Lecture 8: IOP for R1CS and Polynomial Commitments

Zero-knowledge proofs

263-4665-00L

Lecturer: Jonathan Bootle

Announcements

- Graded homework posted.
- Deadline next Friday 24/11/2023 23:59 CET.
- Thanks to those who pointed out typos!
- I will post a new version shortly after today’s lecture.

- Next Friday’s lecture 24/11/2023 fully remote on Zoom.
- Don’t come in person. The room will be empty!
- Exercise session in person as usual.

Plan for the next few lectures

Sumcheck protocol ✓

Interactive proof for layered arithmetic circuits ✓

Interactive oracle proofs for general arithmetic circuits

$\text{DescriptionSize}(C) = N$

Indirect access to instance

V makes queries to instance

Commitments and polynomial commitments

ZK arguments for layered arithmetic circuits

ZK arguments for general arithmetic circuits

Rank 1 Constraint Systems (R1CS)

$$\mathcal{R}_{R1CS} = \left\{ \left((\mathbb{F}, A, B, C, \vec{x}), \vec{w} \right) : \begin{array}{c} A, B, C \in \mathbb{F}^{N_r \times N_c}, \vec{x} \in \mathbb{F}^k \\ \vec{w} \in \mathbb{F}^{N_c - k}, \vec{z} := \vec{x} || \vec{w} \\ A\vec{z} \circ B\vec{z} = C\vec{z} \end{array} \right\}.$$

$\vec{x}$ makes the problem non-trivial

entry-wise product

- **NP**-complete. Exercise: reduce SAT to R1CS.
- N gates $\Rightarrow O(N) \times O(N)$ matrices with $O(N)$ non-zero entries.

Multivariate, $\widetilde{EQ}$-basis. Based on Spartan paper

- We will construct a *holographic* IOP with *polynomial* queries for $\mathcal{R}_{R1CS}$.
- Verifier complexity $O(\ell + N_{in}) = O(\log N + N_{in})$ $\mathbb{F}$-ops.
- Query complexity $O(1)$ (to $\tilde{A}, \tilde{B}, \tilde{C}, \tilde{z}$, other message vectors).
- Prover complexity $O(N + |A| + |B| + |C|)$ $\mathbb{F}$-ops.

Set $N_r = N_c = N = 2^\ell, N_{in} = 2^{\ell_{in}}$

Preprocessing computes MLEs $\tilde{A}, \tilde{B}, \tilde{C}$

Holographic polynomial IOP for R1CS

$$((\mathbb{F}, A, B, C, \vec{x}), \vec{w}) \in \mathcal{R}_{R1CS}$$

$$\Updownarrow$$

$$\vec{z} = \vec{x}||\vec{w}, A\vec{z} \circ B\vec{z} = C\vec{z}$$

$$\Updownarrow$$

$\exists \vec{z}, \vec{z}_A, \vec{z}_B, \vec{z}_C \in \mathbb{F}^N$ such that

$P(A, B, C, \vec{x}, \vec{z})$ $\xrightarrow{\tilde{z}, \tilde{z}_A, \tilde{z}_B, \tilde{z}_C}$ $V^{\tilde{A}, \tilde{B}, \tilde{C}}(\vec{x})$

Row check:	Lincheck:	Input check:
$\vec{z}_A \circ \vec{z}_B = \vec{z}_C$	$\vec{z}_M = M\vec{z}$ $M \in \{A, B, C\}$	$\vec{z} = \vec{x}\|\|\vec{w}$ for some $\vec{w}$

Run parallel IOP subprotocols

Completeness:

If each IOP subprotocol is perfectly complete, so is the whole IOP.

Soundness:

- If $(\mathbb{F}, A, B, C, \vec{x}) \notin \mathcal{L}_{R1CS}$, then for all $\forall \vec{z}, \vec{z}_A, \vec{z}_B, \vec{z}_C \in \mathbb{F}^N$, at least one of the checks fails.
- Soundness follows from IOP subprotocol soundness.

Polynomial IOP for row-check

Communication, verifier complexity

$$p\left(\vec{X}\right) := \left(\tilde{z}_A\left(\vec{X}\right) \cdot \tilde{z}_B\left(\vec{X}\right) - \tilde{z}_C\left(\vec{X}\right)\right) \cdot \widetilde{\mathrm{EQ}}\left(\vec{X}; \vec{r}\right)$$

$p\left(\vec{X}\right)$ has ℓ variables, $d = 3$

Reduction strategy:

$$\sum_{\vec{j} \in \{0,1\}^\ell} \left(\tilde{z}_A(\vec{j}) \cdot \tilde{z}_B(\vec{j}) - \tilde{z}_C(\vec{j})\right) \cdot \widetilde{\mathrm{EQ}}(\vec{j}; \vec{r}) = \sum_{\vec{j} \in \{0,1\}^\ell} p(\vec{j}) = 0.$$

Sumcheck costs $O(\ell)$

$O(\ell)$ $\mathbb{F}$-ops to evaluate $\widetilde{\mathrm{EQ}}$

Total costs $O(\ell)$

Claim: $\vec{z}_A \circ \vec{z}_B = \vec{z}_C$

$P(\vec{z}_A, \vec{z}_B, \vec{z}_C)$

$V^{\vec{z}_A, \vec{z}_B, \vec{z}_C}$

$\vec{r} \leftarrow_\$ \mathbb{F}^\ell$

Sumcheck for $\sum_{\vec{j} \in \{0,1\}^\ell} p(\vec{j}) = 0$

V randomness $\vec{s} \in \mathbb{F}^\ell$

ℓ rounds

Claim:

$$\left(\tilde{z}_A(\vec{s}) \cdot \tilde{z}_B(\vec{s}) - \tilde{z}_C(\vec{s})\right) \cdot \widetilde{\mathrm{EQ}}(\vec{s}; \vec{r}) == v$$

Query complexity 3

Obtain using queries to $\tilde{z}_A, \tilde{z}_B, \tilde{z}_C$

Compute $\widetilde{\mathrm{EQ}}(\vec{s}; \vec{r})$ from scratch

Polynomial IOP for row-check, completeness

If $\vec{z}_A \circ \vec{z}_B = \vec{z}_C$ then $\forall \vec{i} \in \{0,1\}^\ell$, $\tilde{z}_A(\vec{i}) \cdot \tilde{z}_B(\vec{i}) - \tilde{z}_C(\vec{i}) = 0$.

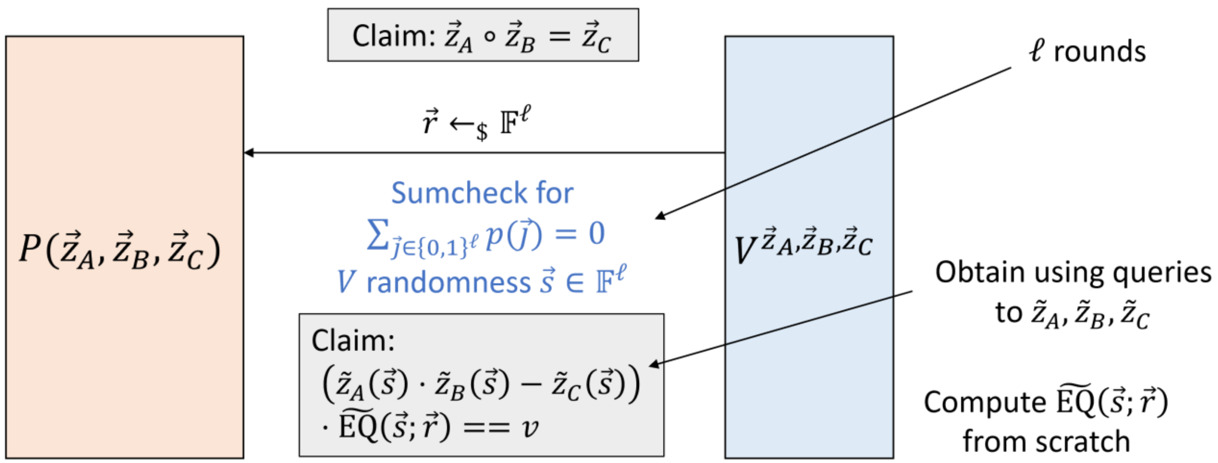
"$\tilde{z}_A(\vec{r}) \cdot \tilde{z}_B(\vec{r}) = \tilde{z}_C(\vec{r})$" isn't true

$\Rightarrow \sum_{\vec{j} \in \{0,1\}^\ell} \left(\tilde{z}_A(\vec{j}) \cdot \tilde{z}_B(\vec{j}) - \tilde{z}_C(\vec{j})\right) \cdot \widetilde{\mathrm{EQ}}(\vec{j}; \vec{i}) = 0$.

The L.H.S and R.H.S are *both* MLEs of 0.

- By uniqueness of MLEs, they are equal as polynomials in $\vec{i}$.
- Therefore we still have equality at $\vec{r} \in \mathbb{F}^\ell$ *outside* $\{0,1\}$.

$\Rightarrow \sum_{\vec{j} \in \{0,1\}^\ell} \left(\tilde{z}_A(\vec{j}) \cdot \tilde{z}_B(\vec{j}) - \tilde{z}_C(\vec{j})\right) \cdot \widetilde{\mathrm{EQ}}(\vec{j}; \vec{r}) = 0$.



