

# FAITHFUL HOMOMORPHISMS AND PIT – A SHORT SURVEY

PRERONA CHATTERJEE

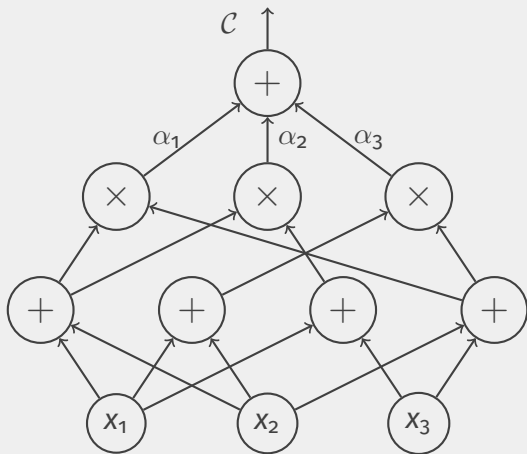
BASED ON JOINT WORK WITH *RAMPRASAD SAPTHARISHI*

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-zerosness

# 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-zerosness

**Trivial Substitution:**  $x_i \rightarrow t^{(d+1)^i}$

distinct monomials  $\rightarrow$  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-zerosness

**Trivial Substitution:**  $x_i \rightarrow t^{(d+1)^i}$

distinct monomials  $\rightarrow$  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-zerosness

**Trivial Substitution:**  $x_i \rightarrow t^{(d+1)^i}$

distinct monomials  $\rightarrow$  distinct power in  $t \implies$  **No Cancellations**

**No. of variables:** 1      **Degree:**  $(d + 1)^n$       **|Hitting Set|:**  $(d + 1)^n$

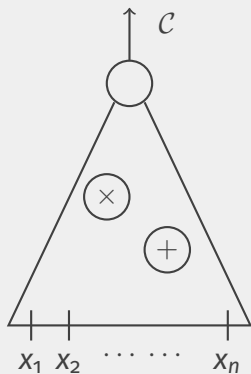
**What we need:** Reduce no. of variables (preferably constant)

Keep degree under control (poly-bounded)

Preserve non-zerosness

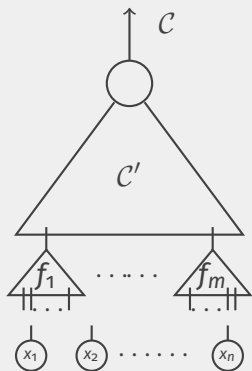


## A SPECIAL SETTING: CAN WE DO BETTER?



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

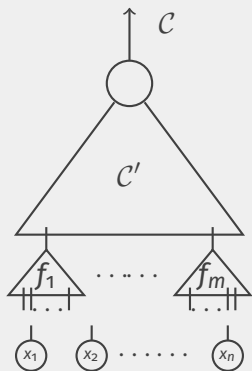
# A SPECIAL SETTING: CAN WE DO BETTER?



Check whether  $C$  computes the zero polynomial or not.

$$C = C'(f_1, f_2, \dots, f_m)$$

# A SPECIAL SETTING: CAN WE DO BETTER?



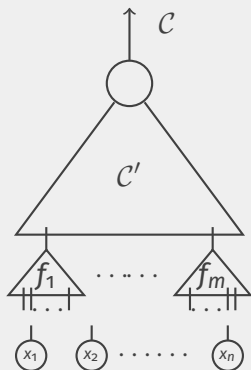
Check whether  $C$  computes the zero polynomial or not.

$$C = C'(f_1, f_2, \dots, f_m)$$

Only  $k$  of them are "relevant" where

$$k \ll n$$

# A SPECIAL SETTING: CAN WE DO BETTER?



Check whether  $C$  computes the zero polynomial or not.

$$C = C'(f_1, f_2, \dots, f_m)$$

Only  $k$  of them are "relevant" where

$$k \ll n$$

**Can we do any better than trivial?**

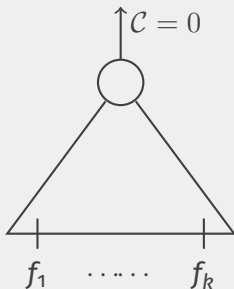
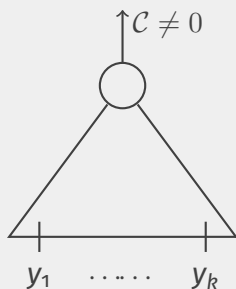
# PRELIMINARIES

# ALGEBRAIC INDEPENDENCE

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

$$A(y_1, \dots, y_k) \neq 0; \quad A(f_1, \dots, f_k) = 0.$$

Otherwise, they are said to be algebraically independent.

