Theory and Practice of Succinct Zero Knowledge Proofs

Lecture 04:
PIOP for R1CS

Pratyush Mishra
UPenn
Fall 2023

A simple PIOP

Background on polynomials

Polynomial over $\mathbb{F}$:

$p(X) = a_0 + a_1X + \ldots + a_dX^d$ where $a_i \in \mathbb{F}$ and X takes values in $\mathbb{F}$.

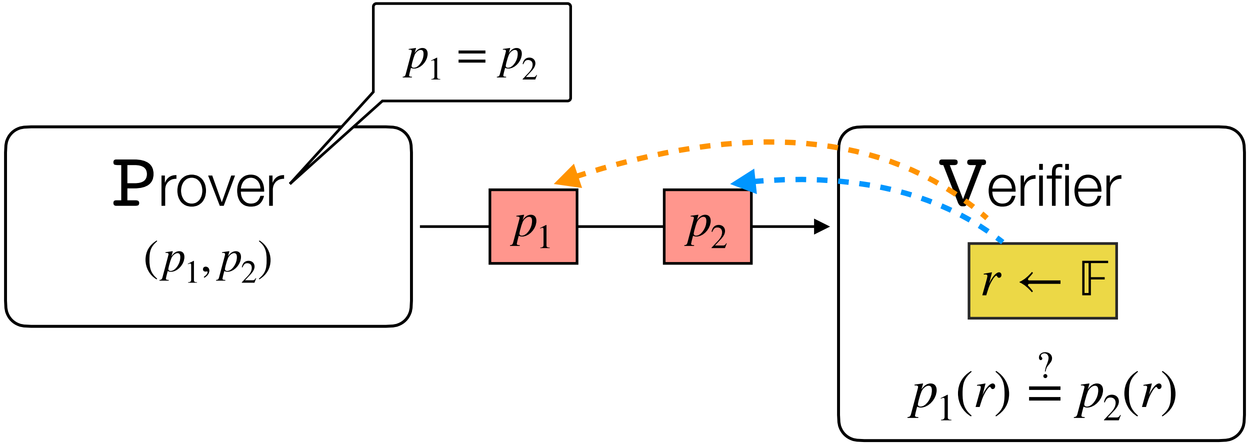
Polynomial Interpolation:

Given a list $A = (a_0, \ldots, a_d)$, and a set $H \subseteq \mathbb{F}$, we can interpolate A over H to obtain $p(X)$ such that $p(h_i) = a_i$ where h_i is the i-th element of H.

Vanishing polynomial:

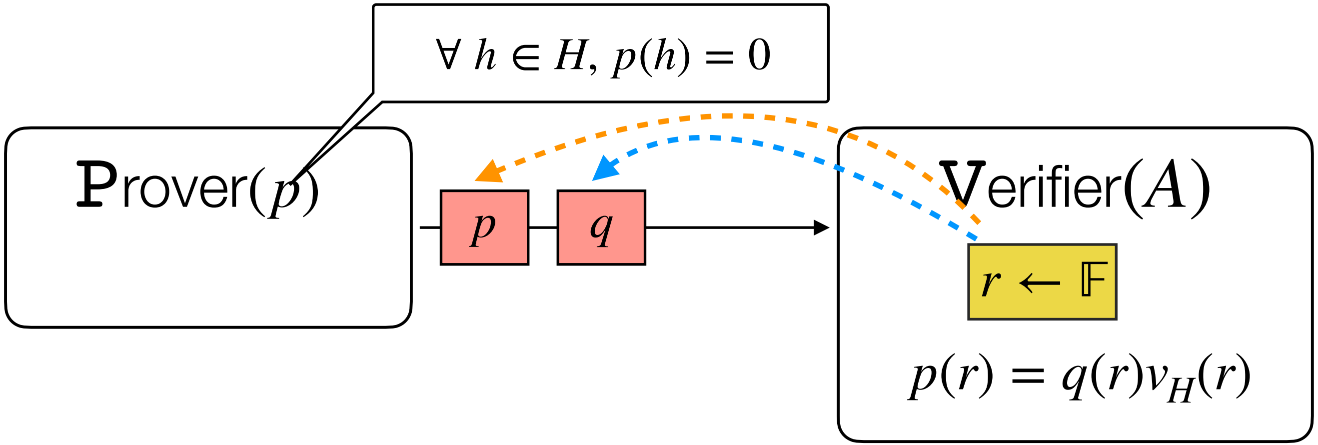
The vanishing polynomial for $H \subseteq \mathbb{F}$ is $v_H(X)$ such that $v_H(h) = 0 \;\; \forall\, h \in H$