- $\left(\tilde{z}_A(\vec{s}) \cdot \tilde{z}_B(\vec{s}) - \tilde{z}_C(\vec{s})\right) \cdot \widetilde{\mathrm{EQ}}(\vec{s}; \vec{r}) = v$ by sumcheck completeness, and sumcheck checks pass.
- V's check of the final claim passes by the previous line, correctness of received query answers, and correct computation of $\widetilde{\mathrm{EQ}}(\vec{s}; \vec{r})$.

Polynomial IOP for row-check, soundness

If $\vec{z}_A \circ \vec{z}_B \neq \vec{z}_C$ then $\exists \vec{\imath} \in \{0,1\}^\ell$, $\tilde{z}_A(\vec{\imath}) \cdot \tilde{z}_B(\vec{\imath}) - \tilde{z}_C(\vec{\imath}) \neq 0$.

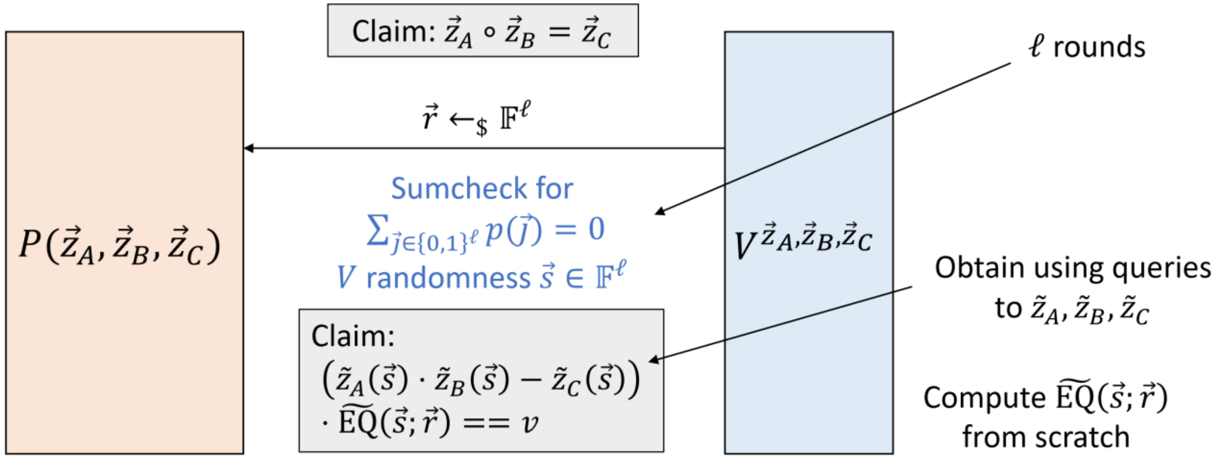
$\Rightarrow \sum_{\vec{\jmath} \in \{0,1\}^\ell} \left(\tilde{z}_A(\vec{\jmath}) \cdot \tilde{z}_B(\vec{\jmath}) - \tilde{z}_C(\vec{\jmath})\right) \cdot \widetilde{\mathrm{EQ}}(\vec{\jmath}; \vec{\imath}) \neq 0$.

The L.H.S and R.H.S are *not* equal as

polynomials in $\vec{\imath}$.

$\Rightarrow \sum_{\vec{\jmath} \in \{0,1\}^\ell} \left(\tilde{z}_A(\vec{\jmath}) \cdot \tilde{z}_B(\vec{\jmath}) - \tilde{z}_C(\vec{\jmath})\right) \cdot \widetilde{\mathrm{EQ}}(\vec{\jmath}; \vec{r}) \neq 0$

except w.p. $\leq \ell / |\mathbb{F}|$ by the Schwarz-Zippel Lemma.



- $\left(\tilde{z}_A(\vec{s}) \cdot \tilde{z}_B(\vec{s}) - \tilde{z}_C(\vec{s})\right) \cdot \widetilde{\mathrm{EQ}}(\vec{s}; \vec{r}) \neq v$

(or one of V's sumcheck checks fails) except w.p. $3\ell / |\mathbb{F}|$ by sumcheck soundness.

- In this case, V's check of the final claim *fails* by the previous line, correctness of received query answers, and correct computation of $\widetilde{\mathrm{EQ}}(\vec{s}; \vec{r})$.

Row-check prover complexity (table method)

$$p\left(\vec{X}\right) := \left(\tilde{z}_A\left(\vec{X}\right) \cdot \tilde{z}_B\left(\vec{X}\right) - \tilde{z}_C\left(\vec{X}\right)\right) \cdot \widetilde{\mathrm{EQ}}\left(\vec{X}; \vec{r}\right)$$

- This time $d + 1 = 4 > 2 = |H|$. Previous algorithm won't work.
- $p\left(\vec{X}\right)$ is too big to store if we want $O(N)$ running time.

Goal: $q_1(X_1) := \sum_{\vec{\omega} \in H^{\ell-1}} p(X_1, \omega_2, .., \omega_\ell)$

$\{q_1(j)\}_{j \in [d+1]}$ defines $q_1(X_1)$

Known from $\vec{z}_A, \vec{z}_B, \vec{z}_C$

Compute in N ops

$\left\{\tilde{z}_A(j, \vec{\omega}), \tilde{z}_B(j, \vec{\omega}), \tilde{z}_C(j, \vec{\omega}), \widetilde{\mathrm{EQ}}(j, \vec{\omega}; \vec{r})\right\}_{j \in \{0,1\}, \vec{\omega} \in H^{\ell-1}}$ Evaluation table

$\boxed{O(d^2|H|^{\ell-1}) \text{ ops for } q_1 \quad \text{Recurse for } O\left(d^2|H|^\ell\right) = O(N) \text{ total}}$

Interpolate in X_1, $O(d|H|^{\ell-1})$ ops

$\left\{\tilde{z}_A(X_1, \vec{\omega}), \tilde{z}_B(X_1, \vec{\omega}), \tilde{z}_C(X_1, \vec{\omega}), \widetilde{\mathrm{EQ}}(X_1, \vec{\omega}; \vec{r})\right\}_{\vec{\omega} \in H^{\ell-1}}$

Evaluate at d points, $O(d^2|H|^{\ell-1})$ ops

$\left\{\tilde{z}_A(j, \vec{\omega}), \tilde{z}_B(j, \vec{\omega}), \tilde{z}_C(j, \vec{\omega}), \widetilde{\mathrm{EQ}}(j, \vec{\omega}; \vec{r})\right\}_{j \in [d+1], \vec{\omega} \in H^{\ell-1}}$

Eval at s_1, $O(d|H|^{\ell-1})$ ops

$\left\{\tilde{z}_A(s_1, \vec{\omega}), \tilde{z}_B(s_1, \vec{\omega}), \tilde{z}_C(s_1, \vec{\omega}), \widetilde{\mathrm{EQ}}(s_1, \vec{\omega}; \vec{r})\right\}_{\vec{\omega} \in H^{\ell-1}}$

Table for next sumcheck iteration

Combine, $O(d|H|^{\ell-1})$ ops

$\{p(j, \vec{\omega})\}_{j \in [d+1], \vec{\omega} \in H^{\ell-1}} \longrightarrow \{q_1(j)\}_{j \in [d+1]}$

Polynomial IOP for lin-check

$$p\left(\vec{X}\right) := \widetilde{M}(\vec{r},\vec{X}) \cdot \tilde{z}(\vec{X})$$

Reduction strategy:

$\sum_{\vec{j}\in\{0,1\}^{\ell}} \widetilde{M}(\vec{r},\vec{j}) \cdot \tilde{z}(\vec{j}) = \tilde{z}_M(\vec{r})$.

Communication, verifier complexity

$p\left(\vec{X}\right)$ has ℓ variables, $d = 2$

Sumcheck costs $O(\ell)$
$O(\ell)$ $\mathbb{F}$-ops to evaluate $\widetilde{\mathrm{EQ}}$
Total costs $O(\ell)$

Claim: $M\vec{z} = \vec{z}_M$

$P(M,\vec{z},\vec{z}_M)$

$V^{M,\vec{z},\vec{z}_M}$

$\vec{r} \leftarrow_{\$} \mathbb{F}^{\ell}$

Query $\tilde{z}_M(\vec{r})$

Sumcheck for
$\sum_{\vec{j}\in\{0,1\}^{\ell}} p(\vec{j}) = 0$
V randomness $\vec{s} \in \mathbb{F}^{\ell}$

