Faithful Homomorphisms and PIT – a short survey

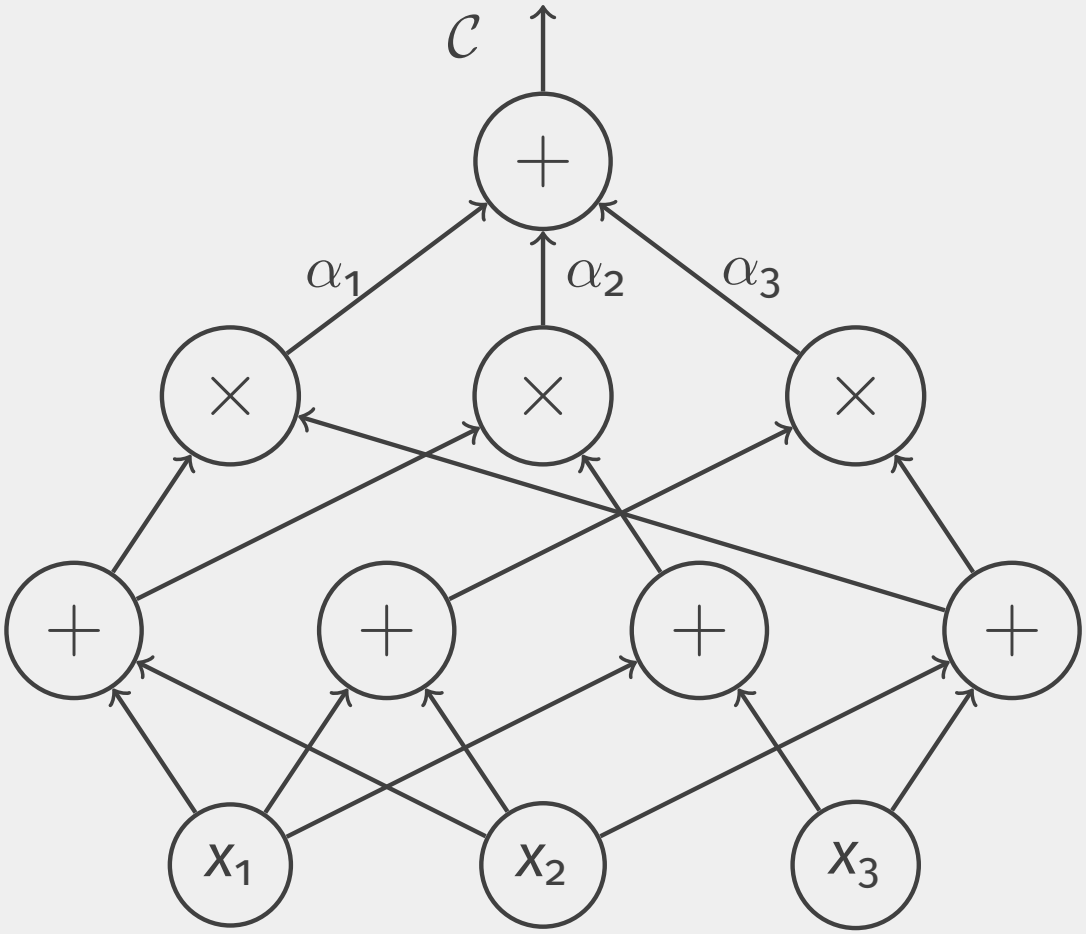
Prerona Chatterjee
based on joint work with *Ramprasad Saptharishi*

IIT Kanpur

November 3, 2018

Introduction

Polynomial Identity Testing



$$C \stackrel{?}{=} 0$$

The Trivial Solution & What is Required

Given: n-variate, degree d polynomial
Size of trivial hitting set: $(d+1)^n$

The Trivial Solution & What is Required

Given: n-variate, degree d polynomial
Size of trivial hitting set: $(d+1)^n$

Approach: Reduce number of variables + Preserve non-zeroness

The Trivial Solution & What is Required

Given: n-variate, degree d polynomial
Size of trivial hitting set: $(d+1)^n$

Approach: Reduce number of variables + Preserve non-zeroness

Trivial Substitution: $x_i \to t^{(d+1)^i}$
distinct monomials $\to$ distinct power in t $\implies$ No Cancellations

The Trivial Solution & What is Required

Given: n-variate, degree d polynomial
Size of trivial hitting set: $(d+1)^n$

Approach: Reduce number of variables + Preserve non-zeroness

Trivial Substitution: $x_i \to t^{(d+1)^i}$
distinct monomials $\to$ distinct power in t $\implies$ No Cancellations
No. of variables: 1 **Degree**: $(d+1)^n$ **|Hitting Set|**: $(d+1)^n$

The Trivial Solution & What is Required

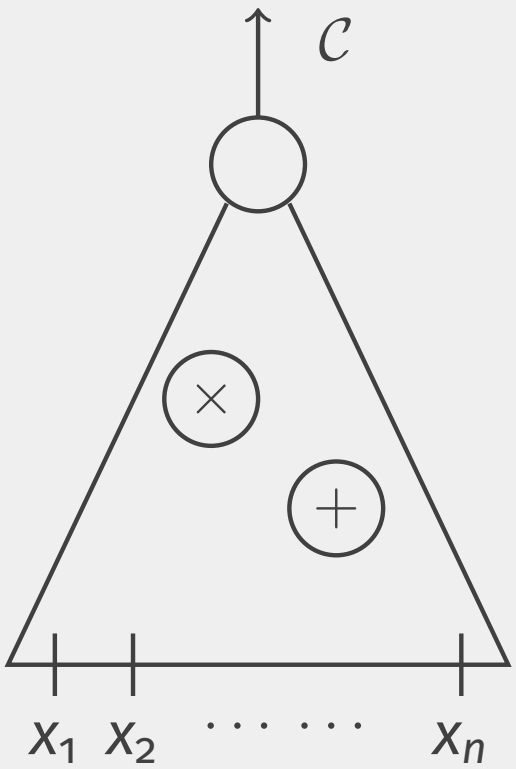
Given: n-variate, degree d polynomial
Size of trivial hitting set: $(d+1)^n$

Approach: Reduce number of variables + Preserve non-zeroness

Trivial Substitution: $x_i \to t^{(d+1)^i}$
distinct monomials $\to$ distinct power in t $\implies$ No Cancellations
No. of variables: 1 **Degree**: $(d+1)^n$ **|Hitting Set|**: $(d+1)^n$

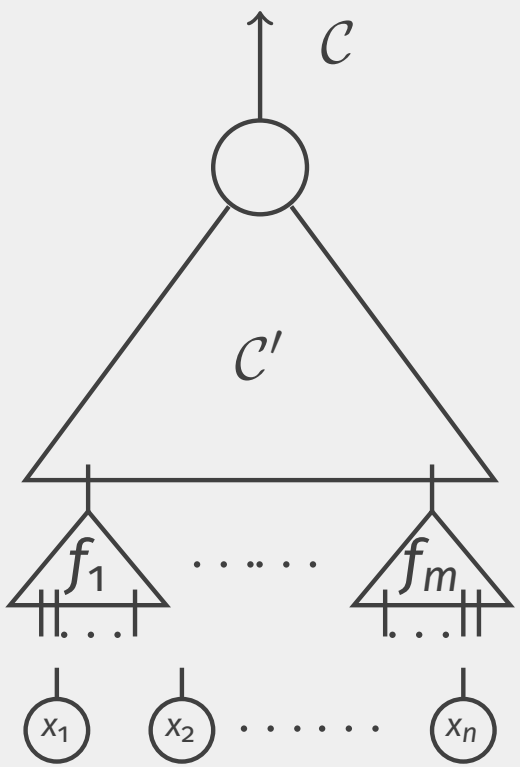
What we need: Reduce no. of variables (preferably constant)
Keep degree under control (poly-bounded)
Preserve non-zeroness

A Special Setting: Can we do better?



Check whether $\mathcal{C}$ computes the zero polynomial or not.

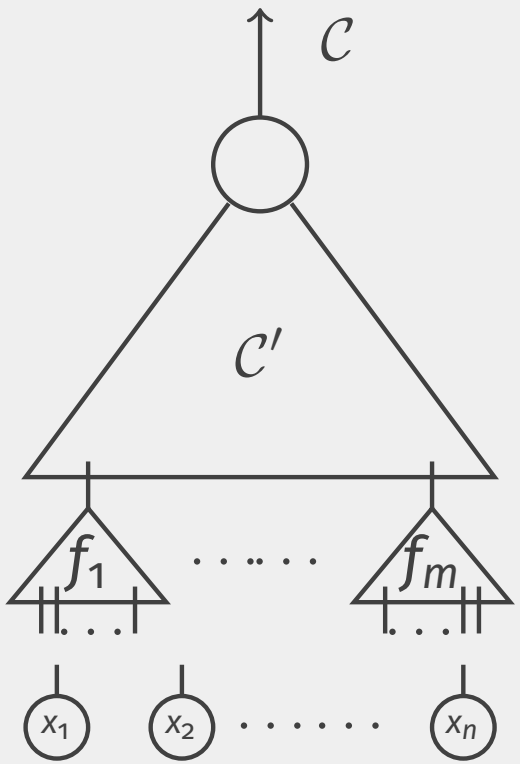
A Special Setting: Can we do better?



Check whether $\mathcal{C}$ computes the zero polynomial or not.

$$\mathcal{C} = \mathcal{C}'(f_1, f_2, \ldots, f_m)$$

A Special Setting: Can we do better?



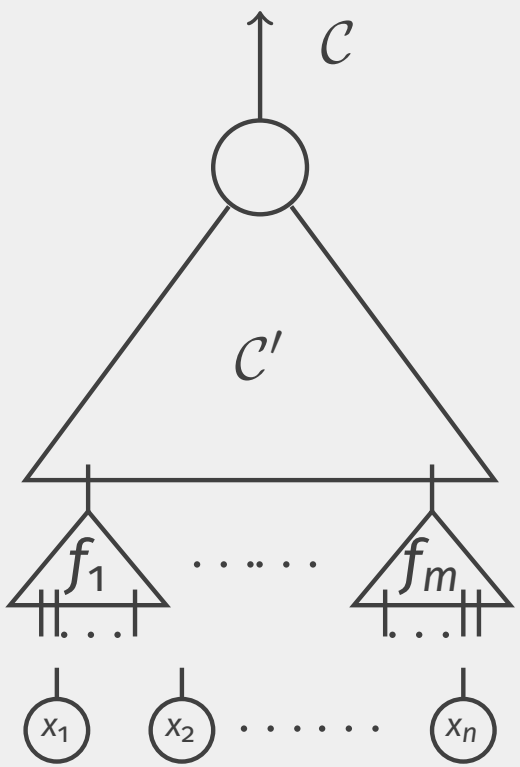
Check whether $\mathcal{C}$ computes the zero polynomial or not.

$$\mathcal{C} = \mathcal{C}'(f_1, f_2, \ldots, f_m)$$

Only k of them are "relevant" where

$$k << n$$

A Special Setting: Can we do better?



Check whether $\mathcal{C}$ computes the zero polynomial or not.

$$\mathcal{C} = \mathcal{C}'(f_1, f_2, \ldots, f_m)$$

Only k of them are "relevant" where

$$k << n$$

Can we do any better than trivial?

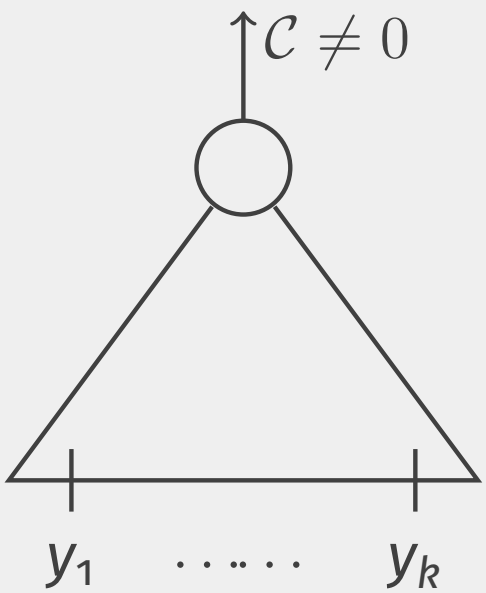
Preliminaries

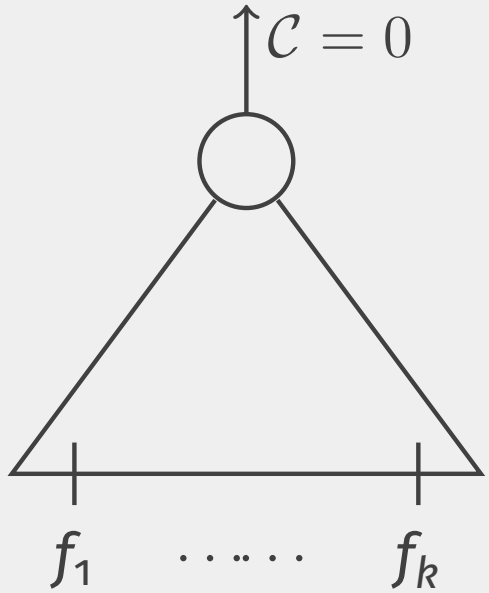
Algebraic Independence

Definition: Suppose $\{f_1, \ldots, f_k\} \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n]$. They are said to be algebraically dependent if there exists $A \in \mathbb{F}[y_1, \ldots, y_k]$ such that

$$A(y_1, \ldots, y_k) \neq 0; \qquad A(f_1, \ldots, f_k) = 0.$$

Otherwise, they are said to be algebraically independent.