Warmup: PIOP for Equality



- **Completeness**: If $p_1 = p_2$, then definitely $p_1(r) = p_2(r)$.
- **Soundness**: If $p_1 \neq p_2$, then $p_1(r) = p_2(r) \implies r$ is a root of $q := p_1 - p_2$. But since r is random, this happens with probability $\frac{\deg(q)}{|\mathbb{F}|}$

PIOP for ZeroCheck



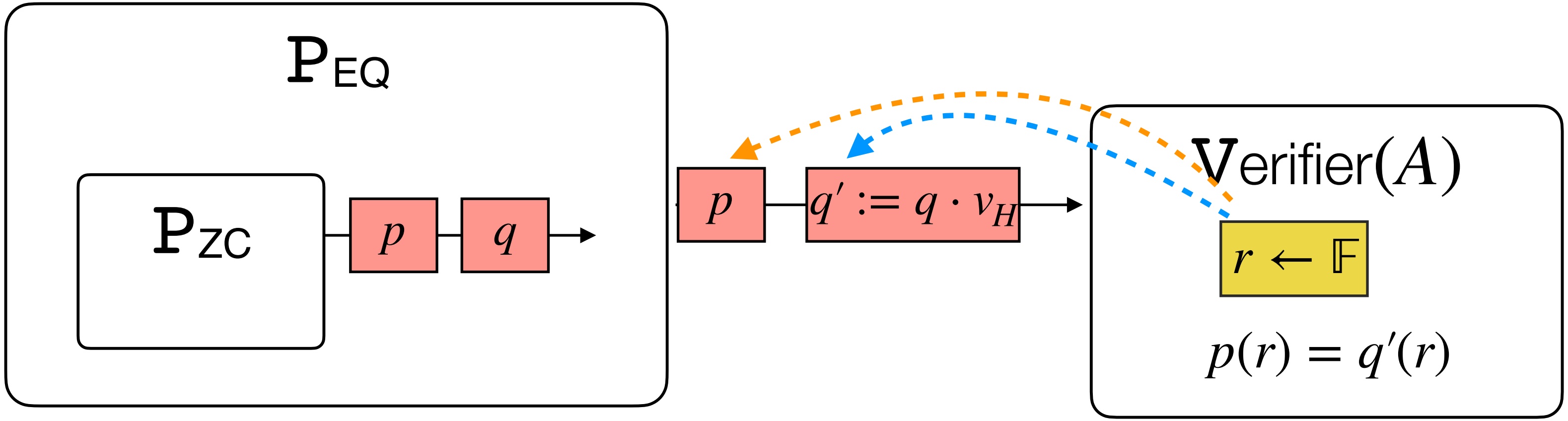
Lemma: $\forall h \in H,\ p(h) = 0$ if and only if $\exists q$ such that $p = q \cdot v_H$.

- **Completeness**: Follows from lemma, and completeness of previous PIOP.
- **Soundness**: The lemma means that we have to check only equality of polynomials via the previous PIOP, and so soundness reduces to that of the previous PIOP.

Soundness

Strategy: Use adversary $\mathbf{P}_{\text{ZC}}$ against PIOP for ZeroCheck

to get adversary $\mathbf{P}_{\text{EQ}}$ against PIOP for Equality



- **Soundness**: If $p \neq q \,.\, v_H$, but $p(r) = q(r) \cdot v_H(r)$, then $\mathbf{P}_{\text{EQ}}$ breaks soundness of the PIOP for Equality. But this happens with negligible probability, so $\mathbf{P}_{\text{ZC}}$ is successful with negl. Probability.