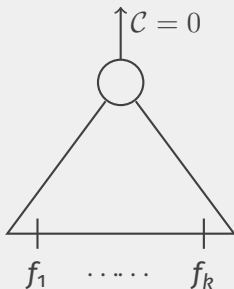
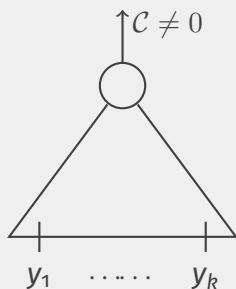


# ALGEBRAIC INDEPENDENCE

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

$$A(y_1, \dots, y_k) \neq 0; \quad A(f_1, \dots, f_k) = 0.$$

Otherwise, they are said to be algebraically independent.

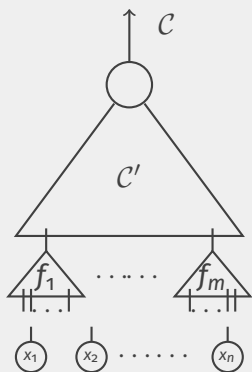


Algebraic Rank  
of  $\{f_1, \dots, f_m\}$

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

# OUR SETTING: HOW IS IT DIFFERENT?

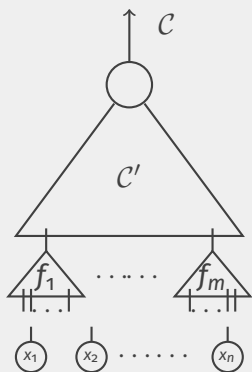
$$C = C'(f_1, \dots, f_m) : \text{algrank}(f_1, \dots, f_m) = k \ll n$$





# OUR SETTING: HOW IS IT DIFFERENT?

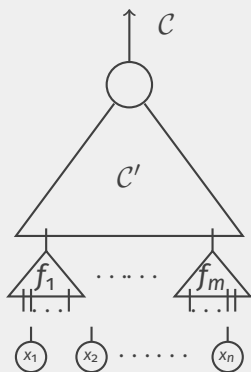
$$C = C'(f_1, \dots, f_m) : \text{algrank}(f_1, \dots, f_m) = k \ll n$$



**Easy Case:**  $k = m$   
Have access to  $C'$

# OUR SETTING: HOW IS IT DIFFERENT?

$$C = C'(f_1, \dots, f_m) : \text{algrank}(f_1, \dots, f_m) = k \ll n$$



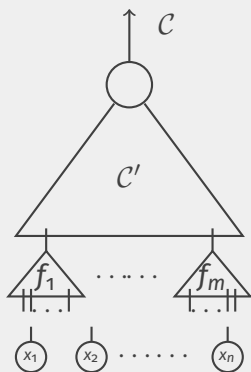
**Easy Case:**  $k = m$

Have access to  $C'$

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

# OUR SETTING: HOW IS IT DIFFERENT?

$$C = C'(f_1, \dots, f_m) : \text{algrank}(f_1, \dots, f_m) = k \ll n$$



**Easy Case:**  $k = m$

Have access to  $C'$

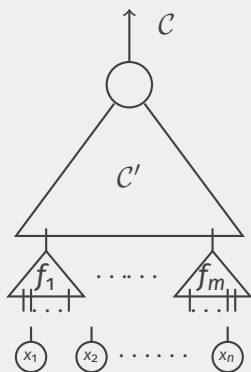
**|Hitting Set| in this case:**  $(d + 1)^k$

**General Case:**  $k \neq m$

Do not have access to  $C'$

# OUR SETTING: HOW IS IT DIFFERENT?

$$C = C'(f_1, \dots, f_m) : \text{algrank}(f_1, \dots, f_m) = k \ll n$$



**Easy Case:**  $k = m$

Have access to  $C'$

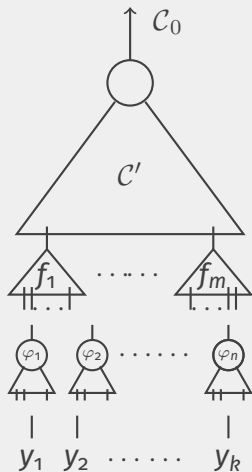
**|Hitting Set| in this case:**  $(d + 1)^k$