ℓ rounds

Claim:
$\widetilde{M}(\vec{r},\vec{s}) \cdot \tilde{z}(\vec{s}) == v$

Obtain using queries to $\widetilde{M}, \tilde{z}$

Query complexity 3

Polynomial IOP for lin-check, completeness

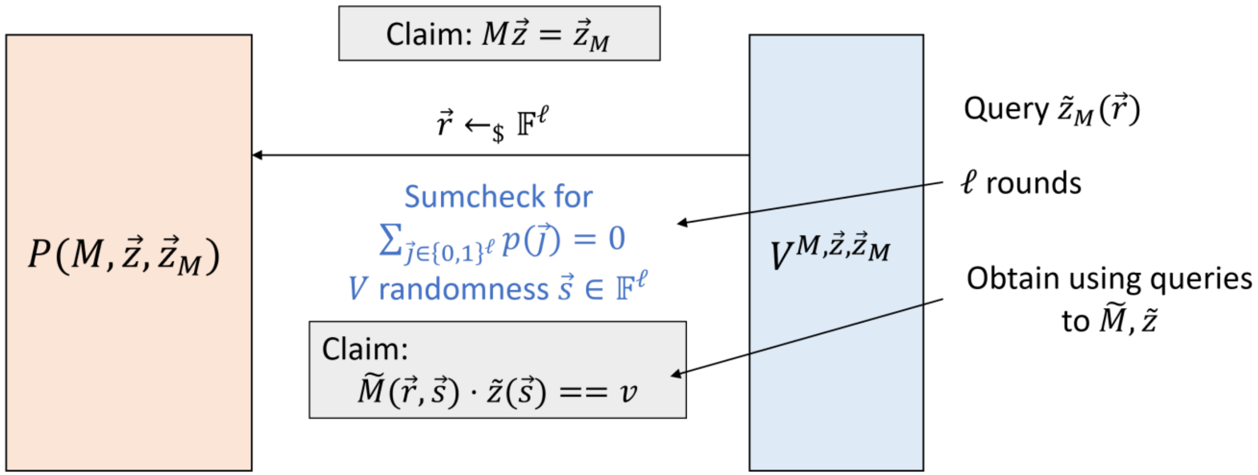
If $M\vec{z} = \vec{z}_M$ then $\forall \vec{\imath} \in \{0,1\}^\ell$, $\sum_{\vec{\jmath} \in \{0,1\}^\ell} M_{\vec{\imath},\vec{\jmath}} \cdot z_{\vec{\jmath}} = z_{M,\vec{\imath}}$ (explicit formula for matrix-vector multiplication)

$\sum_{\vec{\jmath} \in \{0,1\}^\ell} \widetilde{M}(\vec{\imath},\vec{\jmath}) \cdot \tilde{z}(\vec{\jmath}) = \tilde{z}_M(\vec{\imath})$.

The L.H.S and R.H.S are *both* MLEs of $\vec{z}_M$.

- By uniqueness of MLEs, they are equal as polynomials in $\vec{\imath}$.
- Therefore we still have equality at $\vec{r} \in \mathbb{F}^\ell$ *outside* $\{0,1\}$.

$\Rightarrow \sum_{\vec{\jmath} \in \{0,1\}^\ell} \widetilde{M}(\vec{r},\vec{\jmath}) \cdot \tilde{z}(\vec{\jmath}) = \tilde{z}_M(\vec{r})$ (*)



- $\widetilde{M}(\vec{r},\vec{s}) \cdot \tilde{z}(\vec{s}) = v$ by sumcheck completeness, and sumcheck checks pass.
- First sumcheck check involves $\tilde{z}_M(\vec{r})$ and passes by correctness of received query answers.
- V's checks of the final claim passes by (*) and correctness of received query answers.

Polynomial IOP for lin-check, soundness

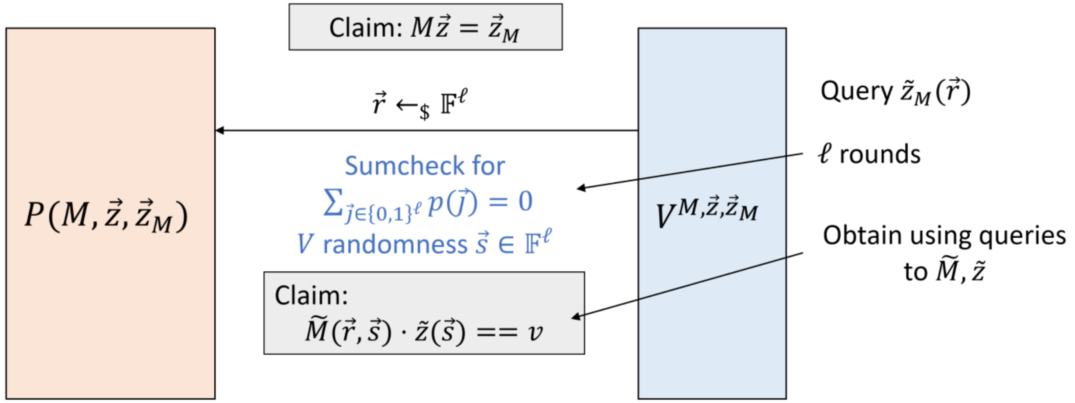
If $M\vec{z} \neq \vec{z}_M$ then $\exists \vec{\imath} \in \{0,1\}^\ell, \sum_{\vec{\jmath}\in\{0,1\}^\ell} M_{\vec{\imath},\vec{\jmath}} \cdot z_{\vec{\jmath}} \neq z_{M,\vec{\imath}}$ (explicit formula for matrix-vector multiplication)

$\sum_{\vec{\jmath}\in\{0,1\}^\ell} \widetilde{M}(\vec{\imath},\vec{\jmath}) \cdot \tilde{z}(\vec{\jmath}) \neq \tilde{z}_M(\vec{\imath})$.

The L.H.S and R.H.S are *not* equal as polynomials in $\vec{\imath}$.

- $\Rightarrow \sum_{\vec{\jmath}\in\{0,1\}^\ell} \widetilde{M}(\vec{r},\vec{\jmath}) \cdot \tilde{z}(\vec{\jmath}) \neq \tilde{z}_M(\vec{r})$

except w.p. $\leq \ell/|\mathbb{F}|$ by the S.Z. Lemma.



$\widetilde{M}(\vec{r},\vec{s}) \cdot \tilde{z}(\vec{s}) \neq v$ (or one of V's sumcheck checks fails) except w.p. $2\ell/|\mathbb{F}|$ by sumcheck soundness.

- In this case, V's check of the final claim *fails* by the previous line, correctness of received query answers.

Lin-check prover complexity (table method)

- $p\left(\vec{X}\right) := \widetilde{M}(\vec{r}, \vec{X}) \cdot \tilde{z}(\vec{X})$

- This time $d + 1 = 3 > 2 = |H|$.
- $p\left(\vec{X}\right)$ is too big to store if we want $O(N)$ running time.

Goal: $q_1(X_1) := \sum_{\vec{\omega} \in H^{\ell-1}} p(X_1, \omega_2, .., \omega_\ell)$

$\{q_1(j)\}_{j \in [d+1]}$ defines $q_1(X_1)$

Known from $\vec{z}$ How to compute?

$\left\{\tilde{z}(j, \vec{\omega}), \widetilde{M}(\vec{r}, j, \vec{\omega})\right\}_{j \in \{0,1\}, \vec{\omega} \in H^{\ell-1}}$

Interpolate in X_1

$O(d|H|^{\ell-1})$ ops

$\left\{\tilde{z}(X_1, \vec{\omega}), \widetilde{M}(\vec{r}, X_1, \vec{\omega})\right\}_{\vec{\omega} \in H^{\ell-1}}$

Eval at s_1, $O(d|H|^{\ell-1})$ ops

$\left\{\tilde{z}(s_1, \vec{\omega}), \widetilde{M}(\vec{r}, s_1, \vec{\omega})\right\}_{\vec{\omega} \in H^{\ell-1}}$

Table for next sumcheck iteration

Evaluate at d points

$O(d^2|H|^{\ell-1})$ ops

$\left\{\tilde{z}(j, \vec{\omega}), \widetilde{M}(\vec{r}, j, \vec{\omega})\right\}_{j \in [d+1], \vec{\omega} \in H^{\ell-1}}$

Combine, $O(d|H|^{\ell-1})$ ops

$\{p(j, \vec{\omega})\}_{j \in [d+1], \vec{\omega} \in H^{\ell-1}} \longrightarrow \{q_1(j)\}_{j \in [d+1]}$

$O(d^2|H|^{\ell-1})$ ops for q_1

Recurse for $O\left(d^2|H|^{\ell}\right) = O(N)$ total

Computing a table of $\widetilde{M}(\vec{r}, j, \vec{\omega})$

- Goal: $\left\{\widetilde{M}(\vec{r}, j, \vec{\omega})\right\}_{j \in \{0,1\}, \vec{\omega} \in H^{\ell-1}}$
- Note $\widetilde{M}\left(\vec{X}, \vec{Y}\right) = \sum_{\vec{i}, \vec{j} \in \{0,1\}^{\log n}} M_{ij} \cdot \widetilde{\mathrm{EQ}}\left(\vec{X}; \vec{i}\right) \cdot \widetilde{\mathrm{EQ}}\left(\vec{Y};\ \vec{j}\right)$.
- $\widetilde{M}\left(\vec{r}, \vec{Y}\right) = \sum_{\vec{i}, \vec{j} \in \{0,1\}^{\log n}} M_{ij} \cdot \widetilde{\mathrm{EQ}}(\vec{r}; \vec{i}) \cdot \widetilde{\mathrm{EQ}}\left(\vec{Y};\ \vec{j}\right)$.
- $\widetilde{M}(\vec{r}, j, \vec{\omega}) = \sum_{\vec{i} \in \{0,1\}^{\log n}} M_{\vec{i}, j, \vec{\omega}} \cdot \widetilde{\mathrm{EQ}}(\vec{r}; \vec{i})$ for $j \in \{0,1\}, \vec{\omega} \in H^{\ell-1}$.