A PIOP for R1CS

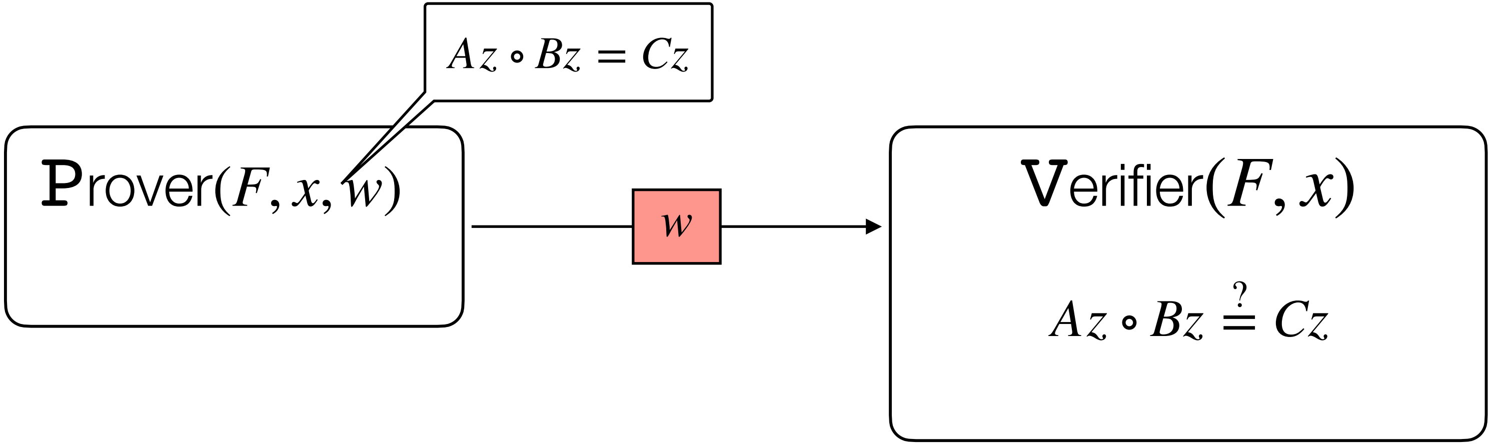
R1CS

An rank-1 constraint system (R1CS) is a generalization of arithmetic circuits

$$(F := (\mathbb{F}, n \in \mathbb{N}, A, B, C), x, w)$$

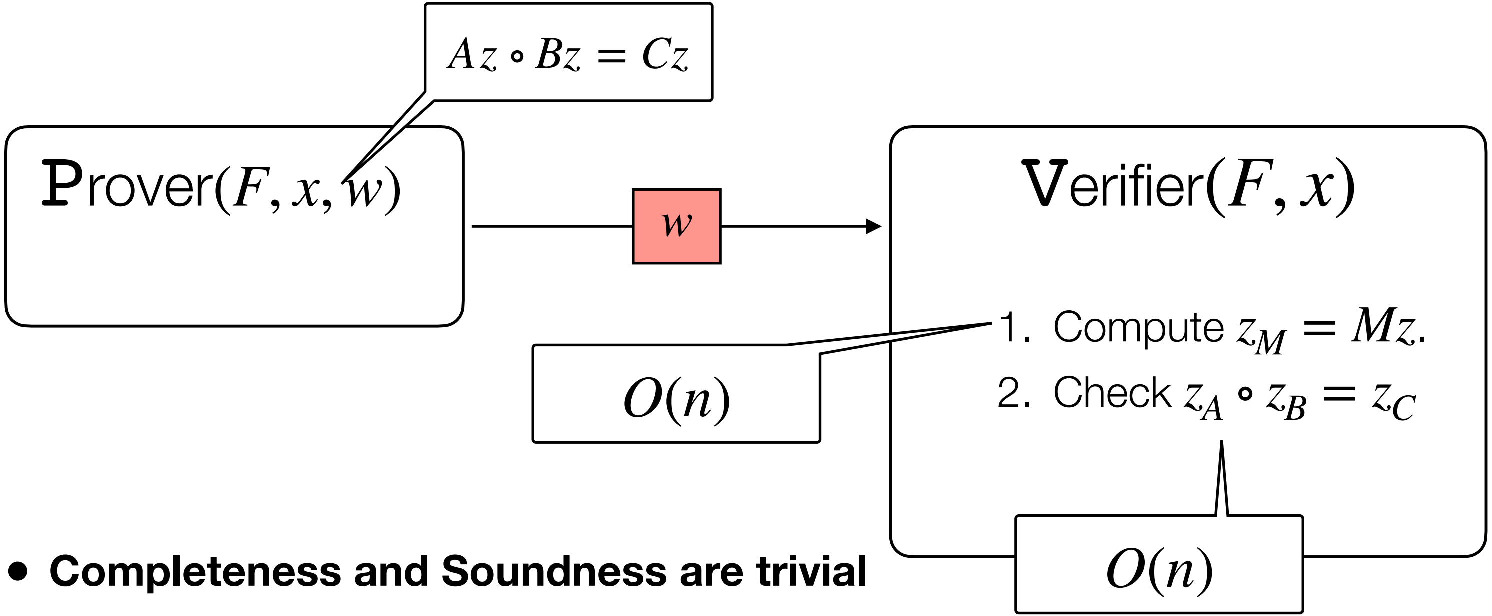
$$z := \begin{bmatrix} x \\ w \end{bmatrix} \quad n\left\{\overbrace{\begin{bmatrix} A \end{bmatrix}}^{n}\right. \begin{bmatrix} z \end{bmatrix} \circ \begin{bmatrix} B \end{bmatrix} \begin{bmatrix} z \end{bmatrix} = \begin{bmatrix} C \end{bmatrix} \begin{bmatrix} z \end{bmatrix}$$

