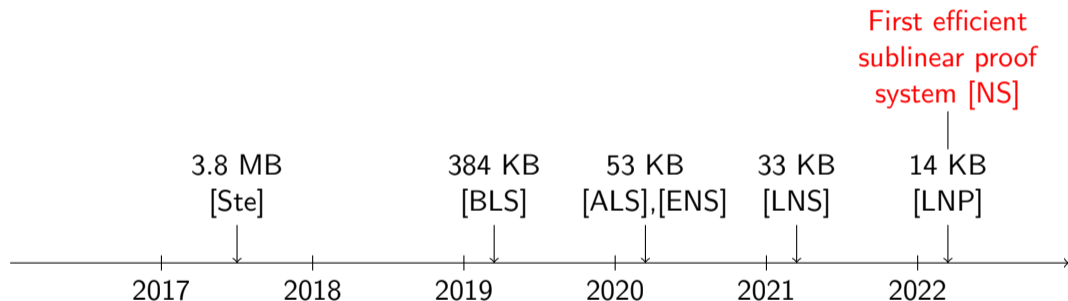
LaBRADOR: Compact proofs for R1CS from Module-SIS

Gregor Seiler, joint work with Ward Beullens

IBM Research Europe

Mai 1, 2023

Evolution of Linear-Sized Lattice-Based Proof Systems



Lattice-Based Recursively Amortized Demonstrations Of R1CS

R1CS Principal Relation

Parameterized by a rank n and a multiplicity r

Witness consists of r (polynomial) vectors $\mathbf{s}_1, \dots, \mathbf{s}_r$ of rank n that fulfill many dot-product constraints

$$f^{(k)}(\mathbf{s}_1, \dots, \mathbf{s}_r) = \sum_{i,j} \mathbf{a}_{ij}^{(k)} \langle \mathbf{s}_i, \mathbf{s}_j \rangle + \sum_i \langle \boldsymbol{\varphi}_i^{(k)}, \mathbf{s}_i \rangle + \mathbf{b}^{(k)} = \mathbf{0},$$

and a norm constraint

$$\|\mathbf{s}_1\|^2 + \dots + \|\mathbf{s}_r\|^2 \leq \beta^2$$

Protocol can be seen as a chain of sub-protocols that transform the relation into new instances with smaller parameters

Inner Commitments

Need commitments to \mathbf{s}_i for sound transformations of relation

- ▶ Prover sends $\mathbf{t}_i = \mathbf{A}\mathbf{s}_i$ for $i = 1, \dots, r$

Note: All commitments share same matrix \mathbf{A} (commitment key)

Current Relation

Witness:

$$\mathbf{s}_1, \dots, \mathbf{s}_r$$

Constraints:

$$f^{(k)}(\mathbf{s}_1, \dots, \mathbf{s}_r) = \mathbf{0} \quad \text{for } k = 1, \dots, K$$

$$\mathbf{A}\mathbf{s}_i = \mathbf{t}_i \quad \text{for } i = 1, \dots, r$$

$$\|\mathbf{s}_1\|^2 + \dots + \|\mathbf{s}_r\|^2 \leq \beta$$

Outer Commitments

Sending lattice commitments is very expensive ($\approx 4\text{KB}$ per commitment)

Idea: Hide inner commitments \mathbf{t}_i in an outer commitment

$$\mathbf{u} = \sum_{i,k} \mathbf{B}_{ik} \mathbf{t}_i^{(k)} \quad \text{where} \quad \mathbf{t}_i = \mathbf{t}_i^{(0)} + b\mathbf{t}_i^{(1)} \dots + b^{(t-1)}\mathbf{t}_i^{(t-1)} \quad \text{with} \quad \|\mathbf{t}_i^{(k)}\|_{\infty} \leq \frac{b}{2}$$

Outer commitment needs to account for less slack; hence much smaller

Current Relation

Witness:

$$\mathbf{s}_1, \dots, \mathbf{s}_r, \mathbf{t}_1^{(0)}, \dots, \mathbf{t}_1^{(t-1)}, \dots, \mathbf{t}_r^{(0)}, \dots, \mathbf{t}_r^{(t-1)}$$