- $\left\{\widetilde{\mathrm{EQ}}(\vec{r}; \vec{i})\right\}_{\vec{i} \in \{0,1\}^{\ell}}$ costs $O(N)$ ops to compute.
- Given a table for $\widetilde{\mathrm{EQ}}$, we can obtain *all* sums in $O(|M|)$ operations.

Polynomial IOP for input-check

No communication.
Verifier complexity:

$O(N_{in})$ $\mathbb{F}$-ops to evaluate $\tilde{x}$
Total costs $O(N_{in})$

$P(\vec{z}, \vec{x})$

Claim: $\vec{z} = \vec{x}||\vec{w}$

$V^{\vec{z}}(\vec{x})$

$\vec{r} \leftarrow_{\$} \mathbb{F}^{\ell_{in}}$

Query
$\tilde{z}(\vec{r}, 0^{\ell-\ell_{in}})$

Query complexity 1

Claim:
$\tilde{z}(\vec{r}, 0^{\ell-\ell_{in}}) == \tilde{x}(\vec{r})$

Compute $\tilde{x}(\vec{r})$ alone

Completeness:

- $\vec{z} = \vec{x}||\vec{w} \Rightarrow \forall i \in [N_{in}], z_i = x_i$

Little endian

- $\Rightarrow \forall i_1, \ldots, i_{\ell_{in}} \in \{0,1\}, \; \tilde{z}(i_1, \ldots, i_{\ell_{in}}, 0, \ldots, 0) = \tilde{x}(i_1, \ldots, i_{\ell_{in}})$.
- The L.H.S and R.H.S are *both* MLEs of $\vec{x}$.
- By uniqueness of MLEs, they are equal as polynomials in $\vec{\imath}$.
- Therefore we still have equality at $\vec{r} \in \mathbb{F}^{\ell_{in}}$ *outside* $\{0,1\}$ and $\tilde{z}(\vec{r}, 0^{\ell-\ell_{in}}) == \tilde{x}(\vec{r})$ (*)
- V's check of the final claim passes by (*) and correctness of received query answer.

Polynomial IOP for input-check, soundness

$P(\vec{z}, \vec{x})$

Claim: $\vec{z} = \vec{x}||\vec{w}$

$V^{\vec{z}}(\vec{x})$

$\vec{r} \leftarrow_{\$} \mathbb{F}^{\ell_{in}}$

Query
$\tilde{z}(\vec{r}, 0^{\ell-\ell_{in}})$

Claim:
$\tilde{z}(\vec{r}, 0^{\ell-\ell_{in}}) == \tilde{x}(\vec{r})$

Compute $\tilde{x}(\vec{r})$
alone

Soundness:

- $\forall \vec{w} : \vec{z} \neq \vec{x}||\vec{w} \Rightarrow \exists i \in [N_{in}], z_i \neq x_i$
- $\Rightarrow \exists i_1, \ldots, i_{\ell_{in}} \in \{0,1\}, \tilde{z}\left(i_1, \ldots, i_{\ell_{in}}, 0, \ldots, 0\right) \neq \tilde{x}(i_1, \ldots, i_{\ell_{in}})$.

The L.H.S and R.H.S are *not* equal as polynomials in $\vec{\imath}$.

- $\Rightarrow \tilde{z}\left(\vec{r}, 0^{\ell-\ell_{in}}\right) \neq \tilde{x}(\vec{r})$ except w.p. $\leq \ell_{in}/|\mathbb{F}|$ by the S.Z. Lemma.
- In this case, V's check of the final claim *fails* by the previous line and correctness of received query answers.

Summary: polynomial IOP for R1CS

Preprocessing computes MLEs $\tilde{A}, \tilde{B}, \tilde{C}$

$P(A, B, C, \vec{x}, \vec{z}) \xrightarrow{\tilde{z}, \tilde{z}_A, \tilde{z}_B, \tilde{z}_C} V^{\tilde{A}, \tilde{B}, \tilde{C}}(\vec{x})$

Row check: $\vec{z}_A \circ \vec{z}_B = \vec{z}_C$

Lincheck: $\vec{z}_M = M\vec{z}$, $M \in \{A, B, C\}$

Input check: $\vec{z} = \vec{x}||\vec{w}$ for some $\vec{w}$

Run parallel IOP subprotocols

Soundness error

$= \text{max over subprotocols}$

$= O(\ell / |\mathbb{F}|) = O(\log N / |\mathbb{F}|)$.

Communication complexity

$= O(\ell) = O(\log N)$ $\mathbb{F}$-elements.

- Verifier complexity $O(\ell + N_{in}) = O(\log N + N_{in})$ $\mathbb{F}$-ops.
- Query complexity $O(1)$ (to $\tilde{A}, \tilde{B}, \tilde{C}, \tilde{z}, \tilde{z}_A, \tilde{z}_B, \tilde{z}_C$).
- Prover complexity $O(N + |A| + |B| + |C|)$ $\mathbb{F}$-ops.

Plan for the next few lectures

Sumcheck protocol

Interactive proof for layered arithmetic circuits

Interactive oracle proofs for general arithmetic circuits

Commitments and polynomial commitments

ZK arguments for layered arithmetic circuits

ZK arguments for general arithmetic circuits

Syntax of polynomial commitment schemes

Definition: Same as standard commitments except for deg and Eval.

A *polynomial commitment (P.C.) scheme* is a collection of 3 p.p.t. algorithms $(\mathrm{Setup}, \mathrm{Commit}, \mathrm{Verify})$ and *interactive protocol* Eval such that $\forall \lambda \in \mathbb{N}$,

- $\mathrm{Setup}(1^\lambda, deg)$ outputs public parameters pp describing a message space $\mathfrak{M}$, randomness space $\mathfrak{R}$, decommitment space $\mathfrak{D}$ and commitment space $\mathfrak{C}$.
- $\mathrm{Commit}(pp, f \in \mathfrak{M}, r \leftarrow_\$ \mathfrak{R})$ outputs a pair $(c, d) \in \mathfrak{C} \times \mathfrak{D}$. f a polynomial
- $\mathrm{Verify}(pp, c \in \mathfrak{C}, d \in \mathfrak{D}, m \in \mathfrak{M})$ outputs a bit $b \in \{0,1\}$.
- Eval is an interactive protocol for

deg degree bound

$$\mathcal{R}_{PC}(pp, deg) := \left\{ \big((c, z, y), (f, d)\big) : \begin{array}{c} f \in \mathbb{F}[X], \deg f \le deg \\ f(y) = z, \mathrm{Verify}(pp, c, d, f) = 1 \end{array} \right\}$$

z, y not hidden

Message space could be $\mathbb{F}^{\le deg}[X], \mathbb{F}^{\le deg}[X_1, \dots, X_\ell]$.
Can make deg a vector of individual degrees.

P.C. schemes – correctness and security

Definition:

$\forall \lambda \in \mathbb{N}$, a P.C. scheme $(\mathrm{Setup}, \mathrm{Commit}, \mathrm{Verify}, \mathrm{Eval})$ satisfies

- *Correctness* if $\forall$ adversaries $A, \forall \lambda, deg \in \mathbb{N}$

Similar to normal commitments
with extra conditions for Eval

$$\Pr\left[\begin{array}{c} pp \leftarrow_{\$} \mathrm{Setup}(1^{\lambda}, deg), f \leftarrow_{\$} A(pp) \\ (c,d) \leftarrow_{\$} Commit(pp, f), b_1 \leftarrow_{\$} Verify(pp, c, d, f) \\ y \leftarrow_{\$} A(pp, c, d, f), f(y) = z, b_2 \leftarrow_{\$} \mathrm{Eval}(P(f,d), V)(pp, c, y, z): \\ b_1 = b_2 = 1 \end{array}\right] =$$

- *Hiding* and *binding* following standard commitments definitions.
- *Knowledge soundness* and *zero-knowledge* if Eval does.