Strawman 1



- **Completeness and Soundness are trivial**
- **What about efficiency?**

Strawman 1



- **Completeness and Soundness are trivial**
- **What about efficiency?**

What checks do we need?

Step 1: Correct Hadamard product

check that for each i, $z_A[i] \cdot z_B[i] = z_C[i]$

Step 2: Correct matrix multiplication

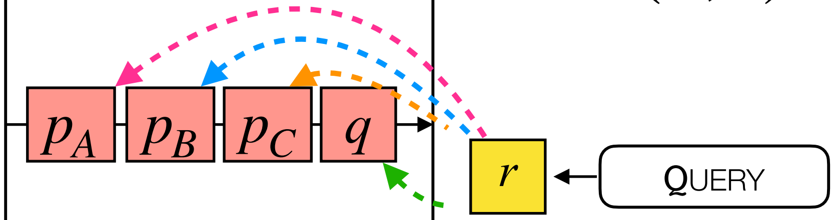
check that $Mz = z_M \quad \forall M \in \{A, B, C\}$

PIOP for Hadamard Product

Prover(F, x, w)

1. Let $H \subseteq \mathbb{F}$ be a set of size n.
2. Interpolate z_A, z_B, z_C over H to get p_A, p_B, p_C.
3. Compute quotient $q = \dfrac{p_A \cdot p_B - p_C}{v_H}$.

Verifier(F, x)



$$p_A(r) \cdot p_B(r) - p_C(r) \stackrel{?}{=} q(r) \cdot v_H(r)$$

Completeness

Let $p = p_A \cdot p_B - p_C$

If p_A, p_B, p_C are interpolations of z_A, z_B, z_C over H, then

$$p_A(h_i) = z_A[i]$$

for each i, we know that $p_B(h_i) = z_B[i]$.