**General Case:**  $k \neq m$

Do not have access to  $C'$

**What is allowed:** Substitute  $x_i$ s

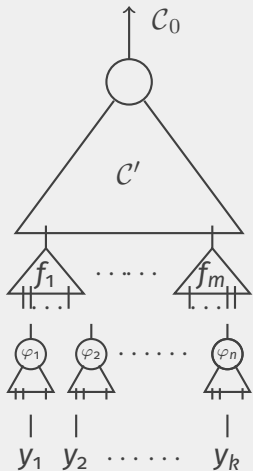
# OUR SETTING: WHAT CAN BE DONE?



$$x_i \rightarrow \varphi_i(y_1, \dots, y_k)$$

**Property required:**  $C \neq 0 \implies C_0 \neq 0$

# OUR SETTING: WHAT CAN BE DONE?



$$x_i \rightarrow \varphi_i(y_1, \dots, y_k)$$

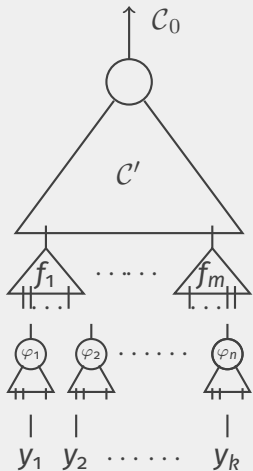
**Property required:**  $C \neq 0 \implies C_0 \neq 0$

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

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

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

# OUR SETTING: WHAT CAN BE DONE?



$$x_i \rightarrow \varphi_i(y_1, \dots, y_k)$$

**Property required:**  $C \neq 0 \implies C_0 \neq 0$

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

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

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

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

# FAITHFUL MAPS

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

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

is said to be faithful if  $\text{algrank}(g_1, \dots, g_m) = k$ .

Here  $g_i(\mathbf{y}) = f_i(\varphi(x_1), \dots, \varphi(x_n))$ .



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

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

is said to be faithful if  $\text{algrank}(g_1, \dots, g_m) = k$ .

Here  $g_i(\mathbf{y}) = f_i(\varphi(x_1), \dots, \varphi(x_n))$ .

**Why should one believe that such maps can exist?**

What we know: If  $\{f_1, \dots, f_k\}$  are algebraically independent, then

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

# FAITHFUL MAPS

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

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

is said to be faithful if  $\text{algrank}(g_1, \dots, g_m) = k$ .

Here  $g_i(\mathbf{y}) = f_i(\varphi(x_1), \dots, \varphi(x_n))$ .

**Why should one believe that such maps can exist?**

What we know: If  $\{f_1, \dots, f_k\}$  are algebraically independent, then

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

What we are asking for: A better way of seeing this isomorphism.

That is, are there  $g_1, \dots, g_k \in \mathbb{F}[y_1, \dots, y_k]$  such that

$g_i = f_i(\varphi(x_1), \dots, \varphi(x_n))$  and

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

# CONSTRUCTING FAITHFUL MAPS ARE ENOUGH

**Lemma** [BMS'11, ASSS'12]

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

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

# CONSTRUCTING FAITHFUL MAPS ARE ENOUGH

## Lemma [BMS'11, ASSS'12]

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

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

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

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

## Useful fact

$\mathbb{F}(f_1, \dots, f_m)$   
|  
 $\mathbb{F}(f_1, \dots, f_k)$  is an  
algebraic extension.  
Thus,  $R(f_1, \dots, f_m)$   
 $= \frac{R'[f_1, \dots, f_m]}{Q[f_1, \dots, f_k]}$

# LINEAR RANK EXTRACTORS [GR'05]

$$\left[ \begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{array} \right] A \times \left[ \begin{array}{ccc} s & \dots & s^k \\ (s^2)^1 & \dots & (s^2)^k \\ \vdots & & \vdots \\ \vdots & \ddots & \vdots \\ \vdots & \ddots & \vdots \\ \vdots & & \vdots \\ (s^n)^1 & \dots & (s^n)^k \end{array} \right] = \left[ \begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{array} \right] A'$$