z, y not hidden

Plan for the next few lectures

Sumcheck protocol ✓

coNP ⊆ IP ✓
Extends to #SAT
(count SAT inputs)
Shows **#P ⊆ IP**

Interactive proof for layered arithmetic circuits ✓

Interactive oracle proofs for general arithmetic circuits ✓

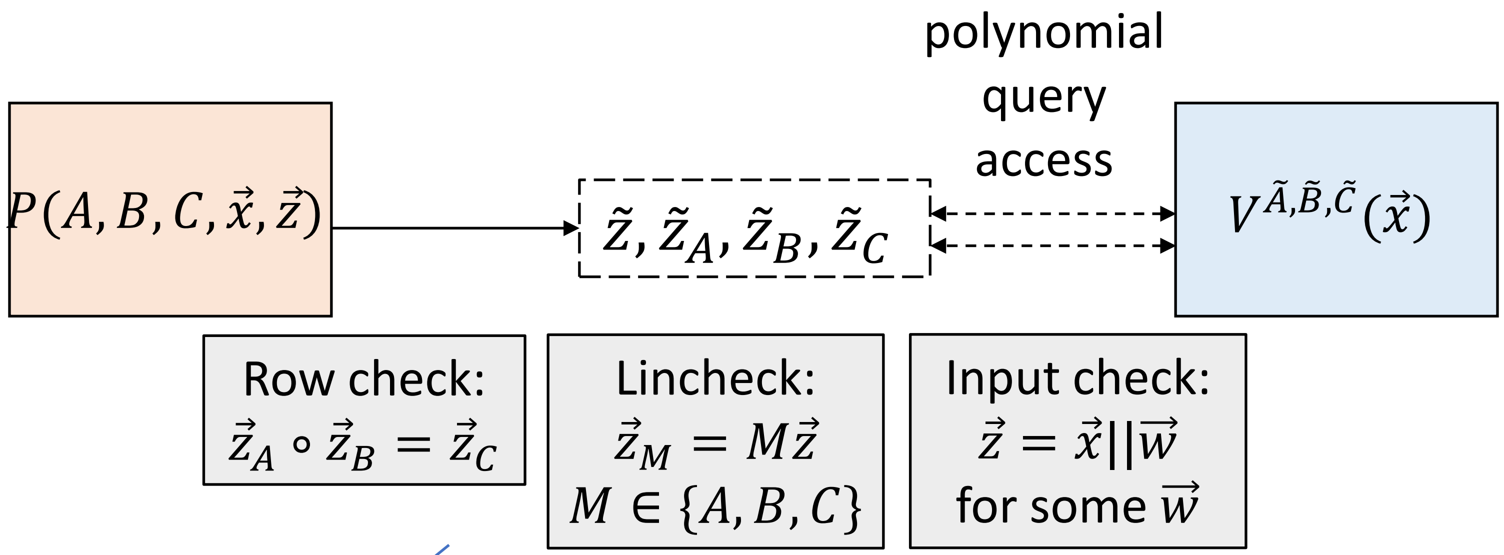
Commitments and polynomial commitments

- **DLOG construction**
- Efficiency improvements
- Adding zero-knowledge

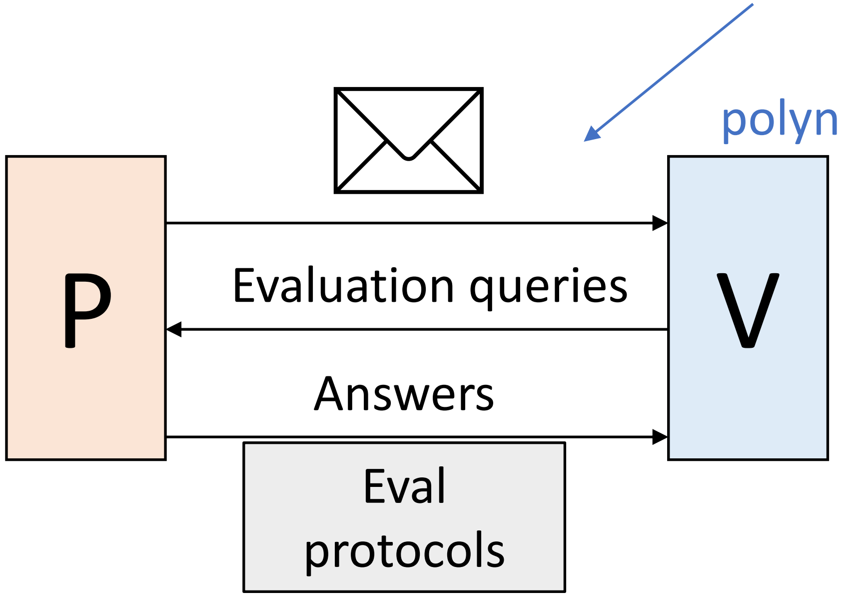
ZK arguments for layered arithmetic circuits

ZK arguments for general arithmetic circuits

Motivation for using PC schemes



Compile with
polynomial commitments



To get preserve efficiency:

We need superfast polylog(N) verification for Eval.

We have $\tilde{A}\left(\vec{X}, \vec{Y}\right) := \sum_{\vec{\imath}, \vec{\jmath} \in \{0,1\}^{\log N}} A_{ij} \cdot \widetilde{\mathrm{EQ}}\left(\vec{X}, \vec{Y}; \vec{\imath}, \vec{\jmath}\right)$.

$O(N^2)$ coefficients. Only $O(N)$ non-zero from CSAT

We need a commitment where the prover only does $O(|A|)$ $\mathbb{F}$-ops for Commit and Eval. $O(N)$ prover for CSAT instances

Simple Pedersen PC scheme for MLEs

Setup$(\mathbf{1}^{\lambda}, \boldsymbol{deg})$**:** Group $\mathbb{G}$ of prime order $p \approx 2^{\lambda}, H \leftarrow_{\$} \mathbb{G}, s \leftarrow_{\$} \mathbb{Z}_p,$

$G = s \cdot H.$ Output $pp \coloneqq (\mathbb{G}, G, H, p).$

Commit$(\boldsymbol{pp}, \tilde{\boldsymbol{f}} \in \mathbb{Z}_{\boldsymbol{p}}[\boldsymbol{X}], \boldsymbol{r} \leftarrow_{\$} \mathbb{Z}_{\boldsymbol{p}})$**:**

Parse $\tilde{f}\left(\vec{X}\right) \coloneqq \sum_{\vec{i} \in \{0,1\}^{\log N}} f_{\vec{i}} \cdot \widetilde{\mathrm{EQ}}\left(\vec{X}; \vec{i}\right)$. $\forall \vec{i} \in \{0,1\}^{\log N}$, sample $r_{\vec{i}} \leftarrow_{\$} \mathbb{Z}_p$.

Compute $(C_{\vec{i}}, d_{\vec{i}}) \coloneqq (f_{\vec{i}} \cdot G + r_{\vec{i}} \cdot H, r_{\vec{i}})$. Output $(c = \{C_{\vec{i}}\}, d = \{d_{\vec{i}}\})$.

$O(N)$ commitment size

Verify$(\boldsymbol{pp}, \boldsymbol{c}, \boldsymbol{d}, \boldsymbol{m})$**:** Output $\bigwedge_{\vec{i} \in \{0,1\}^{\log N}} (C_{\vec{i}} == f_{\vec{i}} \cdot G + r_{\vec{i}} \cdot H)$.

Eval: Given $y_1, \ldots, y_{\log N}, z \in \mathbb{F}, \{c_{\vec{i}}\}$, prove knowledge of openings $C_{\vec{i}} = f_{\vec{i}} \cdot G + r_{\vec{i}} \cdot H$ such that $\sum_{\vec{i} \in \{0,1\}^{\log N}} f_{\vec{i}} \cdot \widetilde{\mathrm{EQ}}(\vec{y}; \vec{i}) = z$.

Use Σ-protocol techniques

$O(N)$ proof size, V complexity

Part of witness

Inside commitments

Part of instance

Linear combination

Pedersen multi-commitments

Setup$(\mathbf{1}^\lambda, \boldsymbol{deg})$: Group $\mathbb{G}$ of prime order $p \approx 2^\lambda$, $G_0, \dots, G_{N-1}, H \leftarrow_\$ \mathbb{G}$. Output $pp \coloneqq (\mathbb{G}, \vec{G} = (G_0, \dots, G_{N-1}), H, p)$.

Commit$(\boldsymbol{pp}, \tilde{\boldsymbol{f}} \in \mathbb{Z}_{\boldsymbol{p}}[\boldsymbol{X}], \boldsymbol{r} \leftarrow_\$ \mathbb{Z}_{\boldsymbol{p}})$: Focus on MLEs

Parse $\tilde{f}\left(\vec{X}\right) \coloneqq \sum_{\vec{i} \in \{0,1\}^{\log N}} f_{\vec{i}} \cdot \widetilde{\mathrm{EQ}}\left(\vec{X}; \vec{i}\right)$. Sample $r \leftarrow_\$ \mathbb{Z}_p$.

$O(1)$ commitment size

Compute $(C, d) \coloneqq \left(\sum_{\vec{i} \in \{0,1\}^{\log N}} f_{\vec{i}} \cdot G_i + r \cdot H, r\right) = \left(\langle \vec{f}, \vec{G} \rangle + r \cdot H, r\right)$. Output (C, d).

Verify$(\boldsymbol{pp}, \boldsymbol{C}, \boldsymbol{d}, \boldsymbol{m})$: Output $C == \sum_{\vec{i} \in \{0,1\}^{\log N}} f_{\vec{i}} \cdot G_i + r \cdot H$.

Eval: Given $y_1, \dots, y_{\log N}, z \in \mathbb{F}$, c, prove knowledge of openings $\{f_{\vec{i}}\}, r$ of C such that $\sum_{\vec{i} \in \{0,1\}^{\log N}} f_{\vec{i}} \cdot \widetilde{\mathrm{EQ}}(\vec{y}; \vec{i}) = z$. Use Σ-protocol techniques $O(N)$ proof size, V complexity

$$\mathcal{R}_{PedPC}(pp) \coloneqq \left\{ \left((C, z, y_1, \dots, y_\ell), (\tilde{f}, r) \right) : \begin{array}{c} \tilde{f} \in \mathbb{F}^{\le 1}[X_1, \dots, X_\ell] \\ \tilde{f}(y_1, \dots, y_\ell) = z, C = \langle \vec{f}, \vec{G} \rangle + r \cdot H \end{array} \right\}$$

Security of Pedersen multi-commitments

Hiding:

- $r \leftarrow_{\$} \mathbb{Z}_p$ so if $H \neq 0_{\mathbb{G}}$, then $r \cdot H$ is uniformly random in $\mathbb{G}$.
- Hence $C = \sum_{\vec{i} \in \{0,1\}^{log\ N}} f_{\vec{i}} \cdot G_i + r \cdot H$ is uniformly random in $\mathbb{G}$.