$$p_C(h_i) = z_C[i]$$

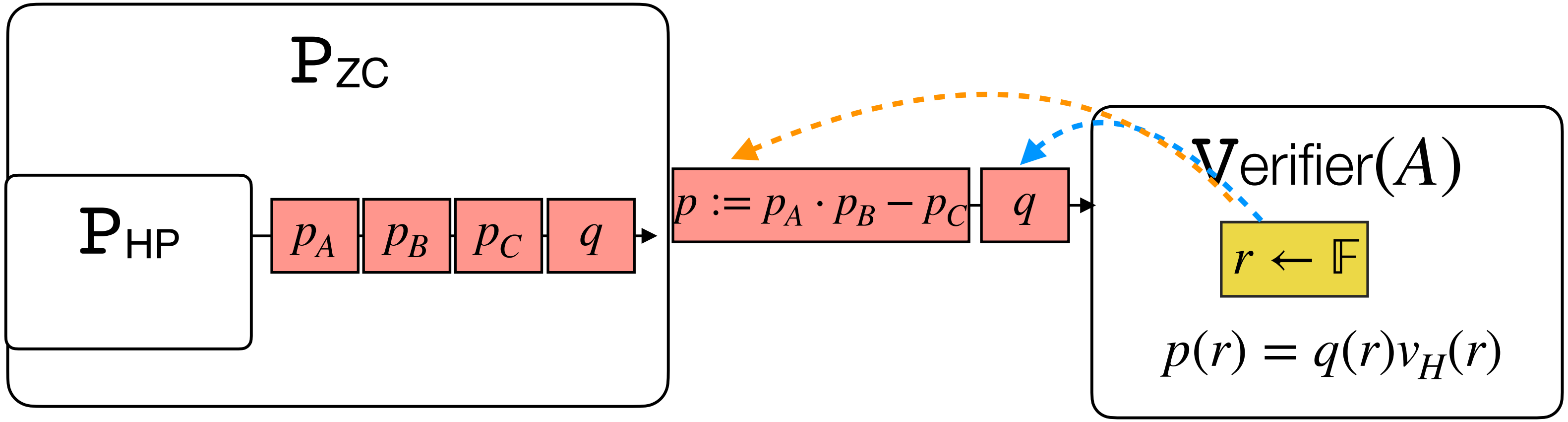
Since for each $z_A[i] \cdot z_B[i] = z_C[i]$, we know $p(h_i) = p_A(h_i) \cdot p_B(h_i) - p_C(h_i) = 0$

The rest follows from completeness of PIOP for ZeroCheck

Soundness

Strategy: Use adversary $\mathbf{P}_{\text{HP}}$ against PIOP for HP

to get adversary $\mathbf{P}_{\text{ZC}}$ against PIOP for ZeroCheck



If $\exists i$ such that $z_A[i] \cdot z_B[i] \neq z_C[i]$, then $p(h_i) \neq 0$, and so $p \neq q$ on H, which breaks soundness of the PIOP for ZeroCheck.

What checks do we need?