Constraints:

$$f^{(k)}(\mathbf{s}_1, \dots, \mathbf{s}_r) = \mathbf{0} \quad \text{for } k = 1, \dots, K + 1$$

$$\mathbf{A}\mathbf{s}_i = \mathbf{t}_i \quad \text{for } i = 1, \dots, r$$

$$\sum_{i,k} \mathbf{B}_{ik} \mathbf{t}_i^{(k)} = \mathbf{u}$$

$$\|\mathbf{s}_1\|^2 + \dots + \|\mathbf{s}_r\|^2 \leq \beta^2$$

$$\sum_{i,k} \|\mathbf{t}_i^{(k)}\|^2 \leq \beta'^2$$

Johnson-Lindenstrauss Projection

Recall: Certain random linear maps from a high-dimensional into a low-dimensional vector space preserve the ℓ_2 -norm up to small constants

- ▶ Verifier sends random matrices Π_i
- ▶ Prover sends projection $\vec{p} = \sum_i \Pi_i \vec{s}_i \in \mathbb{Z}_q^{256}$
- ▶ Verifier checks $\|\vec{p}\| \leq \sqrt{128}\beta$

Current Relation

Witness:

$$\mathbf{s}_1, \dots, \mathbf{s}_r, \mathbf{t}_1^{(0)}, \dots, \mathbf{t}_1^{(t-1)}, \dots, \mathbf{t}_r^{(0)}, \dots, \mathbf{t}_r^{(t-1)}$$

Constraints:

$$f^{(k)}(\mathbf{s}_1, \dots, \mathbf{s}_r) = \mathbf{0} \quad \text{for } k = 1, \dots, K$$
$$f^{(K+k)}(\vec{s}_1, \dots, \vec{s}_r) = \sum_i \langle \vec{\pi}_i^{(k)}, \vec{s}_i \rangle - p_k = 0 \quad \text{for } k = 1, \dots, 256$$

$$\mathbf{A}\mathbf{s}_i = \mathbf{t}_i \quad \text{for } i = 1, \dots, r$$

$$\sum_{i,k} \mathbf{B}_{ik} \mathbf{t}_i^{(k)} = \mathbf{u}$$

$$\|\mathbf{s}_1\|^2 + \dots + \|\mathbf{s}_r\|^2 \leq \beta^2$$

$$\sum_{i,k} \|\mathbf{t}_i^{(k)}\|^2 \leq \beta'^2$$

Aggregation

Randomly linear-combine dot-product constraints $f^{(k)}$ with uniform challenges

- ▶ Verifier sends challenges α_k
- ▶ Prover and verifier compute aggregated constraint

$$f(\mathbf{s}_1, \dots, \mathbf{s}_r) = \sum_{i,j} \mathbf{a}_{ij} \langle \mathbf{s}_i, \mathbf{s}_j \rangle + \sum_i \langle \varphi_i, \mathbf{s}_i \rangle + \mathbf{b} = \mathbf{0} \quad \text{where} \quad \begin{cases} \mathbf{a}_{ij} = \sum_k \alpha_k \mathbf{a}_{ij}^{(k)}, \\ \varphi_i = \sum_k \alpha_k \varphi_i^{(k)}, \\ \mathbf{b} = \sum_k \alpha_k \mathbf{b}^{(k)} \end{cases}$$

Current Relation

Witness:

$$\mathbf{s}_1, \dots, \mathbf{s}_r, \mathbf{t}_1^{(0)}, \dots, \mathbf{t}_1^{(t-1)}, \dots, \mathbf{t}_r^{(0)}, \dots, \mathbf{t}_r^{(t-1)}$$

Constraints:

$$f(\mathbf{s}_1, \dots, \mathbf{s}_r) = \mathbf{0}$$

$$\mathbf{A}\mathbf{s}_i = \mathbf{t}_i \quad \text{for } i = 1, \dots, r$$

$$\sum_{i,k} \mathbf{B}_{ik} \mathbf{t}_i^{(k)} = \mathbf{u}$$

$$\sum_i \|\mathbf{s}_i\|^2 + \sum_{i,k} \|\mathbf{t}_i^{(k)}\|^2 \leq \beta'^2$$