Binding:

- We will reduce to binding for plain Pedersen $C = m \cdot G + r \cdot H$.
- Given efficient A breaking binding for multi-Pedersen w.p. ϵ, we build efficient B breaking binding for plain Pedersen w.p. $\geq \epsilon - 3/p$.

Reducing binding to plain Pedersen binding

$B^A(\mathbb{G}, G, H, p)$:

Failure probability $\leq 3/p$
Success probability $\geq \epsilon - 3/p$

1. If $G = 0_{\mathbb{G}}$ or $H = 0_{\mathbb{G}}$ then abort. Probability $2/p$
2. $x_1, y_1, \ldots, x_{N-1}, y_{N-1}, x_r, y_r \leftarrow_\$ \mathbb{Z}_p$.
3. For $i = 0, \ldots, N-1$, compute $G_i' \coloneqq x_i \cdot G + y_i \cdot H$.
4. Compute $H' \coloneqq x_r \cdot G + y_r \cdot H$.
5. Get $\vec{f}, \vec{f}', r, r' \leftarrow A(\mathbb{G}, \vec{G}', H', p)$ with $\vec{f} \neq \vec{f}'$ and $\langle \vec{f}, \vec{G}' \rangle + r \cdot H' = \langle \vec{f}', \vec{G}' \rangle + r' \cdot H'$.
   Independent of $\vec{x}, \vec{y}, x_r, y_r$ by perfect hiding of plain Pedersen, success prob. still ϵ
6. Let $\vec{x} \coloneqq (x_0, \ldots, x_{N-1})$, $\vec{y} \coloneqq (y_0, \ldots, y_{N-1})$.
   $\langle \vec{f}, \vec{x} \rangle + r x_r \neq \langle \vec{f}', \vec{x} \rangle + r' x_r$ except w.p. $\leq 1/p$ by the Schwartz-Zippel lemma
7. Output $m \coloneqq \langle \vec{f}, \vec{x} \rangle + r x_r$, $s \coloneqq \langle \vec{f}, \vec{y} \rangle + r y_r$, $m' \coloneqq \langle \vec{f}', \vec{x} \rangle + r' x_r$, $s' \coloneqq \langle \vec{f}', \vec{y} \rangle + r' y_r$
   with $m \neq m'$ and $m \cdot G + \cancel{r}\, s \cdot H = m' \cdot G + \cancel{r}\, s' \cdot H$.

Note: not secure for e.g. exponentially large $N \approx \sqrt{p}$ as collisions in Step 3 imply DLOG break w.h.p. and collision probability is large using birthday bound

Eval protocol for Pedersen multicommitments

- Let $y_1, \dots, y_{\log N} \in \mathbb{Z}_p$ with $\tilde{f}(y_1, \dots, y_{\log N}) = z$.
- Let $\vec{Y} := \mathrm{Expand}(\vec{y}) = \left(\widetilde{\mathrm{EQ}}(\vec{y}; \vec{\imath})\right)_{\vec{\imath} \in \{0,1\}^{\log N}}$ satisfying $f(\vec{y}) = \langle \vec{f}, \vec{Y} \rangle$.

Example:

$\tilde{f}(X_1, X_2) = f_{00}(1 - X_1)(1 - X_2) + f_{01}X_1(1 - X_2) + f_{10}(1 - X_1)X_2 + f_{11}X_1X_2,$

$\vec{f} = (f_{00}, f_{01}, f_{10}, f_{11}), \vec{Y} = ((1 - y_1)(1 - y_2), y_1(1 - y_2), (1 - y_1)y_2, y_1y_2).$

- Write $C = \langle \vec{f}, \vec{G} \rangle + r \cdot H$ and $z = \langle \vec{f}, \vec{Y} \rangle$.

Focus: prove scalar products, $O(\log N)$ communication complexity

- $\mathcal{R}_{PedPC}(pp) := \left\{ \left((C, z, y_1, \dots, y_\ell), \tilde{f} \right) : \begin{array}{c} \tilde{f} \in \mathbb{F}^{\leq 1}[X_1, \dots, X_\ell] \\ z = \langle \vec{f}, \vec{Y} \rangle, C = \langle \vec{f}, \vec{G} \rangle \end{array} \right\}$

Set $r = 0$ initially
P can just send r to V.
Both remove $r \cdot H$ from C

- We will construct a protocol for Eval with prover complexity $O(N)$, proof size $O(\log N)$ and verifier complexity $O(N)$.

Improve to polylog(N) later and add ZK

Reduction completeness
$\Downarrow$
Completeness

Evaluation protocol overview

Witness:

- vector $\vec{f} \in \mathbb{F}^N$

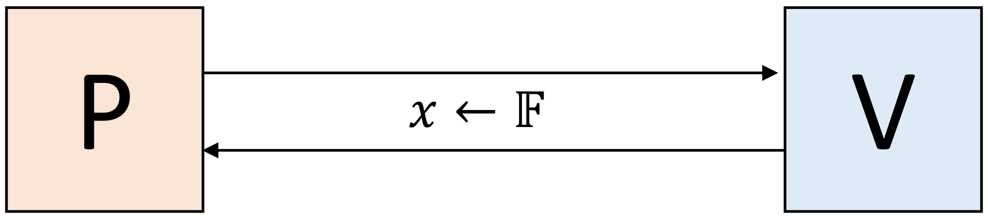
Length N

Instance:

- commitment $C \in \mathbb{G}$, key $\vec{G} \in \mathbb{G}^N$
- vector $\vec{Y} \in \mathbb{F}^N$, target $z \in \mathbb{F}$

Language:

- $C = \langle \vec{f}, \vec{G} \rangle \in \mathbb{G}$
- $z = \langle \vec{f}, \vec{Y} \rangle \in \mathbb{Z}_p$



No verifier checks!

Length $N/2$

New witness:

- vector $\vec{f}' \in \mathbb{F}^{N/2}$

New instance:

- commitment $C' \in \mathbb{G}$, key $\vec{G}' \in \mathbb{G}^{N/2}$
- vector $\vec{Y}' \in \mathbb{F}^{N/2}$, target $z' \in \mathbb{F}$

New language:

- $C' = \langle \vec{f}', \vec{G}' \rangle \in \mathbb{G}$
- $z' = \langle \vec{f}', \vec{Y}' \rangle \in \mathbb{Z}_p$

$\vdots$ $\log N - 1$ more reductions

Reduction 4-soundness
$\Downarrow$
$(4, \ldots, 4)$-soundness

Length 1

Final witness:

- element $f^{(\log N)} \in \mathbb{F}$

Final instance:

- commitment $C^{(\log N)} \in \mathbb{G}$, key $G^{(\log N)} \in \mathbb{G}$
- element $Y^{(\log N)} \in \mathbb{F}$, target $z^{(\log N)} \in \mathbb{F}$

Final language:

- $C^{(\log N)} = f^{(\log N)} \cdot G^{(\log N)} \in \mathbb{G}$
- $z^{(\log N)} = f^{(\log N)} \cdot Y^{(\log N)} \in \mathbb{Z}_p$

P simply sends $f^{(\log N)}$ for V to check

Evaluation protocol reduction details

Witness:

- vector $\vec{f} \in \mathbb{F}^N$

Parse

$$\vec{f} = \left(\vec{f}_L, \vec{f}_R\right) \in \mathbb{F}^{N/2} \times \mathbb{F}^{N/2}$$
$$\vec{Y} = \left(\vec{Y}_L, \vec{Y}_R\right) \in \mathbb{F}^{N/2} \times \mathbb{F}^{N/2}$$
$$\vec{G} = \left(\vec{G}_L, \vec{G}_R\right) \in \mathbb{G}^{N/2} \times \mathbb{G}^{N/2}$$

Compute

$$C_- = \langle \vec{f}_L, \vec{G}_R \rangle,\ C_+ = \langle \vec{f}_R, \vec{G}_L \rangle$$
$$z_- = \langle \vec{f}_L, \vec{Y}_R \rangle,\ z_+ = \langle \vec{f}_R, \vec{Y}_R \rangle$$

Instance:

- commitment $C \in \mathbb{G}$, key $\vec{G} \in \mathbb{G}^N$
- vector $\vec{Y} \in \mathbb{F}^N$, target $z \in \mathbb{F}$

Language:

- $C = \langle \vec{f}, \vec{G} \rangle \in \mathbb{G}$
- $z = \langle \vec{f}, \vec{Y} \rangle \in \mathbb{Z}_p$

P $\xrightarrow{C_-, C_+, z_-, z_+}$ V

P $\xleftarrow{x \leftarrow \mathbb{F}}$ V

Both compute

$$C' := C_- + x \cdot C + x^2 \cdot C_+$$
$$z' := z_- + x \cdot z + x^2 \cdot z_+$$
$$\vec{Y}' := x\vec{Y}_L + \vec{Y}_R \in \mathbb{F}^{N/2}$$
$$\vec{G}' := x\vec{G}_L + \vec{G}_R \in \mathbb{G}^{N/2}$$

$O(\log N)$ communication for full protocol

New witness:

- $\vec{f}' := \vec{f}_L + x\vec{f}_R \in \mathbb{F}^{N/2}$

New instance:

- commitment $C' \in \mathbb{G}$, key $\vec{G}' \in \mathbb{G}^{N/2}$
- vector $\vec{Y}' \in \mathbb{F}^{N/2}$, target $z' \in \mathbb{F}$

New language:

- $C' = \langle \vec{f}', \vec{G}' \rangle \in \mathbb{G}$
- $z' = \langle \vec{f}', \vec{Y}' \rangle \in \mathbb{Z}_p$

Special properties of multicommitments

$$\left\langle \vec{f}_1, \vec{G} \right\rangle + \left\langle \vec{f}_2, \vec{G} \right\rangle = \left\langle \vec{f}_1 + \vec{f}_2, \vec{G} \right\rangle$$

Message homomorphism

Exploit all available structure

$$\left\langle \vec{f}, \vec{G}_1 \right\rangle + \left\langle \vec{f}, \vec{G}_2 \right\rangle = \left\langle \vec{f}, \vec{G}_1 + \vec{G}_2 \right\rangle$$

Key homomorphism

Bilinearity

$$\left\langle \vec{f}_1, \vec{G}_1 \right\rangle + \left\langle \vec{f}_2, \vec{G}_2 \right\rangle = \left\langle \vec{f}_1 || \vec{f}_2, \vec{G}_1 || \vec{G}_2 \right\rangle$$

Concatenation

Completeness analysis of reduction

- We show that valid instance-witness pairs reduce to valid instance-witness pairs i.e. $C' = \langle \vec{f}', \vec{G}' \rangle$ and $z' = \langle \vec{f}', \vec{Y}' \rangle$.

$$\left\langle \vec{f}', \vec{G}' \right\rangle = \left\langle \vec{f}_L + x\vec{f}_R, x\vec{G}_L + \vec{G}_R \right\rangle$$

Expand using bilinearity

$$= \left\langle \vec{f}_L, \vec{G}_R \right\rangle + x\left(\left\langle \vec{f}_L, \vec{G}_L \right\rangle + \left\langle \vec{f}_R, \vec{G}_R \right\rangle\right) + x^2 \left\langle \vec{f}_R, \vec{G}_L \right\rangle$$

Simplify middle term using concatenation

$$= \left\langle \vec{f}_L, \vec{G}_R \right\rangle + x\left\langle \vec{f}, \vec{G} \right\rangle + x^2 \left\langle \vec{f}_R, \vec{G}_L \right\rangle$$

$$= C_- + x \cdot C + x^2 \cdot C_+ = C'$$

- Similarly, $\left\langle \vec{f}', \vec{Y}' \right\rangle = z_- + x \cdot z + x^2 \cdot z_+ = z'$.

(4,..,4)-soundness from reduction 4-soundness

$(4, \dots, 4)$-tree of transcripts

C_-, C_+, z_-, z_+

x_1 distinct x_4

$C'_{-,1}, C'_{+,1}, z'_{-,1}, z'_{+,1} \dots \; C'_{-,4}, C'_{+,4}, z'_{-,4}, z'_{+,4}$

… … … ⋰ ⋱ …

Accepting means that V checks the final witness

$f_{1,\dots,1}^{(\log N)}$ … … $f_{4,\dots,4}^{(\log N)}$

Apply reduction extractor recursively

1 length N opening

$C = \langle \vec{f}, \vec{G} \rangle$

$z = \langle \vec{f}, \vec{Y} \rangle$

⋮

$4^{\log N - 1}$ length 2 openings

$C^{(\log N-1)} = \langle f^{(\log N-1)}, G^{(\log N-1)} \rangle$

$z^{(\log N-1)} = \langle f^{(\log N-1)}, Y^{(\log N-1)} \rangle$

$4^{\log N}$ length 1 openings

$C^{(\log N)} = f^{(\log N)} \cdot G^{(\log N)}$

$z^{(\log N)} = f^{(\log N)} Y^{(\log N)}$

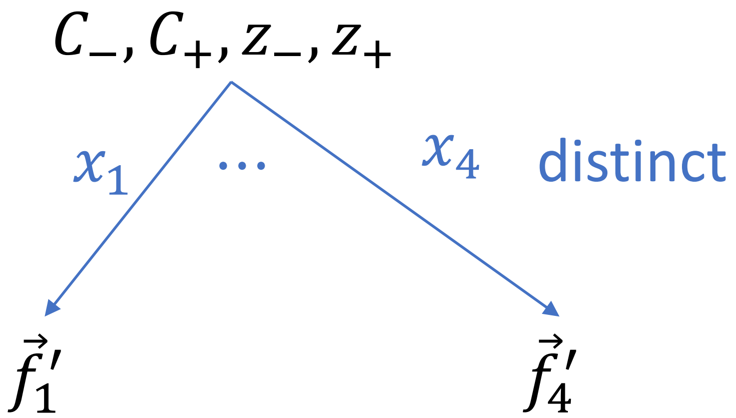
$\vec{Y}_j' := x_j \vec{Y}_L + \vec{Y}_R$

$\vec{G}_j' := x_j \vec{G}_L + \vec{G}_R$

We cannot make assumptions about how $\vec{f}_j'$ were computed.

4-soundness of reduction I

- Consider a 4-tree of transcripts.



Satisfying, $\forall j \in \{1,2,3,4\}$,

$$\left\langle \vec{f}_j', \vec{G}_j' \right\rangle = C' = C_- + x_j \cdot C + x_j^2 \cdot C_+$$

$$\left\langle \vec{f}_j', \vec{Y}_j' \right\rangle = z' = z_- + x_j \cdot z + x_j^2 \cdot z_+$$

- We want openings in terms of $\vec{G}$. Bilinearity Concatenation $\vec{f}_{x,j} := x_j \vec{f}_j' || \vec{f}_j'$
- $\left\langle \vec{f}_j', \vec{G}_j' \right\rangle = \left\langle \vec{f}_j', x_j \vec{G}_L + \vec{G}_R \right\rangle = x_j \left\langle \vec{f}_j', \vec{G}_L \right\rangle + \left\langle \vec{f}_j', \vec{G}_R \right\rangle = \left\langle x_j \vec{f}_j' || \vec{f}_j', \vec{G}_L || \vec{G}_R \right\rangle = \left\langle \vec{f}_{x,j}, \vec{G} \right\rangle$

Taking $j = 1,2,3$

$$\begin{pmatrix} 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \\ 1 & x_3 & x_3^2 \end{pmatrix} \begin{pmatrix} C_- \\ C \\ C_+ \end{pmatrix} = \begin{pmatrix} \vec{f}_{x,1} \\ \vec{f}_{x,2} \\ \vec{f}_{x,3} \end{pmatrix} \cdot \begin{pmatrix} G_0 \\ \vdots \\ G_{N-1} \end{pmatrix} \xrightarrow{\text{Invertibility of Vandermonde matrices}} \begin{pmatrix} C_- \\ C \\ C_+ \end{pmatrix} = \begin{pmatrix} \vec{f}_- \\ \vec{f} \\ \vec{f}_+ \end{pmatrix} \cdot \begin{pmatrix} G_0 \\ \vdots \\ G_{N-1} \end{pmatrix}$$

4-soundness of reduction II

Extractor output: $\vec{f} \in \mathbb{Z}_p^N$.

$\forall j \in \{1,2,3,4\}$,

$$\left\langle \vec{f}_j', \vec{G}_j' \right\rangle = C' = C_- + x_j \cdot C + x_j^2 \cdot C_+$$

$$\left\langle \vec{f}_j', \vec{Y}_j' \right\rangle = z' = z_- + x_j \cdot z + x_j^2 \cdot z_+$$

Why is the output a witness?

By construction, $C = \langle \vec{f}, \vec{G} \rangle$.

We must show that $z = \langle \vec{f}, \vec{Y} \rangle$ to prove $\vec{f}$ is really a witness.

$$\left\langle \vec{f}_{x,j}, \vec{G} \right\rangle = C_- + x_j \cdot C + x_j^2 \cdot C_+, \qquad \left\langle \vec{f}_{x,j}, \vec{Y} \right\rangle = z_- + x_j \cdot z + x_j^2 \cdot z_+.$$

Similarly to the previous slide

Substituting openings, we have

$$\left\langle \vec{f}_{x,j}, \vec{G} \right\rangle = \left\langle \vec{f}_-, \vec{G} \right\rangle + x_j \cdot \left\langle \vec{f}, \vec{G} \right\rangle + x_j^2 \cdot \left\langle \vec{f}_+, \vec{G} \right\rangle = \left\langle \vec{f}_- + x_j \vec{f} + x_j^2 \vec{f}_+, \vec{G} \right\rangle$$

Hence $\vec{f}_{x,j} = \vec{f}_- + x_j \vec{f} + x_j^2 \vec{f}_+$ or the extractor breaks binding.