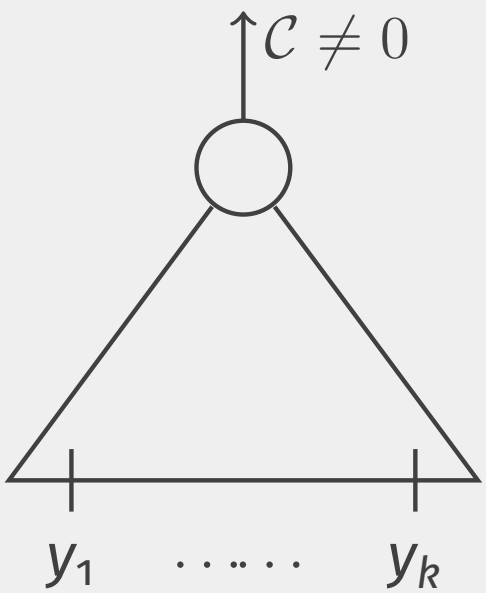


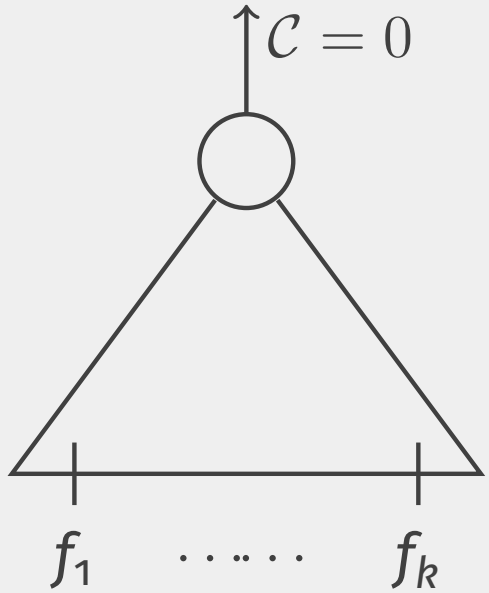
Algebraic Independence

Definition: Suppose $\{f_1, \ldots, f_k\} \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n]$. They are said to be algebraically dependent if there exists $A \in \mathbb{F}[y_1, \ldots, y_k]$ such that

$$A(y_1, \ldots, y_k) \neq 0; \qquad A(f_1, \ldots, f_k) = 0.$$

Otherwise, they are said to be algebraically independent.



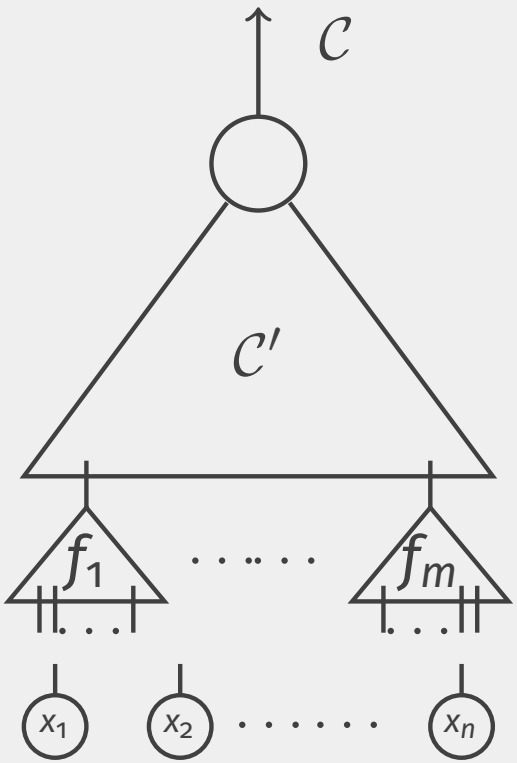


Algebraic Rank of $\{f_1, \ldots, f_m\}$

Size of the maximal algebraically independent subset of $\{f_1, \ldots, f_m\}$.

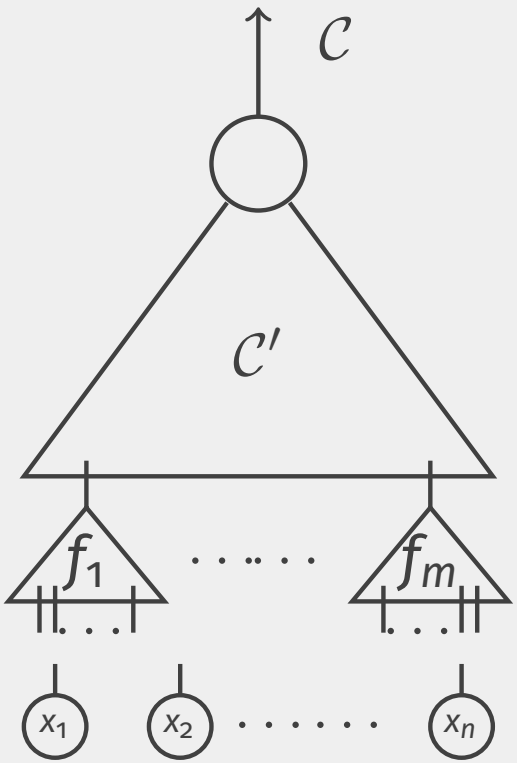
Our Setting: How is it different?

$$\mathcal{C} = \mathcal{C}'(f_1, \ldots f_m) : \text{algrank}(f_1, \ldots, f_m) = k << n$$



Our Setting: How is it different?

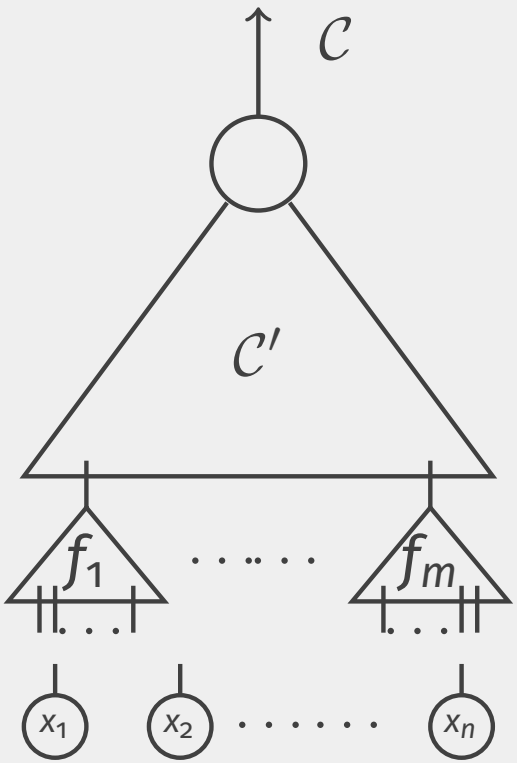
$$\mathcal{C} = \mathcal{C}'(f_1, \ldots f_m) : \text{algrank}(f_1, \ldots, f_m) = k << n$$



Easy Case: $k = m$
Have access to $\mathcal{C}'$

Our Setting: How is it different?

$$\mathcal{C} = \mathcal{C}'(f_1, \ldots f_m) : \text{algrank}(f_1, \ldots, f_m) = k << n$$

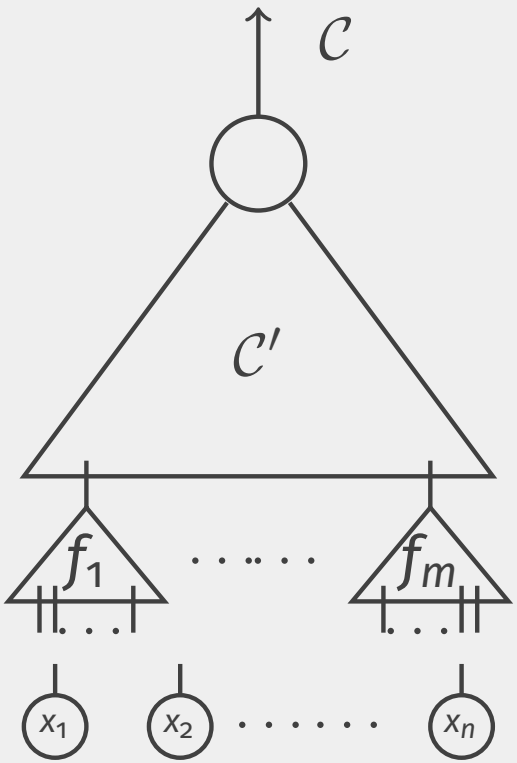


Easy Case: $k = m$
Have access to $\mathcal{C}'$

|Hitting Set| in this case: $(d+1)^k$

Our Setting: How is it different?

$$\mathcal{C} = \mathcal{C}'(f_1, \ldots f_m) : \text{algrank}(f_1, \ldots, f_m) = k << n$$



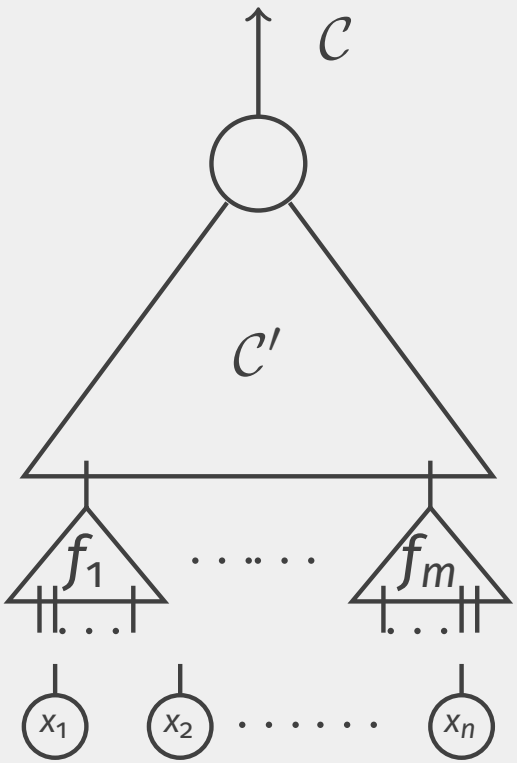
Easy Case: $k = m$
Have access to $\mathcal{C}'$

|Hitting Set| in this case: $(d+1)^k$

General Case: $k \neq m$
Do not have access to $\mathcal{C}'$

Our Setting: How is it different?

$$\mathcal{C} = \mathcal{C}'(f_1, \ldots f_m) : \text{algrank}(f_1, \ldots, f_m) = k << n$$