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

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

# CAPTURING ALGEBRAIC RANK VIA LINEAR RANK

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

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

## The Jacobian Criterion

If  $\mathbb{F}$  has characteristic zero, the algebraic rank of  $\{f_1, f_2, \dots, f_m\}$  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  $\varphi$  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  $\varphi$  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:**  $\mathcal{F} = \left\{ \varphi_{\mathbf{s}, \mathbf{b}} = \sum_{j=1}^k s^{ij} y_j + b_i \right\}_{\mathbf{s} \in \{0, \dots, nk^2\}, \mathbf{b} \in \mathcal{S}}$

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

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

# SOME INSTANTIATIONS

## The PIT Algorithm

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

# SOME INSTANTIATIONS

## The PIT Algorithm

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

**Step 1:** For every  $\varphi \in \mathcal{F}$  not tried yet.

Run trivial PIT on  $\mathcal{C}_0 = \mathcal{C}'(f_1 \circ \varphi, \dots, f_m \circ \varphi)$

If  $\mathcal{C}_0 \neq 0$ , return "NOT ZERO".

**Step 2:** Return "ZERO".

# SOME INSTANTIATIONS

## The PIT Algorithm

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

**Step 1:** For every  $\varphi \in \mathcal{F}$  not tried yet.

Run trivial PIT on  $\mathcal{C}_0 = \mathcal{C}'(f_1 \circ \varphi, \dots, f_m \circ \varphi)$

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

**Step 1:** For every  $\varphi \in \mathcal{F}$  not tried yet.

Run trivial PIT on  $\mathcal{C}_0 = \mathcal{C}'(f_1 \circ \varphi, \dots, f_m \circ \varphi)$

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:**  $\mathcal{C} = \mathcal{C}'(f_1, \dots, f_m)$  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.

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

# 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:**  $\mathbf{J}$  has full rank  $\Leftrightarrow \mathbf{J}$  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:**  $\mathbf{J}$  has full rank  $\Leftrightarrow \mathbf{J}$  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  $f \in \mathbb{F}[x_1, x_2, \dots, x_n]$  and  $\mathbf{z} \in \mathbb{F}^n$ ,

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

## LOOKING FURTHER IN THE TAYLOR EXPANSION

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

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

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



# LOOKING FURTHER IN THE TAYLOR EXPANSION

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

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

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

## A New Operator

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

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

# LOOKING FURTHER IN THE TAYLOR EXPANSION

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

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

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

## A New Operator

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

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

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

# THE PSS CRITERION

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

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

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

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

# ALTERNATE STATEMENT FOR THE PSS CRITERION

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

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

# THE GOAL

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

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

# THE GOAL

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

**Required:**  $C = C'(f_1, \dots, f_m) \neq 0$ ,  $\text{algrank}(f_1, \dots, f_m) \leq k$   
 $\implies$  for some  $\varphi \in \mathcal{F}$ ,  $C_0 = C'(f_1 \circ \varphi, \dots, f_m \circ \varphi) \neq 0$ .

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

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

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

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

# **CONSTRUCTING FAITHFUL HOMOMORPHISMS OVER ARBITRARY FIELDS**

# WHAT TO ASK FOR FROM THE MAP

$$\varphi : x_i \rightarrow \sum_{j=1}^k a_{ij}y_j + b_iy_0 \quad \text{and} \quad \varphi_z : z_i \rightarrow \sum_{j=1}^k a_{ij}w_j + b_iw_0$$



# WHAT TO ASK FOR FROM THE MAP

$$\varphi : x_j \rightarrow \sum_{j=1}^k a_{ij}y_j + b_iy_0 \quad \text{and} \quad \varphi_z : z_j \rightarrow \sum_{j=1}^k a_{ij}w_j + b_iw_0$$

## 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

$$\varphi : x_j \rightarrow \sum_{j=1}^k a_{ij}y_j + b_iy_0 \quad \text{and} \quad \varphi_z : z_j \rightarrow \sum_{j=1}^k a_{ij}w_j + b_iw_0$$