Amortization

Amortize over witness vectors \mathbf{s}_i

- ▶ Prover sends garbage polynomials $\mathbf{g}_{ij} = \langle \mathbf{s}_i, \mathbf{s}_j \rangle$ and $\mathbf{h}_{ij} = \langle \varphi_i, \mathbf{s}_j \rangle$
- ▶ Verifier sends challenge polynomials $\mathbf{c}_1, \dots, \mathbf{c}_r$
- ▶ Prover sends amortized opening

$$\mathbf{z} = \mathbf{c}_1 \mathbf{s}_1 + \mathbf{c}_2 \mathbf{s}_2 + \dots + \mathbf{c}_r \mathbf{s}_r$$

Current Relation

Witness:

$$\mathbf{z}, \mathbf{t}_i^{(k)}$$

Constraints:

$$\sum_{i,j} \mathbf{a}_{ij} \mathbf{g}_{ij} + \sum_i \mathbf{h}_{ii} + \mathbf{b} = \mathbf{0}$$

$$\langle \mathbf{z}, \mathbf{z} \rangle = \sum_{i,j} \mathbf{c}_i \mathbf{c}_j \mathbf{g}_{ij}$$

$$\langle \varphi, \mathbf{z} \rangle = \sum_{i,j} \mathbf{c}_i \mathbf{c}_j \mathbf{h}_{ij}$$

$$\mathbf{A}\mathbf{z} = \mathbf{c}_1 \mathbf{t}_1 + \cdots + \mathbf{c}_r \mathbf{t}_r$$

$$\sum_{i,k} \mathbf{B}_{ik} \mathbf{t}_i^{(k)} = \mathbf{u}$$

$$\|\mathbf{z}\|^2 + \sum_{i,k} \|\mathbf{t}_i^{(k)}\|^2 \leq \beta^{r^2}$$

Target Relation of Multiplicity 2

Witness:

$$\mathbf{z}, \mathbf{v} = \left(\mathbf{t}_i^{(k)} \right)$$

Constraints:

$$\sum_{i,j} \mathbf{a}_{ij} \mathbf{g}_{ij} + \sum_i \mathbf{h}_{ii} + \mathbf{b} = \mathbf{0}$$

$$\langle \mathbf{z}, \mathbf{z} \rangle = \sum_{i,j} \mathbf{c}_i \mathbf{c}_j \mathbf{g}_{ij}$$

$$\langle \varphi, \mathbf{z} \rangle = \sum_{i,j} \mathbf{c}_i \mathbf{c}_j \mathbf{h}_{ij}$$

$$\mathbf{A}\mathbf{z} = \mathbf{c}_1 \mathbf{t}_1 + \cdots + \mathbf{c}_r \mathbf{t}_r$$

$$\sum_{i,k} \mathbf{B}_{ik} \mathbf{t}_i^{(k)} = \mathbf{u}$$

$$\|\mathbf{z}\|^2 + \|\mathbf{v}\|^2 \leq \beta'^2$$

Decomposition in Rank

Before recursing the protocol, want to increase multiplicity and decrease rank

Decomposition in rank: Split vectors of rank n into r vectors of rank n/r :

$$\mathbf{z} = \mathbf{z}_1 \parallel \cdots \parallel \mathbf{z}_r$$

Quadratic term $\langle \mathbf{z}, \mathbf{z} \rangle$ transforms as

$$\langle \mathbf{z}, \mathbf{z} \rangle = \langle \mathbf{z}_1, \mathbf{z}_1 \rangle + \cdots + \langle \mathbf{z}_r, \mathbf{z}_r \rangle$$

Decomposition in Width

Amortization blows up standard deviation due to multiplication by challenge polynomials; consequently, lattice parameters need to increase to retain SIS-hardness

Decomposition in width:

$$\mathbf{z} = \mathbf{z}_0 + b\mathbf{z}_1 \text{ with } \|\mathbf{z}_0\|_\infty \leq \frac{b}{2}$$

Quadratic term $\langle \mathbf{z}, \mathbf{z} \rangle$ transforms as

$$\langle \mathbf{z}, \mathbf{z} \rangle = \langle \mathbf{z}_0, \mathbf{z}_0 \rangle + 2b\langle \mathbf{z}_0, \mathbf{z}_1 \rangle + b^2\langle \mathbf{z}_1, \mathbf{z}_1 \rangle$$

Matrix (\mathbf{a}_{ij}) was diagonal, now becomes tridiagonal

Lattice Bulletproofs?