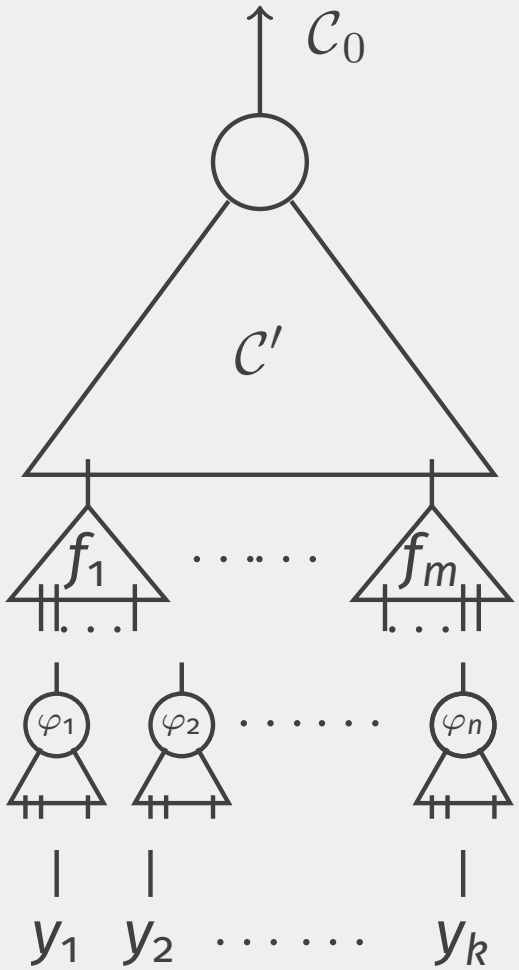
Easy Case: $k = m$
Have access to $\mathcal{C}'$

|Hitting Set| in this case: $(d+1)^k$

General Case: $k \neq m$
Do not have access to $\mathcal{C}'$

What is allowed: Substitute x_is

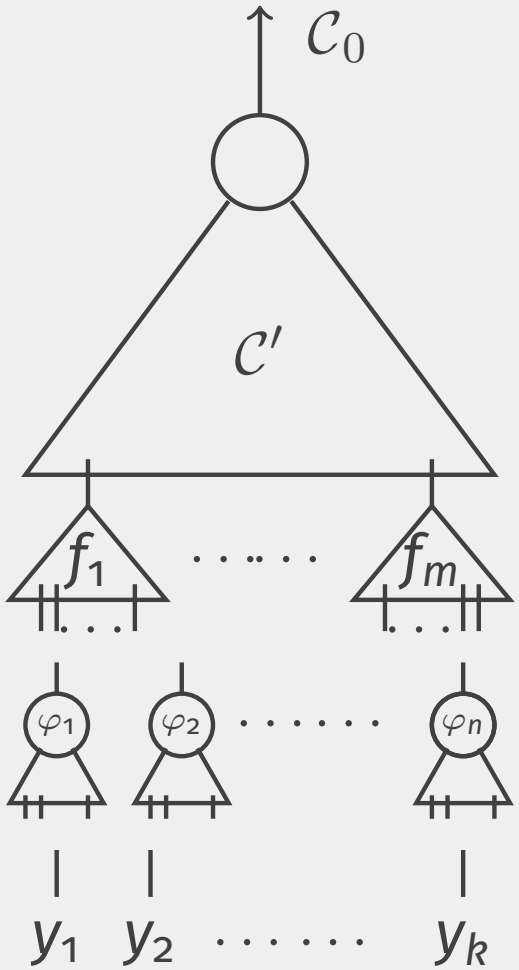
Our Setting: What can be done?



$x_i \to \varphi_i(y_1, \ldots, y_k)$

Property required: $\mathcal{C} \neq 0 \implies \mathcal{C}_0 \neq 0$

Our Setting: What can be done?



$x_i \to \varphi_i(y_1, \ldots, y_k)$

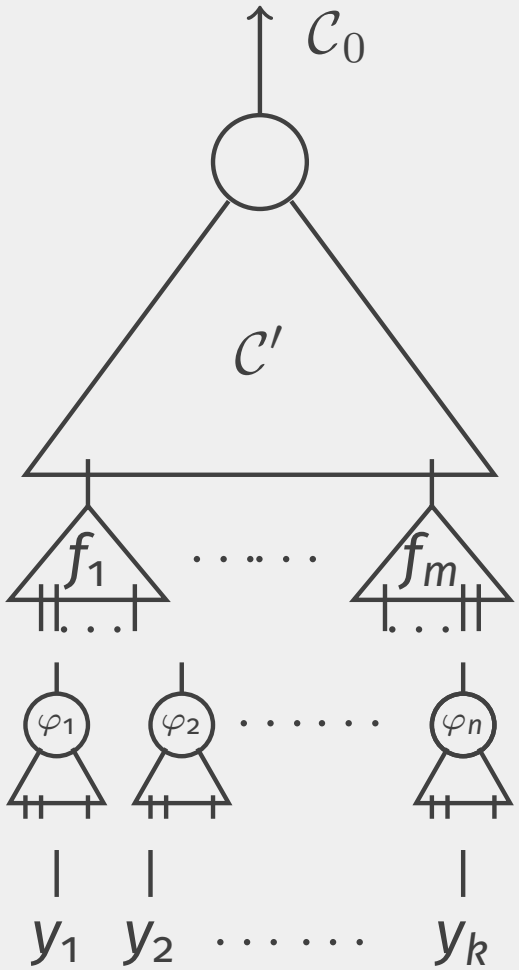
Property required: $\mathcal{C} \neq 0 \implies \mathcal{C}_0 \neq 0$

For $k = m$, **sufficient property** of φ_i's:

$$g_i = f_i(\varphi_1, \ldots, \varphi_n)$$

$\{f_1, \ldots, f_k\}$ are A.I. $\Leftrightarrow$ $\{g_1, \ldots, g_k\}$ are A.I.

Our Setting: What can be done?



$x_i \to \varphi_i(y_1, \ldots, y_k)$

Property required: $\mathcal{C} \neq 0 \implies \mathcal{C}_0 \neq 0$

For $k = m$, **sufficient property** of φ_i's:

$$g_i = f_i(\varphi_1, \ldots, \varphi_n)$$

$\{f_1, \ldots, f_k\}$ are A.I. $\Leftrightarrow$ $\{g_1, \ldots, g_k\}$ are A.I.

Amazing fact [BMS'11, ASSS'12]:
Works even in the general case ($k < m$).

Faithful Maps

Definition: Let $\{f_1, \ldots, f_m\} \subseteq \mathbb{F}[\mathbf{x}]$ with $\operatorname{algrank}(f_1, \ldots, f_m) = k$. A map

$$\varphi : \{x_1, \ldots x_n\} \to \mathbb{F}[y_1, y_2, \ldots, y_k]$$

is said to be faithful if $\operatorname{algrank}(g_1, \ldots, g_m) = k$.
Here $g_i(\mathbf{y}) = f_i(\varphi(x_1), \ldots, \varphi(x_n))$.

Faithful Maps

Definition: Let $\{f_1, \ldots, f_m\} \subseteq \mathbb{F}[\mathbf{x}]$ with $\operatorname{algrank}(f_1, \ldots, f_m) = k$. A map

$$\varphi : \{x_1, \ldots x_n\} \to \mathbb{F}[y_1, y_2, \ldots, y_k]$$

is said to be faithful if $\operatorname{algrank}(g_1, \ldots, g_m) = k$.
Here $g_i(\mathbf{y}) = f_i(\varphi(x_1), \ldots, \varphi(x_n))$.

Why should one believe that such maps can exist?
What we know: If $\{f_1, \ldots, f_k\}$ are algebraically independent, then

$$\mathbb{F}(f_1, \ldots, f_k) \cong \mathbb{F}(y_1, \ldots, y_k).$$

Faithful Maps

Definition: Let $\{f_1, \ldots, f_m\} \subseteq \mathbb{F}[\mathbf{x}]$ with $\operatorname{algrank}(f_1, \ldots, f_m) = k$. A map

$$\varphi : \{x_1, \ldots x_n\} \to \mathbb{F}[y_1, y_2, \ldots, y_k]$$

is said to be faithful if $\operatorname{algrank}(g_1, \ldots, g_m) = k$.
Here $g_i(\mathbf{y}) = f_i(\varphi(x_1), \ldots, \varphi(x_n))$.

Why should one believe that such maps can exist?
What we know: If $\{f_1, \ldots, f_k\}$ are algebraically independent, then

$$\mathbb{F}(f_1, \ldots, f_k) \cong \mathbb{F}(y_1, \ldots, y_k).$$

What we are asking for: A better way of seeing this isomorphism.
That is, are there $g_1, \ldots, g_k \in \mathbb{F}[y_1, \ldots y_k]$ such that
$g_i = f_i(\varphi(x_1), \ldots, \varphi(x_n))$ and

$$\mathbb{F}(f_1, \ldots, f_k) \cong \mathbb{F}(g_1, \ldots, g_k)?$$

Constructing Faithful Maps are enough

Lemma [BMS'11, ASSS'12]

If φ is a faithful map for $\{f_1, \ldots, f_m\} \subseteq \mathbb{F}[\mathbf{x}]$, then for any $\mathcal{C}$

$$\mathcal{C}(f_1, \ldots, f_m) \neq 0 \implies \mathcal{C}(f_1 \circ \varphi, \ldots, f_m \circ \varphi) \neq 0$$

Constructing Faithful Maps are enough

Lemma [BMS'11, ASSS'12]

If φ is a faithful map for $\{f_1, \ldots, f_m\} \subseteq \mathbb{F}[\mathbf{x}]$, then for any $\mathcal{C}$

$$\mathcal{C}(f_1, \ldots, f_m) \neq 0 \implies \mathcal{C}(f_1 \circ \varphi, \ldots, f_m \circ \varphi) \neq 0$$

Proof: Let $g_i = f_i(\varphi(x_1), \ldots, \varphi(x_n))$.

$$\begin{aligned}
&\mathcal{C}[f_1, \ldots, f_m] \neq 0 \Rightarrow \mathcal{C}(f_1, \ldots, f_m) \neq 0 \\
&\Rightarrow \mathcal{C}(f_1, \ldots, f_m) \cdot R(f_1, \ldots, f_m) = 1 \\
&\Rightarrow \mathcal{C}(f_1, \ldots, f_m) \cdot R'[f_1, \ldots, f_m] = Q[f_1, \ldots, f_k] \\
&\Rightarrow \mathcal{C}(g_1, \ldots, g_m) \cdot R'[g_1, \ldots, g_m] \\
&\qquad\qquad = Q[g_1, \ldots, g_k] \neq 0 \\
&\Rightarrow \mathcal{C}(g_1, \ldots, g_m) = \mathcal{C}(f_1 \circ \varphi, \ldots, f_m \circ \varphi) \neq 0
\end{aligned}$$

Useful fact

$\mathbb{F}(f_1, \ldots, f_m)$ | $\mathbb{F}(f_1, \ldots, f_k)$ is an algebraic extension. Thus, $R(f_1, \ldots, f_m)$

$$= \frac{R'[f_1, \ldots, f_m]}{Q[f_1, \ldots, f_k]}$$

Linear Rank Extractors [GR'05]

$$\begin{bmatrix} \\ A \\ \\ \end{bmatrix} \times \begin{bmatrix} s & \dots & s^k \\ (s^2)^1 & \dots & (s^2)^k \\ \vdots & & \vdots \\ \vdots & \ddots & \vdots \\ \vdots & \ddots & \vdots \\ \vdots & & \vdots \\ (s^n)^1 & \dots & (s^n)^k \end{bmatrix} = \begin{bmatrix} \\ A' \\ \\ \end{bmatrix}$$

A has full $\mathbb{F}$-rank

$\implies$ $\det(A')$ is a non-zero polynomial in s of degree at most nk^2

$\implies$ A' has full $\mathbb{F}(s)$-rank

$\implies$ For some $s \in \{0, \dots, nk^2\}$ A' has full $\mathbb{F}$-rank

Capturing Algebraic Rank via Linear Rank

For $f_1, f_2, \ldots, f_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ and $\mathbf{f} = (f_1, f_2, \ldots, f_m)$,

$$\mathbf{J}_{\mathbf{x}}(\mathbf{f}) = \begin{bmatrix} \partial_{x_1}(f_1) & \partial_{x_2}(f_1) & \cdots & \partial_{x_n}(f_1) \\ \partial_{x_1}(f_2) & \partial_{x_2}(f_2) & \cdots & \partial_{x_n}(f_2) \\ \vdots & \vdots & \ddots & \vdots \\ \partial_{x_1}(f_m) & \partial_{x_2}(f_m) & \cdots & \partial_{x_n}(f_m) \end{bmatrix}$$

Capturing Algebraic Rank via Linear Rank

For $f_1, f_2, \ldots, f_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ and $\mathbf{f} = (f_1, f_2, \ldots, f_m)$,

$$\mathbf{J_x}(\mathbf{f}) = \begin{bmatrix} \partial_{x_1}(f_1) & \partial_{x_2}(f_1) & \ldots & \partial_{x_n}(f_1) \\ \partial_{x_1}(f_2) & \partial_{x_2}(f_2) & \ldots & \partial_{x_n}(f_2) \\ \vdots & \vdots & \ddots & \vdots \\ \partial_{x_1}(f_m) & \partial_{x_2}(f_m) & \ldots & \partial_{x_n}(f_m) \end{bmatrix}$$

The Jacobian Criterion

If $\mathbb{F}$ has characteristic zero, the algebraic rank of $\{f_1, f_2, \ldots, f_m\}$ is equal to the linear rank of its Jacobian matrix.