Recall that by definition, $\vec{f}_{x,j} \coloneqq x_j \vec{f}_j' || \vec{f}_j'$ so $x_j \vec{f}_j' || \vec{f}_j' = \vec{f}_- + x_j \vec{f} + x_j^2 \vec{f}_+, j \in \{1,2,3,4\}$

4-soundness of reduction III

$x_j \vec{f}_j' || \vec{f}_j' = \vec{f}_- + x_j \vec{f} + x_j^2 \vec{f}_+, j \in \{1,2,3,4\}$

Splitting $\vec{f}_- = \vec{f}_{-,L} || \vec{f}_{-,R}, \vec{f} = \vec{f}_L || \vec{f}_R$ and $\vec{f}_+ = \vec{f}_{+,L} || \vec{f}_{+,R}$, we have

$$(x_j \vec{f}_j' || \vec{f}_j') = (\vec{f}_{-,L} || \vec{f}_{-,R}) + x_j (\vec{f}_L || \vec{f}_R) + x_j^2 (\vec{f}_{+,L} || \vec{f}_{+,R})$$

Considering the left and right halves separately,

$$x_j \vec{f}_j' = \vec{f}_{-,L} + x_j \vec{f}_L + x_j^2 \vec{f}_{+,L}, \qquad \vec{f}_j' = \vec{f}_{-,R} + x_j \vec{f}_R + x_j^2 \vec{f}_{+,R}$$

Substituting the right expression for $\vec{f}_j'$ into the left expression,

$$x_j \vec{f}_{-,R} + x_j^2 \vec{f}_R + x_j^3 \vec{f}_{+,R} = \vec{f}_{-,L} + x_j \vec{f}_L + x_j^2 \vec{f}_{+,L}$$

Degree 3, holds for 4 distinct $x_j \Rightarrow$ identically zero

Comparing coefficients,

$$\vec{f}_{-,L} = 0, \qquad \vec{f}_L = \vec{f}_{-,R}, \qquad \vec{f}_R = \vec{f}_{+,L}, \qquad \vec{f}_{+,R} = 0.$$

$$\vec{f}_j' = \vec{f}_L + x_j \vec{f}_R$$

4-soundness of reduction IV

Now we finally show that $z = \langle \vec{f}, \vec{Y} \rangle$.

Recall that $\left\langle \vec{f}_j', \vec{Y}_j' \right\rangle = z_- + x_j \cdot z + x_j^2 \cdot z_+, \quad \forall j \in \{1,2,3,4\}$,

$\vec{Y}_j' := x_j \vec{Y}_L + \vec{Y}_R$

Now we know also know

$\vec{f}_j' = \vec{f}_L + x_j \vec{f}_R$

Substituting, we have

$$\left\langle \vec{f}_j', \vec{Y}_j' \right\rangle = \left\langle \vec{f}_L + x_j \vec{f}_R, x_j \vec{Y}_L + \vec{Y}_R \right\rangle$$

Expand using bilinearity

$$= \left\langle \vec{f}_L, \vec{Y}_R \right\rangle + x_j \left(\left\langle \vec{f}_L, \vec{Y}_L \right\rangle + \left\langle \vec{f}_R, \vec{Y}_R \right\rangle \right) + x_j^2 \left\langle \vec{f}_R, \vec{Y}_L \right\rangle$$

Simplify middle term using concatenation

$$= \left\langle \vec{f}_L, \vec{Y}_R \right\rangle + x_j \left\langle \vec{f}, \vec{Y} \right\rangle + x_j^2 \left\langle \vec{f}_R, \vec{Y}_L \right\rangle = z_- + x_j \cdot z + x^2 \cdot z_+$$

Degree 3, holds for 4 distinct $x_j \Rightarrow$ identically zero

Middle term $\Rightarrow \langle \vec{f}, \vec{Y} \rangle = z$.

Communication and prover complexity

Witness:

- vector $\vec{f} \in \mathbb{F}^N$

Compute

$C_- = \langle \vec{f}_L, \vec{G}_R \rangle$, $C_+ = \langle \vec{f}_R, \vec{G}_L \rangle$

$z_- = \langle \vec{f}_L, \vec{Y}_R \rangle$, $z_+ = \langle \vec{f}_R, \vec{Y}_R \rangle$

Instance:

- commitment $C \in \mathbb{G}$, key $\vec{G} \in \mathbb{G}^N$
- vector $\vec{Y} \in \mathbb{F}^N$, target $z \in \mathbb{F}$

Language:

- $C = \langle \vec{f}, \vec{G} \rangle \in \mathbb{G}$
- $z = \langle \vec{f}, \vec{Y} \rangle \in \mathbb{Z}_p$

P

C_-, C_+, z_-, z_+

$x \leftarrow \mathbb{F}$

V

$O(1)$ $\mathbb{F}$ and $\mathbb{G}$ ops in each reduction

Total: $O(\log N)$ ops

Both compute

$C' := C_- + x \cdot C + x^2 \cdot C_+$

$z' := z_- + x \cdot z + x^2 \cdot z_+$

$\vec{Y}' := x\vec{Y}_L + \vec{Y}_R \in \mathbb{F}^{N/2}$

$\vec{G}' := x\vec{G}_L + \vec{G}_R \in \mathbb{G}^{N/2}$

$O(1)$ communication per round

$O(\log N)$ rounds

$O(\log N)$ communication complexity

$O(N)$ $\mathbb{F}$ and $\mathbb{G}$ ops in first reduction

Total prover complexity:

$O(N + N/2 + \cdots 1) = O(N)$ ops

$\vdots$ $\log N - 1$ more reductions

Final witness:

- element $f^{(\log N)} \in \mathbb{F}$

Final instance:

- commitment $C^{(\log N)} \in \mathbb{G}$, key $G^{(\log N)} \in \mathbb{G}$
- element $Y^{(\log N)} \in \mathbb{F}$, target $z^{(\log N)} \in \mathbb{F}$

Final language:

- $C^{(\log N)} = f^{(\log N)} \cdot G^{(\log N)} \in \mathbb{G}$
- $z^{(\log N)} = f^{(\log N)} \cdot Y^{(\log N)} \in \mathbb{Z}_p$

P simply sends $f^{(\log N)}$ for V to check

Verifier complexity

Witness:

- vector $\vec{f} \in \mathbb{F}^N$

Instance:

- commitment $C \in \mathbb{G}$, key $\vec{G} \in \mathbb{G}^N$
- vector $\vec{Y} \in \mathbb{F}^N$, target $z \in \mathbb{F}$

P $\xrightarrow{C_-, C_+, z_-, z_+}$ V

P $\xleftarrow{x \leftarrow \mathbb{F}}$ V

$O(1)$ $\mathbb{F}$ and $\mathbb{G}$ ops in each reduction

Total: $O(\log N)$ ops

Both compute

$C' := C_- + x \cdot C + x^2 \cdot C_+$

$z' := z_- + x \cdot z + x^2 \cdot z_+$

$\vec{Y}' := x\vec{Y}_L + \vec{Y}_R \in \mathbb{F}^{N/2}$

$\vec{G}' := x\vec{G}_L + \vec{G}_R \in \mathbb{G}^{N/2}$

$O(N)$ $\mathbb{G}$ ops to get $\vec{G}'$

Total verifier complexity:

$O(N + N/2 + \cdots 1) = O(N)$ ops

Compute $Y^{(\log N)}$ all in one at the end

$\vec{Y} = \left(\widetilde{\mathrm{EQ}}(\vec{y}; \vec{\imath})\right)_{\vec{\imath} \in \{0,1\}^{\log N}}$

$= \left(\prod_{j=1}^{\log N} \widetilde{\mathrm{EQ}}(y_j; i_j)\right)_{\vec{\imath} \in \{0,1\}^{\log N}}$

$\vec{Y}_L = (1 - y_1) \cdot \left(\prod_{j=2}^{\log N} \widetilde{\mathrm{EQ}}(y_j; i_j)\right)_{\vec{\imath} \in \{0,1\}^{\log N - 1}}$

$\vec{Y}_R = y_1 \cdot \left(\prod_{j=2}^{\log N} \widetilde{\mathrm{EQ}}(y_j; i_j)\right)_{\vec{\imath} \in \{0,1\}^{\log N - 1}}$

$\vec{Y}' =$

$(x - xy_1 + y_1)\left(\prod_{j=2}^{\log N} \widetilde{\mathrm{EQ}}(y_j; i_j)\right)_{\vec{\imath} \in \{0,1\}^{\log N - 1}}$

$Y^{(\log N)} = \prod_{j=1}^{\log N} (x_j - x_j y_j + y_j)$

Costs $O(\log N)$ $\mathbb{F}$-ops

Final witness:

- element $f^{(\log N)} \in \mathbb{F}$

Final instance:

- commitment $C^{(\log N)} \in \mathbb{G}$, key $G^{(\log N)} \in \mathbb{G}$
- element $Y^{(\log N)} \in \mathbb{F}$, target $z^{(\log N)} \in \mathbb{F}$

Final language:

- $C^{(\log N)} = f^{(\log N)} \cdot G^{(\log N)} \in \mathbb{G}$
- $z^{(\log N)} = f^{(\log N)} \cdot Y^{(\log N)} \in \mathbb{Z}_p$

Plan for the next few lectures

Sumcheck protocol ✓

coNP ⊆ IP ✓
Extends to #SAT
(count SAT inputs)
Shows **#P ⊆ IP**

Interactive proof for layered arithmetic circuits ✓

Interactive oracle proofs for general arithmetic circuits ✓

Commitments and polynomial commitments

- DLOG construction ✓
- Efficiency improvements
- Adding zero-knowledge

ZK arguments for layered arithmetic circuits

ZK arguments for general arithmetic circuits