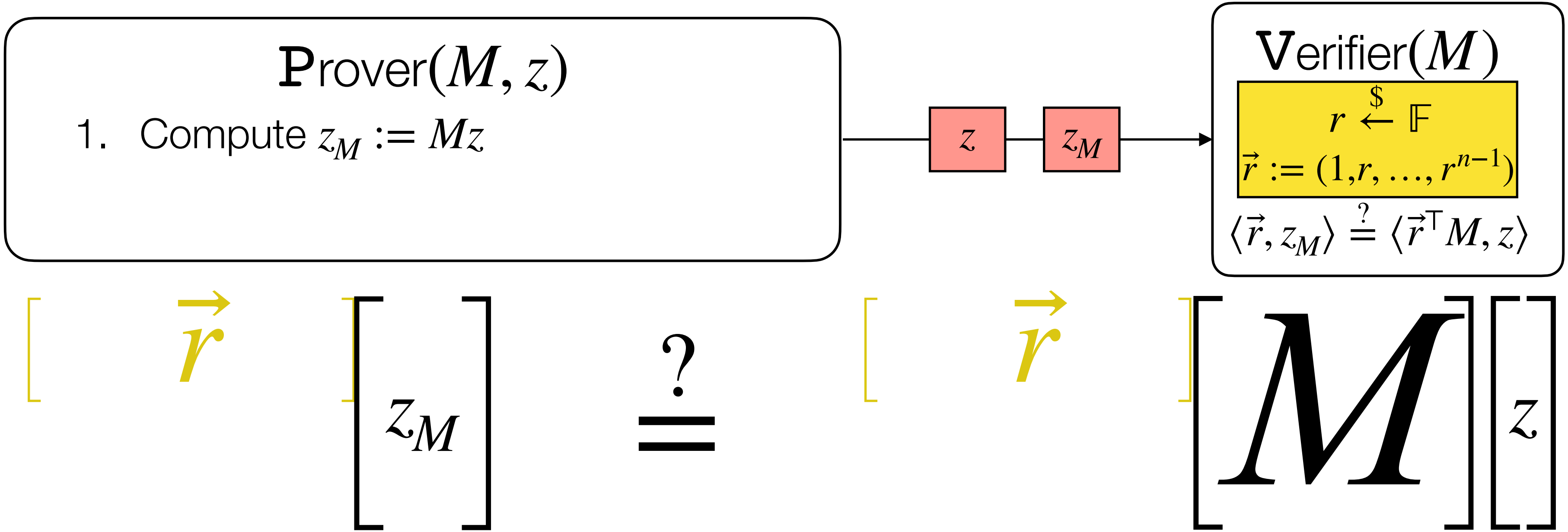
Step 1: Correct Hadamard product

check that for each i, $z_A[i] \cdot z_B[i] = z_C[i]$

Step 2: Correct matrix multiplication

check that $Mz = z_M \quad \forall M \in \{A, B, C\}$

Starting point: *IP* for MV checks



- **Soundness**: If there exists i such that $z_M[i] \neq Mz[i]$, then $\langle \vec{r}, z_M \rangle = \langle \vec{r}^\top M, z \rangle$ wp at most $1/|\mathbb{F}|$

Next point: *PIOP* for MV checks

Prover(M, z)

1. Compute $z_M := Mz$
2. Interpolate z_M over H to get $\hat{z}_M$

z — $\hat{z}_M$ →

Verifier(M)

1. $r \xleftarrow{\$} \mathbb{F}$
2. $\vec{r} := (1, r, \ldots, r^{n-1})$
3. Interpolate $(\vec{r}, \vec{r}^{\top} M)$ to get $(\hat{r}, \hat{r}_M)$

How to compute inner products $\langle \hat{r}, \hat{z}_M \rangle, \langle \hat{r}_M, \hat{z} \rangle$?

New tool: univariate sum check

Lemma:

$$\sum_{h \in H} p(h) = \sigma$$

$$\Updownarrow$$

$\exists\, q, g$ s.t.

$$p(X) = X g(X) + \frac{\sigma}{|H|} + q(X) \cdot v_H(X)$$

Reduce sumcheck to Zero check!

Sumcheck → Inner product check

For vectors, we have that $\langle \vec{a}, \vec{b} \rangle = \sum_{i=1}^{n} a_i b_i$

What if $(\vec{a}, \vec{b})$ are represented as their interpolations $(\hat{a}, \hat{b})$?

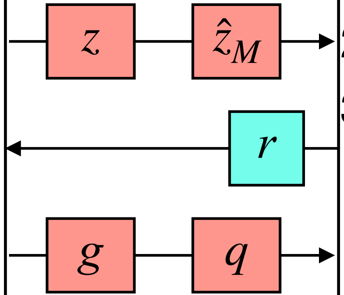
Ans: $\sum_{i=1}^{n} a_i b_i = \sum_{h \in H} \hat{a}(h) \cdot \hat{b}(h)$

Next point: *PIOP* for MV checks

Prover(M, z)

1. Compute $z_M := Mz$
2. Interpolate z_M over H to get $\hat{z}_M$
3. Interpolate $(\vec{r}, \vec{r}^\top M)$ to get $(\hat{r}, \hat{r}_M)$
4. Use sumcheck lemma to compute g, q such that

$$\hat{r}(X) \cdot \hat{z}_M(X) - \hat{r}_M(X) \cdot \hat{z}(X) = X \cdot g(X) + q(X) v_H(X)$$



Verifier(M)

1. $r \xleftarrow{\$} \mathbb{F}$
2. $\vec{r} := (1, r, \ldots, r^{n-1})$
3. Interpolate $(\vec{r}, \vec{r}^\top M)$ to get $(\hat{r}, \hat{r}_M)$
4. Invoke PIOP for ZC!