Characteristic Zero Fields: [Jac'41], [BMS'11], [ASSS'12]

The Goal

What we need: $\mathbf{J_x}(\mathbf{f})$ has full rank $\implies$ $\mathbf{J_y}(\mathbf{f} \circ \varphi)$ has full rank

The Goal

What we need: $\mathbf{J_x}(\mathbf{f})$ has full rank $\implies$ $\mathbf{J_y}(\mathbf{f} \circ \varphi)$ has full rank

What we can do: Write $\mathbf{J_y}(\mathbf{f} \circ \varphi)$ in terms of $\mathbf{J_x}(\mathbf{f})$.

The Goal

What we need: $\mathbf{J_x}(\mathbf{f})$ has full rank $\implies$ $\mathbf{J_y}(\mathbf{f} \circ \varphi)$ has full rank

What we can do: Write $\mathbf{J_y}(\mathbf{f} \circ \varphi)$ in terms of $\mathbf{J_x}(\mathbf{f})$.

Suppose φ is a generic linear map: $\varphi : x_i = \sum_{j=1}^{k} a_{ij} y_j + b_i$.

The Goal

What we need: $\mathbf{J_x}(\mathbf{f})$ has full rank $\implies$ $\mathbf{J_y}(\mathbf{f} \circ \varphi)$ has full rank

What we can do: Write $\mathbf{J_y}(\mathbf{f} \circ \varphi)$ in terms of $\mathbf{J_x}(\mathbf{f})$.

Suppose φ is a generic linear map: $\varphi : x_i = \sum_{j=1}^{k} a_{ij} y_j + b_i$.
Then for $M_\varphi[i, j] = a_{ij}$,

$$\begin{bmatrix} \\ \mathbf{J_y}(\mathbf{f} \circ \varphi) \\ \\ \end{bmatrix} = \begin{bmatrix} \\ \varphi(\mathbf{J_x}(\mathbf{f})) \\ \\ \end{bmatrix} \times \begin{bmatrix} \\ M_\varphi \\ \\ \end{bmatrix}$$

The Revised Goal & The Solution

What we need: $M_\varphi[i,j] = s^{ij}$: Easy (define a_{ij} to be s^{ij})

The Revised Goal & The Solution

What we need: $M_\varphi[i,j] = s^{ij}$: Easy (define a_{ij} to be s^{ij})
$\mathbf{J_x}(\mathbf{f})$ has full rank $\implies$ $\varphi(\mathbf{J_x}(\mathbf{f}))$ has full rank

The Revised Goal & The Solution

What we need: $M_\varphi[i,j] = s^{ij}$: Easy (define a_{ij} to be s^{ij})
$\mathbf{J_x}(\mathbf{f})$ has full rank $\implies$ $\varphi(\mathbf{J_x}(\mathbf{f}))$ has full rank

How to ensure $\mathbf{J_x}(\mathbf{f})$ has full rank $\implies$ $\varphi(\mathbf{J_x}(\mathbf{f}))$ has full rank:

- $\mathcal{S}$: Hitting set for the family of all $k \times k$ minors of $\mathbf{J_x}(\mathbf{f})$

The Revised Goal & The Solution

What we need: $M_\varphi[i,j] = s^{ij}$: Easy (define a_{ij} to be s^{ij})
$\mathbf{J_x}(\mathbf{f})$ has full rank $\implies$ $\varphi(\mathbf{J_x}(\mathbf{f}))$ has full rank

How to ensure $\mathbf{J_x}(\mathbf{f})$ has full rank $\implies$ $\varphi(\mathbf{J_x}(\mathbf{f}))$ has full rank:

- $\mathcal{S}$: Hitting set for the family of all $k \times k$ minors of $\mathbf{J_x}(\mathbf{f})$
- Choose $\mathbf{b}$ to be points from $\mathcal{S}$

The Revised Goal & The Solution

What we need: $M_\varphi[i,j] = s^{ij}$: Easy (define a_{ij} to be s^{ij})
$\mathbf{J_x}(\mathbf{f})$ has full rank $\implies$ $\varphi(\mathbf{J_x}(\mathbf{f}))$ has full rank

How to ensure $\mathbf{J_x}(\mathbf{f})$ has full rank $\implies$ $\varphi(\mathbf{J_x}(\mathbf{f}))$ has full rank:

- $\mathcal{S}$: Hitting set for the family of all $k \times k$ minors of $\mathbf{J_x}(\mathbf{f})$
- Choose $\mathbf{b}$ to be points from $\mathcal{S}$

What we get: $\mathcal{F} = \left\{\varphi_{s,\mathbf{b}} = \sum_{j=1}^{k} s^{ij} y_j + b_i\right\}_{s\in\{0,\ldots,nk^2\},\mathbf{b}\in\mathcal{S}}$

The Revised Goal & The Solution

What we need: $M_\varphi[i,j] = s^{ij}$: Easy (define a_{ij} to be s^{ij})
$\mathbf{J_x}(\mathbf{f})$ has full rank $\implies$ $\varphi(\mathbf{J_x}(\mathbf{f}))$ has full rank

How to ensure $\mathbf{J_x}(\mathbf{f})$ has full rank $\implies$ $\varphi(\mathbf{J_x}(\mathbf{f}))$ has full rank:

- $\mathcal{S}$: Hitting set for the family of all $k \times k$ minors of $\mathbf{J_x}(\mathbf{f})$
- Choose $\mathbf{b}$ to be points from $\mathcal{S}$

What we get: $\mathcal{F} = \left\{\varphi_{s,\mathbf{b}} = \sum_{j=1}^{k} s^{ij} y_j + b_i\right\}_{s\in\{0,\ldots,nk^2\},\mathbf{b}\in\mathcal{S}}$

Guarantee: If $\mathcal{C} = \mathcal{C}'(f_1,\ldots,f_m) \neq 0$, then for some $\varphi \in \mathcal{F}$,
$\mathcal{C}_0 = \mathcal{C}'(f_1 \circ \varphi,\ldots,f_m \circ \varphi) \neq 0.$

Some Instantiations

The PIT Algorithm

Input: $\mathcal{C} = \mathcal{C}'(f_1, \ldots, f_m)$, $k \geq \text{algrank}(f_1, \ldots, f_m)$

Some Instantiations

The PIT Algorithm

Input: $\mathcal{C} = \mathcal{C}'(f_1, \ldots, f_m)$, $k \geq \text{algrank}(f_1, \ldots, f_m)$

Step 1: For every $\varphi \in \mathcal{F}$ not tried yet.
Run trivial PIT on $\mathcal{C}_0 = \mathcal{C}'(f_1 \circ \varphi, \ldots, f_m \circ \varphi)$
If $\mathcal{C}_0 \neq 0$, return "NOT ZERO".

Step 2: Return "ZERO".

Some Instantiations

The PIT Algorithm

Input: $\mathcal{C} = \mathcal{C}'(f_1, \ldots, f_m)$, $k \geq \text{algrank}(f_1, \ldots, f_m)$

Step 1: For every $\varphi \in \mathcal{F}$ not tried yet.
Run trivial PIT on $\mathcal{C}_0 = \mathcal{C}'(f_1 \circ \varphi, \ldots, f_m \circ \varphi)$
If $\mathcal{C}_0 \neq 0$, return "NOT ZERO".

Step 2: Return "ZERO".

When is it useful? k is a constant and $|\mathcal{S}| \leq \text{poly}(n)$.

Some Instantiations

The PIT Algorithm

Input: $\mathcal{C} = \mathcal{C}'(f_1, \ldots, f_m)$, $k \geq \text{algrank}(f_1, \ldots, f_m)$

Step 1: For every $\varphi \in \mathcal{F}$ not tried yet.
Run trivial PIT on $\mathcal{C}_0 = \mathcal{C}'(f_1 \circ \varphi, \ldots, f_m \circ \varphi)$
If $\mathcal{C}_0 \neq 0$, return "NOT ZERO".

Step 2: Return "ZERO".

When is it useful? k is a constant and $|\mathcal{S}| \leq \text{poly}(n)$.

Some Examples: $\mathcal{C} = \mathcal{C}'(f_1, \ldots, f_m)$ where

- each f_i is a sparse polynomial
- each f_i is a product of multilinear, variable disjoint, sparse polynomials
- each f_i is a product of linear polynomials

Arbitrary Fields: The PSS Criterion [PSS'16]

What goes wrong over arbitrary fields?

Jacobian Matrix has partial derivatives as entries

What goes wrong over arbitrary fields?

Jacobian Matrix has partial derivatives as entries - Entries can start becoming zero

What goes wrong over arbitrary fields?

Jacobian Matrix has partial derivatives as entries - Entries can start becoming zero : Not the only case.

What goes wrong over arbitrary fields?

Jacobian Matrix has partial derivatives as entries - Entries can start becoming zero : Not the only case.

$f_1 = xy^{p-1}, f_2 = x^{p-1}y$: Algebraically Independent over $\mathbb{F}_p$.

What goes wrong over arbitrary fields?

Jacobian Matrix has partial derivatives as entries - Entries can start becoming zero : Not the only case.

$f_1 = xy^{p-1}, f_2 = x^{p-1}y$: Algebraically Independent over $\mathbb{F}_p$.

$$\mathbf{J}_{x,y} = \begin{bmatrix} y^{p-1} & (p-1)xy^{p-2} \\ (p-1)x^{p-2}y & x^{p-1} \end{bmatrix}$$

$$\det(\mathbf{J}_{x,y}) = (xy)^{p-1} - (p^2 - 2p + 1)(xy)^{p-1} = 0 \text{ over } \mathbb{F}_p.$$

What goes wrong over arbitrary fields?

Jacobian Matrix has partial derivatives as entries - Entries can start becoming zero : Not the only case.

$f_1 = xy^{p-1}, f_2 = x^{p-1}y$: Algebraically Independent over $\mathbb{F}_p$.

$$\mathbf{J}_{x,y} = \begin{bmatrix} y^{p-1} & (p-1)xy^{p-2} \\ (p-1)x^{p-2}y & x^{p-1} \end{bmatrix}$$

$$\det(\mathbf{J}_{x,y}) = (xy)^{p-1} - (p^2 - 2p + 1)(xy)^{p-1} = 0 \text{ over } \mathbb{F}_p.$$

Characteristic Zero: **J** has full rank $\Leftarrow$ **J** has an inverse

What goes wrong over arbitrary fields?

Jacobian Matrix has partial derivatives as entries - Entries can start becoming zero : Not the only case.

$f_1 = xy^{p-1}, f_2 = x^{p-1}y$: Algebraically Independent over $\mathbb{F}_p$.

$$\mathbf{J}_{x,y} = \begin{bmatrix} y^{p-1} & (p-1)xy^{p-2} \\ (p-1)x^{p-2}y & x^{p-1} \end{bmatrix}$$

$$\det(\mathbf{J}_{x,y}) = (xy)^{p-1} - (p^2 - 2p + 1)(xy)^{p-1} = 0 \text{ over } \mathbb{F}_p.$$

Characteristic Zero: **J** has full rank $\Leftarrow$ **J** has an inverse

Finite Characteristic: Entries in "inverse" have denominators that are partial derivatives of some annihilators - Can become zero.

Looking Further in the Taylor Expansion

For any $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ and $\mathbf{z} \in \mathbb{F}^n$,

$$f(\mathbf{x}+\mathbf{z}) - f(\mathbf{z}) = \underbrace{x_1 \cdot \partial_{x_1} f + \cdots + x_n \cdot \partial_{x_n} f}_{\text{Jacobian}} + \text{higher order terms}$$

Looking Further in the Taylor Expansion

For any $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ and $\mathbf{z} \in \mathbb{F}^n$,

$$f(\mathbf{x}+\mathbf{z}) - f(\mathbf{z}) = \underbrace{x_1 \cdot \partial_{x_1} f + \cdots + x_n \cdot \partial_{x_n} f}_{\text{Jacobian}} + \text{higher order terms}$$

[PSS'16]: Look at Taylor expansions up to the "inseparable degree".