Want to prove commitment $\mathbf{t} = \mathbf{A}\mathbf{s} = \mathbf{A}_0\mathbf{s}_0 + \mathbf{A}_1\mathbf{s}_1$ using folding $\mathbf{z} = \mathbf{s}_0 + \mathbf{c}\mathbf{s}_1$

Bulletproofs: Quadratic verification using bilinearity of commitment:

$$(\mathbf{A}_0 + \mathbf{c}\mathbf{A}_1)(\mathbf{s}_0 + \mathbf{c}\mathbf{s}_1) = \mathbf{A}_0\mathbf{s}_0 + \mathbf{c}(\mathbf{A}_0\mathbf{s}_1 + \mathbf{A}_1\mathbf{s}_0) + \mathbf{c}^2\mathbf{A}_1\mathbf{s}_1 = \mathbf{t} + \mathbf{c}\mathbf{t}_1 + \mathbf{c}^2\mathbf{t}_2$$

Generalization to n parts needs $O(n^2)$ garbage commitments

Amortization: Linear verification

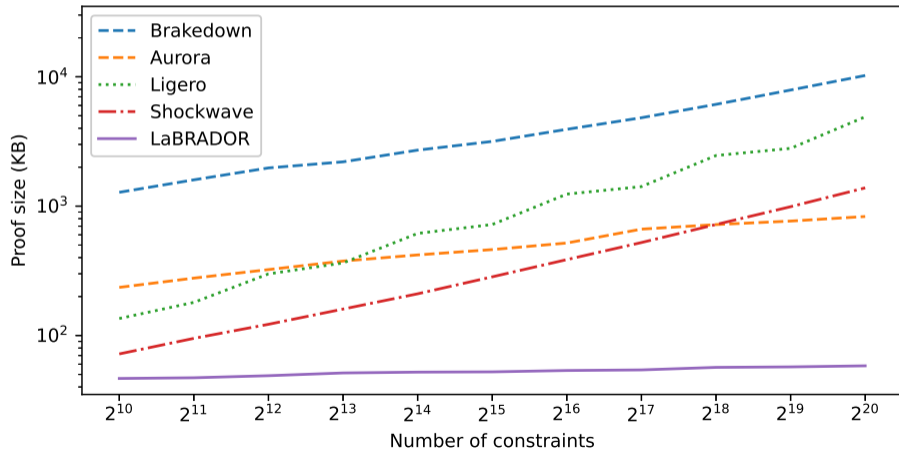
$$\mathbf{A}_0(\mathbf{s}_0 + \mathbf{c}\mathbf{s}_1) = \mathbf{A}_0\mathbf{s}_0 + \mathbf{A}_0\mathbf{s}_1 = \mathbf{t}_0 + \mathbf{c}\mathbf{t}_1$$

using only n “garbage commitments”. Doesn’t prove initial commitment \mathbf{t} , but fixes \mathbf{s} , so can collapse (“aggregate”) initial commitment to single polynomial and prove with $O(n^2)$ garbage polynomials (for free when aggregated together with relation constraints)

Results I: Proof sizes in Kilobytes for binary R1CS

| No. of constraints | 2^{20} | 2^{21} | 2^{22} | 2^{23} | 2^{24} | 2^{25} |
|--------------------|----------|----------|----------|----------|----------|----------|
| Proof Size | 49.02 | 49.37 | 51.47 | 51.6 | 52.7 | 53.84 |

Results II: R1CS mod $2^{64} + 1$



Thank you!