## 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

$$\varphi : x_j \rightarrow \sum_{j=1}^k a_{ij}y_j + b_iy_0 \quad \text{and} \quad \varphi_z : z_i \rightarrow \sum_{j=1}^k a_{ij}w_j + b_iw_0$$

## 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.  $\text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})) = \text{rank}(\varphi_z(\mathcal{H}(\mathbf{f}, \mathbf{v})))$ :  $b_i$ s are responsible for this

# WHAT TO ASK FOR FROM THE MAP

$$\varphi : x_i \rightarrow \sum_{j=1}^k a_{ij}y_j + b_iy_0 \quad \text{and} \quad \varphi_z : z_i \rightarrow \sum_{j=1}^k a_{ij}w_j + b_iw_0$$

## 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.  $\text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})) = \text{rank}(\varphi_z(\mathcal{H}(\mathbf{f}, \mathbf{v})))$ :  $b_i$ s are responsible for this
4.  $M_\varphi$  preserves rank

# THE MATRIX DECOMPOSITION

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

# THE MATRIX DECOMPOSITION

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

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?

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

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

# WHAT MAKES VANDERMONDE TYPE MATRICES WORK?

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

$$\begin{array}{c} x_1 \\ x_2 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ x_n \end{array} \begin{bmatrix} (S^{\text{wt}(x_1)})^1 & \dots & (S^{\text{wt}(x_1)})^k \\ (S^{\text{wt}(x_2)})^1 & \dots & (S^{\text{wt}(x_2)})^k \\ \vdots & & \vdots \\ \vdots & \ddots & \vdots \\ \vdots & \ddots & \vdots \\ \vdots & & \vdots \\ (S^{\text{wt}(x_n)})^1 & \dots & (S^{\text{wt}(x_n)})^k \end{bmatrix} \quad \text{wt}(x_i) = i$$

■ If  $B = (x_{i_1}, x_{i_2}, \dots, x_{i_k})$ , then  $\text{wt}(B) = \sum_{j=1}^k j \text{wt}(x_{i_j})$

# WHAT MAKES VANDERMONDE TYPE MATRICES WORK?

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

$$\begin{array}{c} x_1 \\ x_2 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ x_n \end{array} \begin{bmatrix} (S^{\text{wt}(x_1)})^1 & \dots & (S^{\text{wt}(x_1)})^k \\ (S^{\text{wt}(x_2)})^1 & \dots & (S^{\text{wt}(x_2)})^k \\ \vdots & & \vdots \\ \vdots & \ddots & \vdots \\ \vdots & \ddots & \vdots \\ \vdots & & \vdots \\ (S^{\text{wt}(x_n)})^1 & \dots & (S^{\text{wt}(x_n)})^k \end{bmatrix} \quad \text{wt}(x_i) = i$$

- If  $B = (x_{i_1}, x_{i_2}, \dots, x_{i_k})$ , then  $\text{wt}(B) = \sum_{j=1}^k j \text{wt}(x_{i_j})$
- $\deg_S(\det(M_B)) = \text{wt}(B)$

# WHAT MAKES VANDERMONDE TYPE MATRICES WORK?

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

$$\begin{array}{l} x_1 \\ x_2 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ x_n \end{array} \begin{bmatrix} (S^{\text{wt}(x_1)})^1 & \dots & (S^{\text{wt}(x_1)})^k \\ (S^{\text{wt}(x_2)})^1 & \dots & (S^{\text{wt}(x_2)})^k \\ \vdots & & \vdots \\ \vdots & \ddots & \vdots \\ \vdots & \ddots & \vdots \\ \vdots & & \vdots \\ (S^{\text{wt}(x_n)})^1 & \dots & (S^{\text{wt}(x_n)})^k \end{bmatrix} \quad \text{wt}(x_i) = i$$

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

# WHAT MAKES VANDERMONDE TYPE MATRICES WORK?

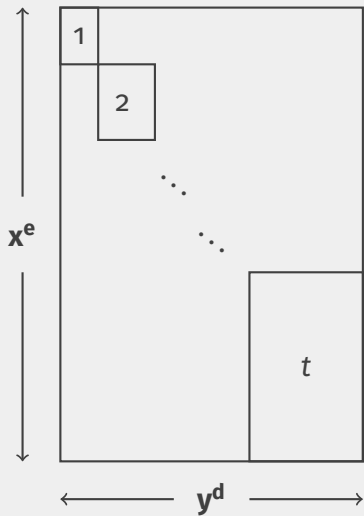
**Cauchy-Binet:**  $\det(AM) = \sum_{B \subseteq \{x_i\}, |B|=k} \det(A_B) \det(M_B)$ .