Looking Further in the Taylor Expansion

For any $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ and $\mathbf{z} \in \mathbb{F}^n$,

$$f(\mathbf{x}+\mathbf{z}) - f(\mathbf{z}) = \underbrace{x_1 \cdot \partial_{x_1} f + \cdots + x_n \cdot \partial_{x_n} f}_{\text{Jacobian}} + \text{higher order terms}$$

[PSS'16]: Look at Taylor expansions up to the "inseparable degree".

A New Operator

For any $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$,

$$\mathcal{H}_t(f) = \deg^{\leq t}\left(f(\mathbf{x}+\mathbf{z}) - f(\mathbf{z})\right)$$

Looking Further in the Taylor Expansion

For any $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ and $\mathbf{z} \in \mathbb{F}^n$,

$$f(\mathbf{x}+\mathbf{z}) - f(\mathbf{z}) = \underbrace{x_1 \cdot \partial_{x_1} f + \cdots + x_n \cdot \partial_{x_n} f}_{\text{Jacobian}} + \text{higher order terms}$$

[PSS'16]: Look at Taylor expansions up to the "inseparable degree".

A New Operator

For any $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$,

$$\mathcal{H}_t(f) = \deg^{\leq t}\left(f(\mathbf{x}+\mathbf{z}) - f(\mathbf{z})\right)$$

$$\hat{\mathcal{H}}(\mathbf{f}) = \begin{bmatrix} \ldots & \mathcal{H}_t(f_1) & \ldots \\ \ldots & \mathcal{H}_t(f_2) & \ldots \\ & \vdots & \\ \ldots & \mathcal{H}_t(f_k) & \ldots \end{bmatrix}.$$

The PSS Criterion

A given set of polynomials $\{f_1, f_2, \ldots, f_k\} \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ is algebraically independent if and only if for a random $\mathbf{z} \in \mathbb{F}^n$, $\{\mathcal{H}_t(f_1), \mathcal{H}_t(f_2), \ldots, \mathcal{H}_t(f_k)\}$ are linearly independent in

$$\frac{\mathbb{F}(\mathbf{z})[x_1, x_2, \ldots, x_n]}{\mathcal{I}_t}$$

where t is the inseparable degree of $\{f_1, f_2, \ldots, f_k\}$ and

$$\mathcal{I}_t = \langle \mathcal{H}_t(f_1), \mathcal{H}_t(f_2), \ldots, \mathcal{H}_t(f_k) \rangle_{\mathbb{F}(\mathbf{z})}^{\geq 2} \bmod \langle \mathbf{x} \rangle^{t+1} \subseteq \mathbb{F}(\mathbf{z})[\mathbf{x}].$$

Alternate Statement for the PSS Criterion

$\{f_1, f_2, \ldots, f_k\}$ is algebraically independent if and only if for every $(v_1, v_2, \ldots, v_k)$ with v_is in $\mathcal{I}_t$,

$$\mathcal{H}(\mathbf{f}, \mathbf{v}) = \begin{bmatrix} \ldots & \mathcal{H}_t(f_1) + v_1 & \ldots \\ \ldots & \mathcal{H}_t(f_2) + v_2 & \ldots \\ & \vdots & \\ \ldots & \mathcal{H}_t(f_k) + v_k & \ldots \end{bmatrix}$$ has full rank over $\mathbb{F}(\mathbf{z})$.

The Goal

Define: $\mathcal{F} = \{\varphi : \{x_1, \ldots, x_n\} \to \mathbb{F}[y_1, \ldots y_k]\}$ with $|\mathcal{F}| \approx \text{poly}(n)$.

Required: $\mathcal{C} = \mathcal{C}'(f_1, \ldots, f_m) \neq 0$, $\text{algrank}(f_1, \ldots, f_m) \leq k$

$\implies$ for some $\varphi \in \mathcal{F}$, $\mathcal{C}_0 = \mathcal{C}'(f_1 \circ \varphi, \ldots, f_m \circ \varphi) \neq 0$.

The Goal

Define: $\mathcal{F} = \{\varphi : \{x_1, \ldots, x_n\} \to \mathbb{F}[y_1, \ldots y_k]\}$ with $|\mathcal{F}| \approx \text{poly}(n)$.

Required: $\mathcal{C} = \mathcal{C}'(f_1, \ldots, f_m) \neq 0$, $\text{algrank}(f_1, \ldots, f_m) \leq k$
$\implies$ for some $\varphi \in \mathcal{F}$, $\mathcal{C}_0 = \mathcal{C}'(f_1 \circ \varphi, \ldots, f_m \circ \varphi) \neq 0$.

Sufficient: Let $g_i = f_i \circ \varphi$ and $\mathcal{H}_t(g) = \deg^{\leq t}(g(\mathbf{y} + \mathbf{v}) - g(\mathbf{v}))$.
Then,

$$\mathcal{H}(\mathbf{f} \circ \varphi, \mathbf{u}) = \begin{bmatrix} \ldots & \mathcal{H}_t(f_1 \circ \varphi) + u_1 & \ldots \\ \ldots & \mathcal{H}_t(f_2 \circ \varphi) + u_2 & \ldots \\ & \vdots & \\ \ldots & \mathcal{H}_t(f_m \circ \varphi) + u_m & \ldots \end{bmatrix}$$

has full rank for every $u_1, u_2, \ldots, u_m \in \mathcal{I}_t(\varphi)$ where

$$\mathcal{I}_t(\varphi) = \langle \mathcal{H}_t(g_1), \ldots, \mathcal{H}_t(g_m) \rangle^{\geq 2}_{\mathbb{F}(\mathbf{g}(\mathbf{v}))} \bmod \langle \mathbf{y} \rangle^{t+1} \subseteq \mathbb{F}(\mathbf{v})[\mathbf{y}].$$

Constructing Faithful Homomorphisms over Arbitrary Fields

What to ask for from the map

$$\varphi : x_i \to \sum_{j=1}^{k} a_{ij} y_j + b_i y_0 \qquad \text{and} \qquad \varphi_z : z_i \to \sum_{j=1}^{k} a_{ij} w_j + b_i w_0$$

What to ask for from the map

$$\varphi : x_i \to \sum_{j=1}^{k} a_{ij} y_j + b_i y_0 \qquad \text{and} \qquad \varphi_z : z_i \to \sum_{j=1}^{k} a_{ij} w_j + b_i w_0$$

Sufficient Properties

1. For every $\mathbf{u} \in \mathcal{I}_t(\varphi)$, there is a $\mathbf{v} \in \mathcal{I}_t$ for which $\mathbf{u} = \varphi_z(\mathbf{v} \circ \varphi)$

What to ask for from the map

$$\varphi : x_i \to \sum_{j=1}^{k} a_{ij} y_j + b_i y_0 \qquad \text{and} \qquad \varphi_z : z_i \to \sum_{j=1}^{k} a_{ij} w_j + b_i w_0$$

Sufficient Properties

1. For every $\mathbf{u} \in \mathcal{I}_t(\varphi)$, there is a $\mathbf{v} \in \mathcal{I}_t$ for which $\mathbf{u} = \varphi_z(\mathbf{v} \circ \varphi)$
2. $\mathcal{H}(\mathbf{f} \circ \varphi, \mathbf{u}) = \varphi_z(\mathcal{H}(\mathbf{f}, \mathbf{v})) \times M_\varphi$: Chain Rule

What to ask for from the map

$$\varphi : x_i \to \sum_{j=1}^{k} a_{ij} y_j + b_i y_0 \qquad \text{and} \qquad \varphi_z : z_i \to \sum_{j=1}^{k} a_{ij} w_j + b_i w_0$$

Sufficient Properties

1. For every $\mathbf{u} \in \mathcal{I}_t(\varphi)$, there is a $\mathbf{v} \in \mathcal{I}_t$ for which $\mathbf{u} = \varphi_z(\mathbf{v} \circ \varphi)$
2. $\mathcal{H}(\mathbf{f} \circ \varphi, \mathbf{u}) = \varphi_z(\mathcal{H}(\mathbf{f}, \mathbf{v})) \times M_\varphi$: Chain Rule
3. $\text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})) = \text{rank}(\varphi_z(\mathcal{H}(\mathbf{f}, \mathbf{v})))$: b_is are responsible for this

What to ask for from the map

$$\varphi : x_i \to \sum_{j=1}^{k} a_{ij} y_j + b_i y_0 \qquad \text{and} \qquad \varphi_z : z_i \to \sum_{j=1}^{k} a_{ij} w_j + b_i w_0$$

Sufficient Properties

1. For every $\mathbf{u} \in \mathcal{I}_t(\varphi)$, there is a $\mathbf{v} \in \mathcal{I}_t$ for which $\mathbf{u} = \varphi_z(\mathbf{v} \circ \varphi)$
2. $\mathcal{H}(\mathbf{f} \circ \varphi, \mathbf{u}) = \varphi_z(\mathcal{H}(\mathbf{f}, \mathbf{v})) \times M_\varphi$: Chain Rule
3. $\text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})) = \text{rank}(\varphi_z(\mathcal{H}(\mathbf{f}, \mathbf{v})))$: b_is are responsible for this
4. M_φ preserves rank

The Matrix Decomposition

$$\left[\quad \mathcal{H}(\mathbf{f}\circ\varphi,\mathbf{u}) \quad\right] = \overbrace{\left[\quad \varphi_z(\mathcal{H}(\mathbf{f},\mathbf{v})) \quad\right]}^{\text{labelled by } \mathbf{x^e}} \times \underbrace{\left[\quad M_\varphi \quad\right]}_{\text{labelled by } \mathbf{y^d}}$$

The Matrix Decomposition

$$\left[\quad \mathcal{H}(\mathbf{f}\circ\varphi,\mathbf{u}) \quad\right] = \overbrace{\left[\quad \varphi_Z(\mathcal{H}(\mathbf{f},\mathbf{v})) \quad\right]}^{\text{labelled by } \mathbf{x^e}} \times \underbrace{\left[\quad M_\varphi \quad\right]}_{\text{labelled by } \mathbf{y^d}}$$

where

$$M_\varphi(\mathbf{x^e},\mathbf{y^d}) = \begin{cases} \text{coeff}_{\mathbf{y^d}}(\varphi(\mathbf{x^e})) & \text{if } \sum e_i = \sum d_i \\ 0 & \text{otherwise} \end{cases}$$

What makes Vandermonde type matrices work?

$$\begin{bmatrix} & A & \end{bmatrix} \times \begin{bmatrix} & M & \end{bmatrix} = \begin{bmatrix} & AM & \end{bmatrix}$$

What makes Vandermonde type matrices work?

$$\begin{bmatrix} & A & \end{bmatrix} \times \begin{bmatrix} & M & \end{bmatrix} = \begin{bmatrix} & AM & \end{bmatrix}$$

Cauchy-Binet: $\det(AM) = \sum_{B \subseteq \{x_i\},\, |B|=k} \det(A_B) \det(M_B)$.

What makes Vandermonde type matrices work?

Cauchy-Binet: $\det(AM) = \sum_{B \subseteq \{x_i\},\, |B|=k} \det(A_B) \det(M_B)$.

$$\begin{bmatrix} s & s^2 & \dots & s^k \\ s^2 & s^4 & \dots & s^{2k} \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & & \vdots \\ s^n & s^{2n} & \dots & s^{kn} \end{bmatrix}$$

What makes Vandermonde type matrices work?

Cauchy-Binet: $\det(AM) = \sum_{B \subseteq \{x_i\},\, |B|=k} \det(A_B) \det(M_B)$.

$$\begin{bmatrix} s & \dots & s^k \\ (s^2)^1 & \dots & (s^2)^k \\ \vdots & & \vdots \\ \vdots & \ddots & \vdots \\ \vdots & \ddots & \vdots \\ \vdots & & \vdots \\ (s^n)^1 & \dots & (s^n)^k \end{bmatrix}$$

What makes Vandermonde type matrices work?

Cauchy-Binet: $\det(AM) = \sum_{B \subseteq \{x_i\},\, |B|=k} \det(A_B) \det(M_B)$.

$$
\begin{array}{c}
x_1 \\ x_2 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ x_n
\end{array}
\begin{bmatrix}
\left(s^{\mathrm{wt}(x_1)}\right)^1 & \cdots & \left(s^{\mathrm{wt}(x_1)}\right)^k \\
\left(s^{\mathrm{wt}(x_2)}\right)^1 & \cdots & \left(s^{\mathrm{wt}(x_2)}\right)^k \\
\vdots & & \vdots \\
\vdots & \ddots & \vdots \\
\vdots & \ddots & \vdots \\
\vdots & & \vdots \\
\left(s^{\mathrm{wt}(x_n)}\right)^1 & \cdots & \left(s^{\mathrm{wt}(x_n)}\right)^k
\end{bmatrix}
\qquad \mathrm{wt}(x_i) = i
$$

What makes Vandermonde type matrices work?

Cauchy-Binet: $\det(AM) = \sum_{B \subseteq \{x_i\},\, |B|=k} \det(A_B)\det(M_B)$.

$$\begin{array}{c} \\ x_1 \\ x_2 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ x_n \end{array} \begin{bmatrix} \left(s^{\mathrm{wt}(x_1)}\right)^1 & \cdots & \left(s^{\mathrm{wt}(x_1)}\right)^k \\ \left(s^{\mathrm{wt}(x_2)}\right)^1 & \cdots & \left(s^{\mathrm{wt}(x_2)}\right)^k \\ \vdots & & \vdots \\ \vdots & \ddots & \vdots \\ \vdots & \ddots & \vdots \\ \vdots & & \vdots \\ \left(s^{\mathrm{wt}(x_n)}\right)^1 & \cdots & \left(s^{\mathrm{wt}(x_n)}\right)^k \end{bmatrix} \qquad \mathrm{wt}(x_i) = i$$

- If $B = \left(x_{i_1}, x_{i_2}, \ldots, x_{i_k}\right)$, then $\mathrm{wt}(B) = \sum_{j=1}^{k} j\,\mathrm{wt}(x_{i_j})$

What makes Vandermonde type matrices work?

Cauchy-Binet: $\det(AM) = \sum_{B \subseteq \{x_i\},\, |B|=k} \det(A_B)\det(M_B)$.

$$\begin{array}{c} \\ x_1 \\ x_2 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ x_n \end{array} \begin{bmatrix} \left(s^{\mathrm{wt}(x_1)}\right)^1 & \cdots & \left(s^{\mathrm{wt}(x_1)}\right)^k \\ \left(s^{\mathrm{wt}(x_2)}\right)^1 & \cdots & \left(s^{\mathrm{wt}(x_2)}\right)^k \\ \vdots & & \vdots \\ \vdots & \ddots & \vdots \\ \vdots & \ddots & \vdots \\ \vdots & & \vdots \\ \left(s^{\mathrm{wt}(x_n)}\right)^1 & \cdots & \left(s^{\mathrm{wt}(x_n)}\right)^k \end{bmatrix} \qquad \mathrm{wt}(x_i) = i$$

- If $B = \left(x_{i_1}, x_{i_2}, \ldots, x_{i_k}\right)$, then $\mathrm{wt}(B) = \sum_{j=1}^{k} j\,\mathrm{wt}(x_{i_j})$
- $\deg_s(\det(M_B)) = \mathrm{wt}(B)$

What makes Vandermonde type matrices work?

Cauchy-Binet: $\det(AM) = \sum_{B \subseteq \{x_i\},\, |B|=k} \det(A_B)\det(M_B)$.

$$\begin{array}{c} \\ x_1 \\ x_2 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ x_n \end{array} \begin{bmatrix} \left(s^{\mathrm{wt}(x_1)}\right)^1 & \dots & \left(s^{\mathrm{wt}(x_1)}\right)^k \\ \left(s^{\mathrm{wt}(x_2)}\right)^1 & \dots & \left(s^{\mathrm{wt}(x_2)}\right)^k \\ \vdots & & \vdots \\ \vdots & \ddots & \vdots \\ \vdots & \ddots & \vdots \\ \vdots & & \vdots \\ \left(s^{\mathrm{wt}(x_n)}\right)^1 & \dots & \left(s^{\mathrm{wt}(x_n)}\right)^k \end{bmatrix} \qquad \mathrm{wt}(x_i) = i$$

- If $B = \left(x_{i_1}, x_{i_2}, \dots, x_{i_k}\right)$, then $\mathrm{wt}(B) = \sum_{j=1}^{k} j\,\mathrm{wt}(x_{i_j})$
- $\deg_s(\det(M_B)) = \mathrm{wt}(B)$
- Isolate a unique non-zero minor of A with maximum weight

What makes Vandermonde type matrices work?

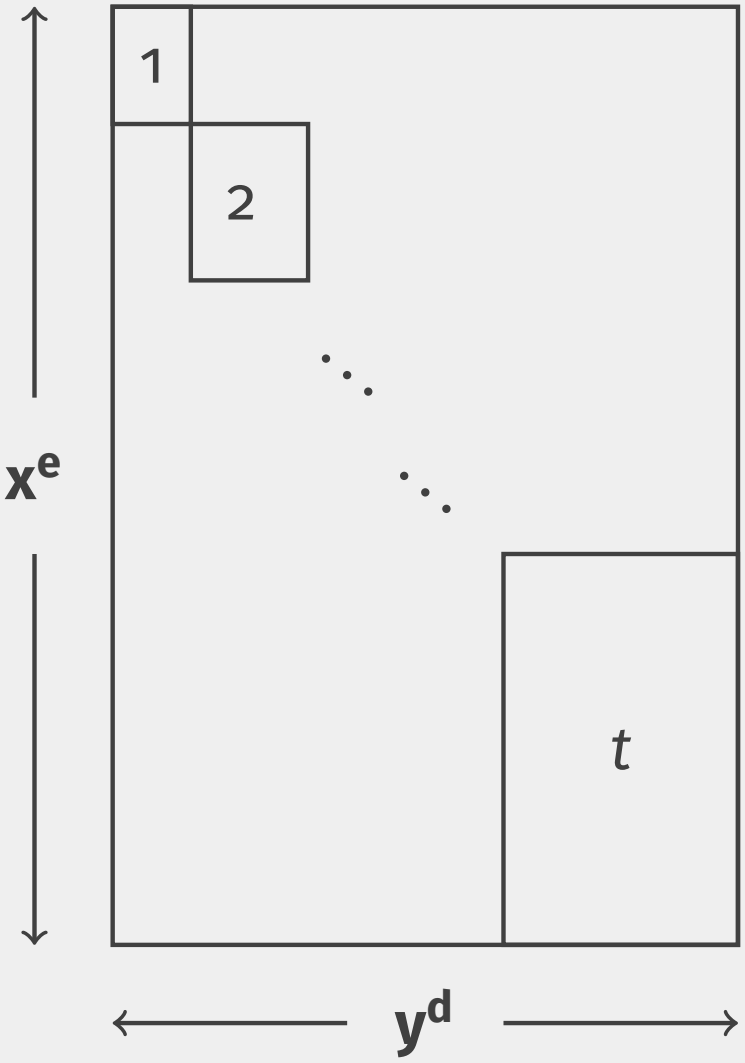
Cauchy-Binet: $\det(AM) = \sum_{B \subseteq \{x_i\},\, |B|=k} \det(A_B)\det(M_B)$.

$$
\begin{array}{c}
x_1 \\ x_2 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ x_n
\end{array}
\begin{bmatrix}
\left(s^{\mathrm{wt}(x_1)}\right)^1 & \dots & \left(s^{\mathrm{wt}(x_1)}\right)^k \\
\left(s^{\mathrm{wt}(x_2)}\right)^1 & \dots & \left(s^{\mathrm{wt}(x_2)}\right)^k \\
\vdots & & \vdots \\
\vdots & \ddots & \vdots \\
\vdots & \ddots & \vdots \\
\vdots & & \vdots \\
\left(s^{\mathrm{wt}(x_n)}\right)^1 & \dots & \left(s^{\mathrm{wt}(x_n)}\right)^k
\end{bmatrix}
$$

$\mathrm{wt}(x_i)$ is distinct for each i

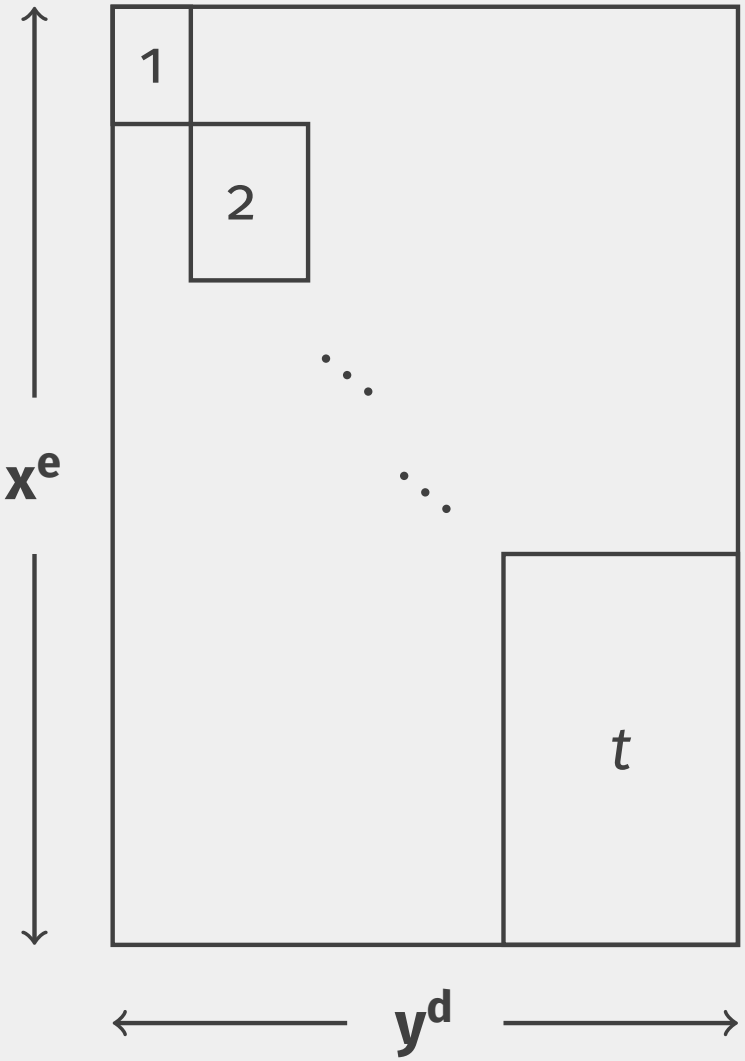
- If $B = \left(x_{i_1}, x_{i_2}, \dots, x_{i_k}\right)$, then $\mathrm{wt}(B) = \sum_{j=1}^{k} j\,\mathrm{wt}(x_{i_j})$
- $\deg_s(\det(M_B)) = \mathrm{wt}(B)$
- Isolate a unique non-zero minor of A with maximum weight

The Current Matrix



$$M_\varphi(\mathbf{x^e}, \mathbf{y^d}) = \mathrm{coeff}_{\mathbf{y^d}}(\varphi(\mathbf{x^e}))$$

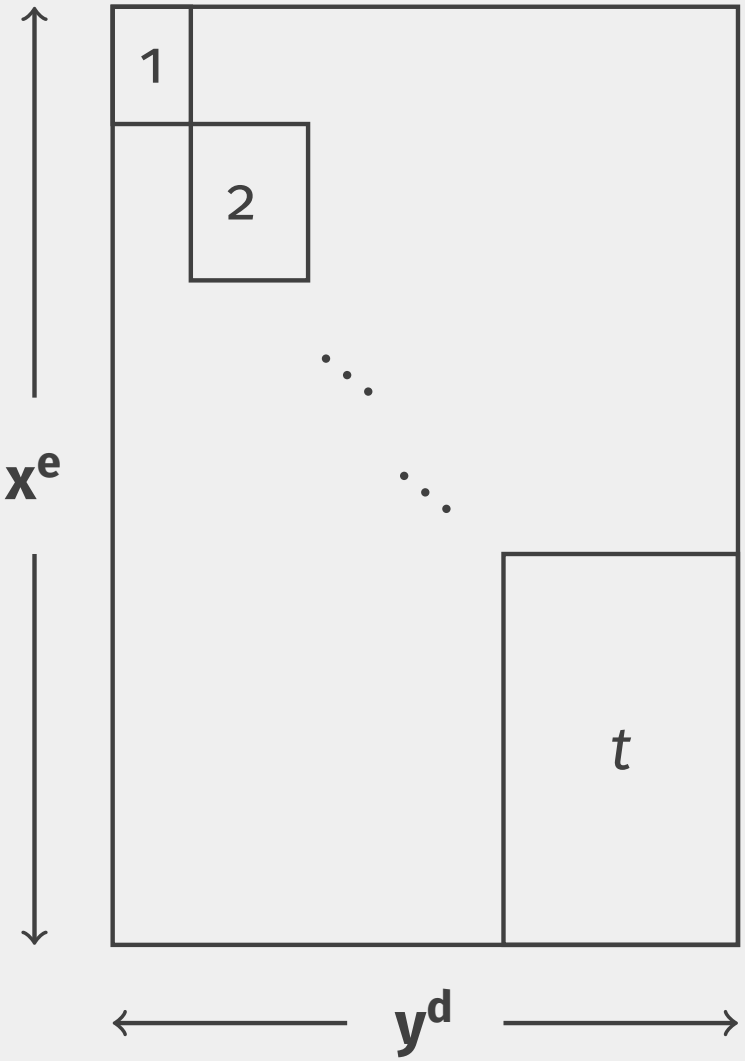
The Current Matrix



$$M_\varphi(\mathbf{x^e}, \mathbf{y^d}) = \text{coeff}_{\mathbf{y^d}}(\varphi(\mathbf{x^e}))$$

Taking inspiration from the prev. case: $M_\varphi(x_i, y_j) = s^{\text{wt}(i)j}$

The Current Matrix

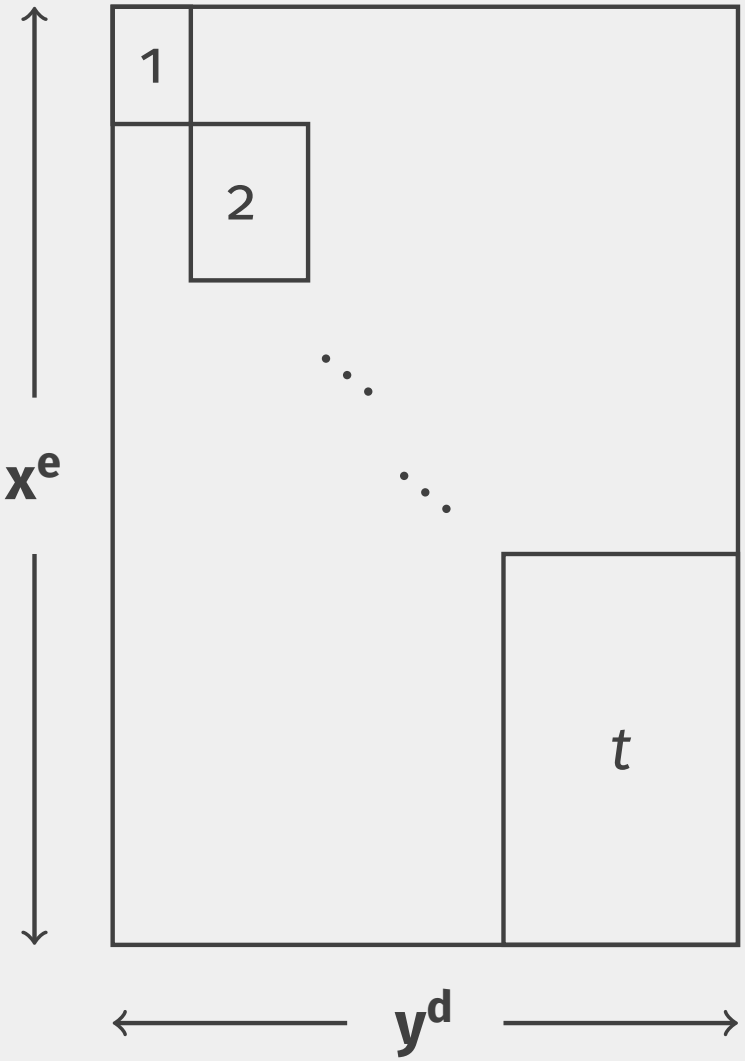


$$M_\varphi(\mathbf{x^e}, \mathbf{y^d}) = \operatorname{coeff}_{\mathbf{y^d}}(\varphi(\mathbf{x^e}))$$

Taking inspiration from the prev. case: $M_\varphi(x_i, y_j) = s^{\operatorname{wt}(i)j}$

$$\operatorname{wt}(\mathbf{x^e}) = \textstyle\sum_{i\in[n]} e_i \operatorname{wt}(i)$$

The Current Matrix



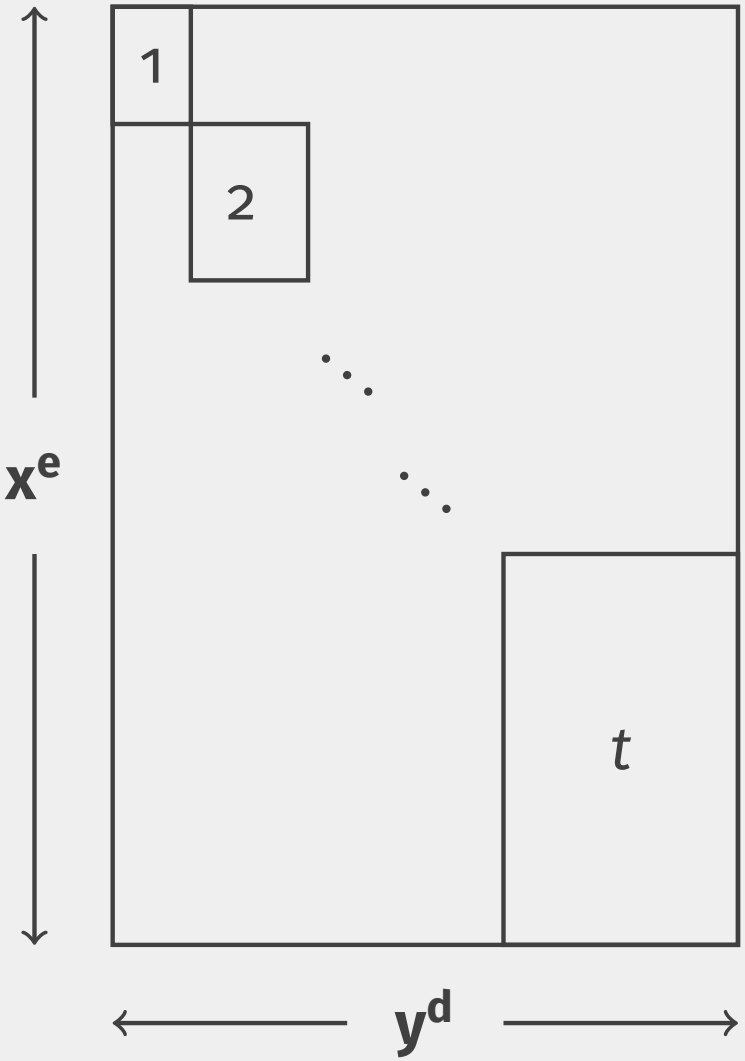
$$M_\varphi(\mathbf{x^e}, \mathbf{y^d}) = \mathrm{coeff}_{\mathbf{y^d}}(\varphi(\mathbf{x^e}))$$

Taking inspiration from the prev. case: $M_\varphi(x_i, y_j) = s^{\mathrm{wt}(i)j}$

$$\mathrm{wt}(\mathbf{x^e}) = \textstyle\sum_{i\in[n]} e_i \,\mathrm{wt}(i)$$

$$M_\varphi(\mathbf{x^e}, y_j^d) = s^{\mathrm{wt}(\mathbf{x^e})j}$$

The Current Matrix



$$M_\varphi(\mathbf{x^e}, \mathbf{y^d}) = \text{coeff}_{\mathbf{y^d}}(\varphi(\mathbf{x^e}))$$

Taking inspiration from the prev. case: $M_\varphi(x_i, y_j) = s^{\text{wt}(i)j}$

$$\text{wt}(\mathbf{x^e}) = \sum_{i\in[n]} e_i \,\text{wt}(i)$$

$$M_\varphi(\mathbf{x^e}, y_j^d) = s^{\text{wt}(\mathbf{x^e})j}$$

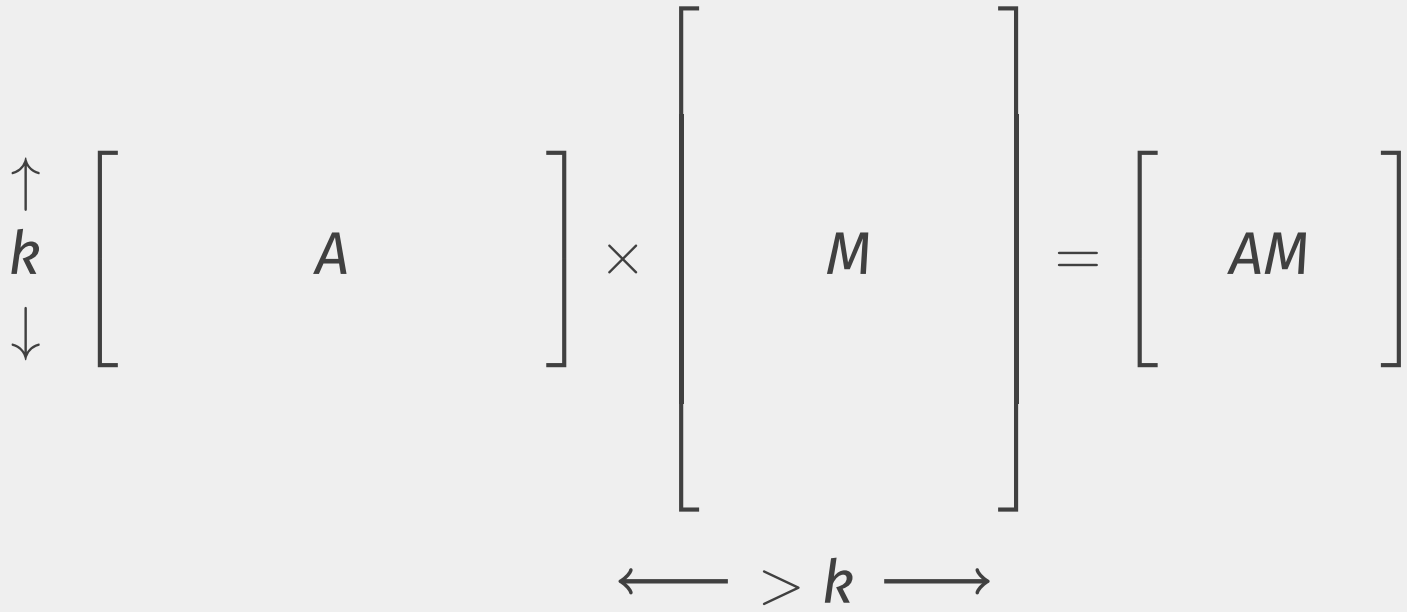
$$\text{If } B = (\mathbf{x}^{\mathbf{e}_1}, \mathbf{x}^{\mathbf{e}_2}, \ldots, \mathbf{x}^{\mathbf{e}_k}),$$

$$\text{then } \text{wt}(B) = \sum_{j\in[k]} j \,\text{wt}(\mathbf{x}^{\mathbf{e}_j})$$

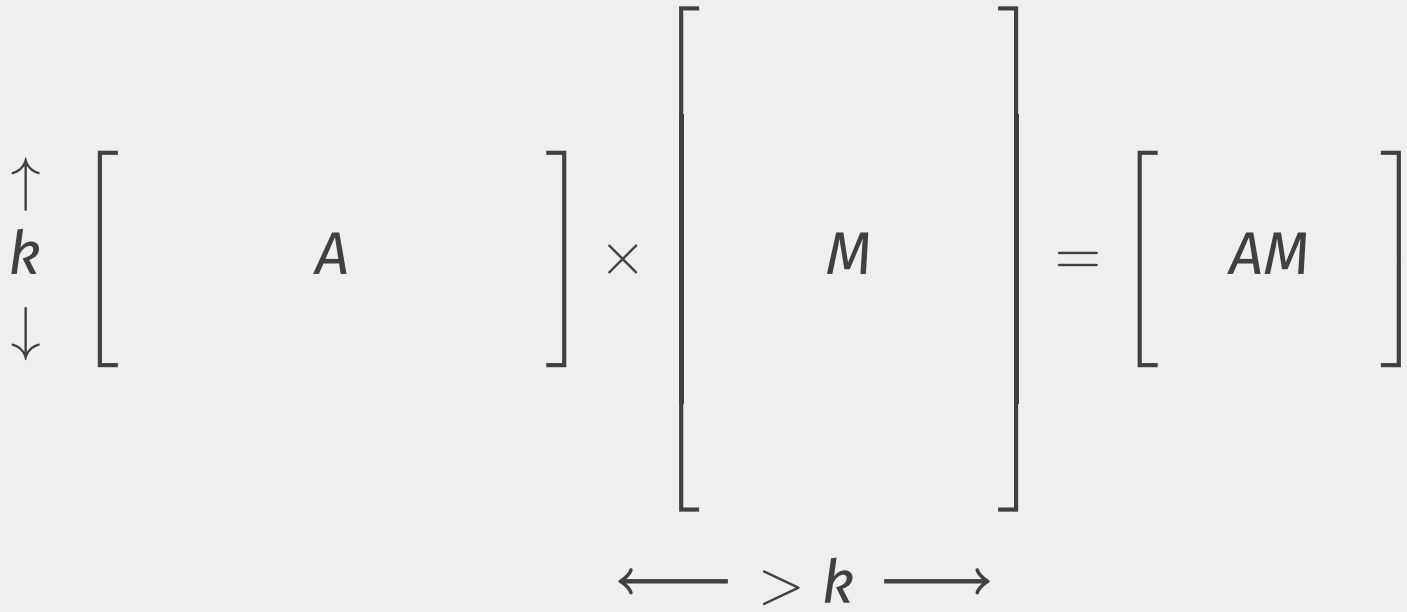
A Rank Preserving Matrix

$$\begin{bmatrix} \\ A \\ \\ \end{bmatrix} \times \begin{bmatrix} \\ \\ M \\ \\ \\ \end{bmatrix} = \begin{bmatrix} \\ AM \\ \\ \end{bmatrix}$$

A Rank Preserving Matrix

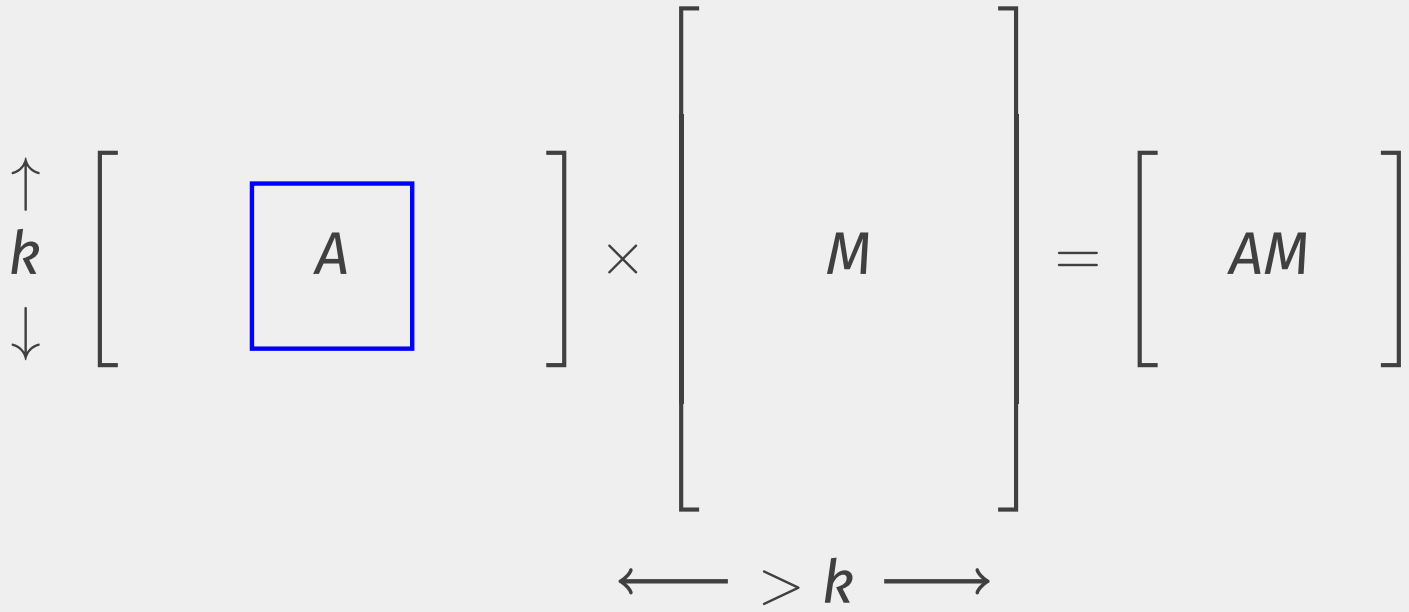


A Rank Preserving Matrix



What we want: k columns of AM that are linearly independent.

A Rank Preserving Matrix

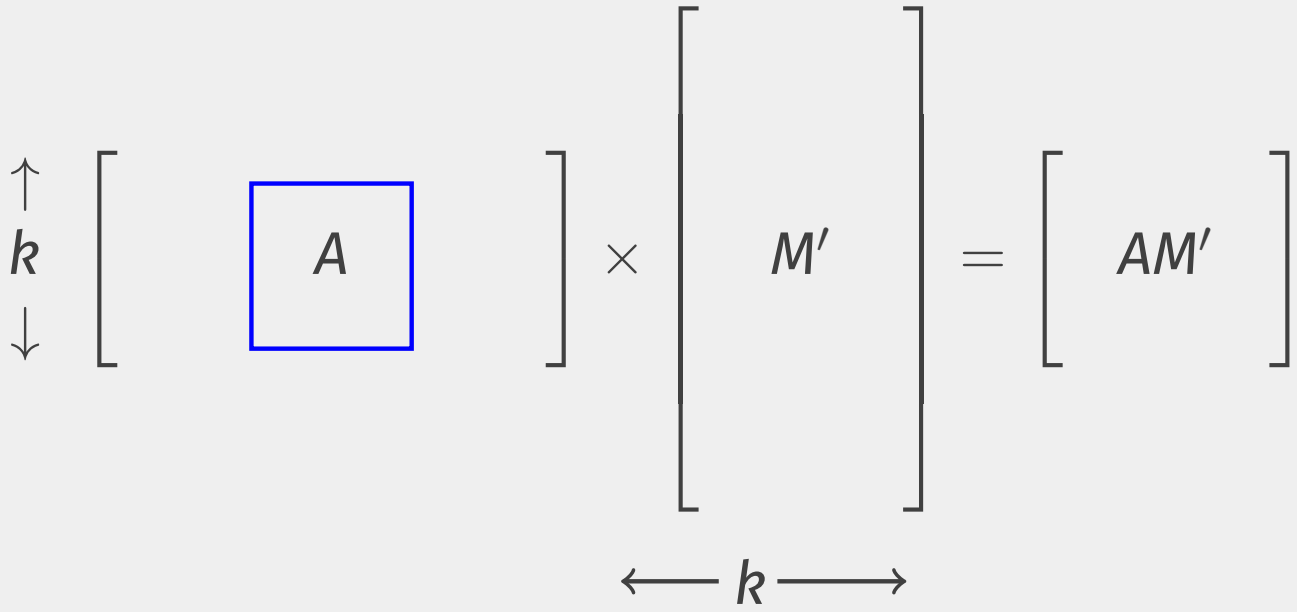


What we want: k columns of AM that are linearly independent.

Proof Strategy:

- Isolate a unique non-zero minor A_{B_0} with maximum weight

A Rank Preserving Matrix



What we want: k columns of AM that are linearly independent.

Proof Strategy:

- Isolate a unique non-zero minor A_{B_0} with maximum weight
- $M' \equiv k$ columns of M such that $\deg_s(\det(M'_{B_0})) = \mathrm{wt}(B_0)$

A few details

About $\deg_s(\det(M'_{B_0}))$ **for** $B \neq B_0$:

- $\deg_s(\det(M'_B)) \leq \mathrm{wt}(B)$ for $B \neq B_0$

A few details

About $\deg_s(\det(M'_{B_0}))$ **for** $B \neq B_0$:

- $\deg_s(\det(M'_B)) \leq \mathrm{wt}(B)$ for $B \neq B_0$

About wt:

- wt "hashes" the monomials in question
  $\Rightarrow$ there is a unique B of maximum weight.

A few details

About $\deg_s(\det(M'_{B_0}))$ **for** $B \neq B_0$:

- $\deg_s(\det(M'_B)) \leq \mathrm{wt}(B)$ for $B \neq B_0$

About wt:

- wt "hashes" the monomials in question
  $\Rightarrow$ there is a unique B of maximum weight.

About M'

- M' can always be chosen such that its columns are indexed by "pure" monomials.

A Faithful Map over Arbitrary Fields

$$\varphi : x_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} y_j + a_i y_0 \quad \text{and} \quad \varphi_z : z_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} w_j + a_i y_0$$

where t is the inseparable degree and $\mathrm{wt}(i) = (t+1)^i \bmod p$.

A Faithful Map over Arbitrary Fields

$$\varphi : x_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} y_j + a_i y_0 \quad \text{and} \quad \varphi_z : z_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} w_j + a_i y_0$$

where t is the inseparable degree and $\mathrm{wt}(i) = (t+1)^i \bmod p$.

Properties

1. For every $\mathbf{u} \in \mathcal{I}_t(\varphi)$, there is a $\mathbf{v} \in \mathcal{I}_t$ for which $\mathbf{u} = \varphi_z(\mathbf{v} \circ \varphi)$

A Faithful Map over Arbitrary Fields

$$\varphi : x_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} y_j + a_i y_0 \quad \text{and} \quad \varphi_z : z_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} w_j + a_i y_0$$

where t is the inseparable degree and $\mathrm{wt}(i) = (t+1)^i \bmod p$.

Properties

1. For every $\mathbf{u} \in \mathcal{I}_t(\varphi)$, there is a $\mathbf{v} \in \mathcal{I}_t$ for which $\mathbf{u} = \varphi_z(\mathbf{v} \circ \varphi)$
2. $\varphi_z(\mathcal{H}(\mathbf{f}, \mathbf{v})) \times M_\varphi$ is a sub-matrix of $\mathcal{H}(\mathbf{f} \circ \varphi, \mathbf{u})$

A Faithful Map over Arbitrary Fields

$$\varphi : x_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} y_j + a_i y_0 \quad \text{and} \quad \varphi_z : z_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} w_j + a_i y_0$$

where t is the inseparable degree and $\mathrm{wt}(i) = (t+1)^i \bmod p$.

Properties

1. For every $\mathbf{u} \in \mathcal{I}_t(\varphi)$, there is a $\mathbf{v} \in \mathcal{I}_t$ for which $\mathbf{u} = \varphi_z(\mathbf{v} \circ \varphi)$
2. $\varphi_z(\mathcal{H}(\mathbf{f}, \mathbf{v})) \times M_\varphi$ is a sub-matrix of $\mathcal{H}(\mathbf{f} \circ \varphi, \mathbf{u})$
3. $\mathrm{rank}(\varphi_z(\mathcal{H}(\mathbf{f}, \mathbf{v}))) = \mathrm{rank}(\varphi_z(\mathcal{H}(\mathbf{f}, \mathbf{v})) \times M_\varphi)$

A Faithful Map over Arbitrary Fields

$$\varphi : x_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} y_j + a_i y_0 \quad \text{and} \quad \varphi_z : z_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} w_j + a_i y_0$$

where t is the inseparable degree and $\mathrm{wt}(i) = (t+1)^i \bmod p$.

Properties

1. For every $\mathbf{u} \in \mathcal{I}_t(\varphi)$, there is a $\mathbf{v} \in \mathcal{I}_t$ for which $\mathbf{u} = \varphi_z(\mathbf{v} \circ \varphi)$
2. $\varphi_z(\mathcal{H}(\mathbf{f}, \mathbf{v})) \times M_\varphi$ is a sub-matrix of $\mathcal{H}(\mathbf{f} \circ \varphi, \mathbf{u})$
3. $\mathrm{rank}(\varphi_z(\mathcal{H}(\mathbf{f}, \mathbf{v}))) = \mathrm{rank}(\varphi_z(\mathcal{H}(\mathbf{f}, \mathbf{v})) \times M_\varphi)$
4. $\mathrm{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})) = \mathrm{rank}(\varphi_z(\mathcal{H}(\mathbf{f}, \mathbf{v})))$

Open Threads

1. Improve the dependence on "inseparable degree".

Open Threads

1. Improve the dependence on "inseparable degree".

2. [GSS'18]: Different characterisation for Algebraic dependence - not algorithmic but has no dependence on "inseparable degree"

   Can we get PIT applications out of it?

Open Threads

1. Improve the dependence on "inseparable degree".

2. [GSS'18]: Different characterisation for Algebraic dependence - not algorithmic but has no dependence on "inseparable degree"

   Can we get PIT applications out of it?

Thank you!