$$\begin{array}{c} x_1 \\ x_2 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ x_n \end{array} \begin{bmatrix} (S^{\text{wt}(x_1)})^1 & \dots & (S^{\text{wt}(x_1)})^k \\ (S^{\text{wt}(x_2)})^1 & \dots & (S^{\text{wt}(x_2)})^k \\ \vdots & & \vdots \\ \vdots & \ddots & \vdots \\ \vdots & \ddots & \vdots \\ \vdots & & \vdots \\ (S^{\text{wt}(x_n)})^1 & \dots & (S^{\text{wt}(x_n)})^k \end{bmatrix}$$

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

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

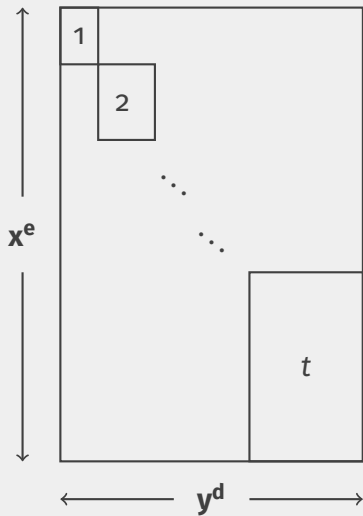
# THE CURRENT MATRIX



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



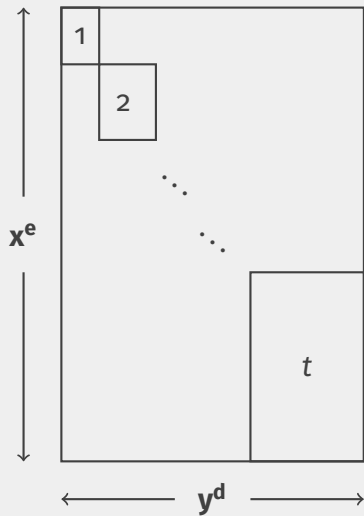
# THE CURRENT MATRIX



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

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

# THE CURRENT MATRIX

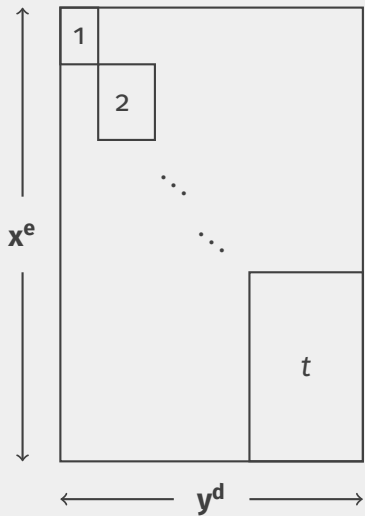


$$M_{\varphi}(\mathbf{x}^e, \mathbf{y}^d) = \text{coeff}_{\mathbf{y}^d}(\varphi(\mathbf{x}^e))$$

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

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

# THE CURRENT MATRIX



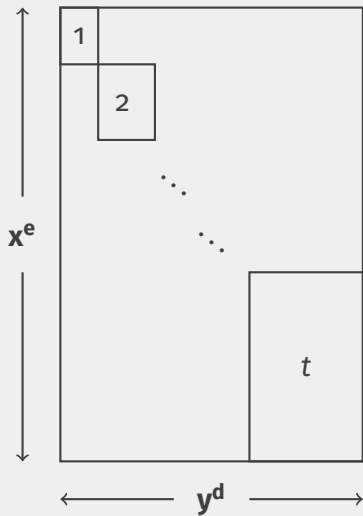
$$M_{\varphi}(\mathbf{x}^e, \mathbf{y}^d) = \text{coeff}_{\mathbf{y}^d}(\varphi(\mathbf{x}^e))$$

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

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

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

# 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:**  $M_{\varphi}(x_i, y_j) = s^{\text{wt}(i)j}$

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

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

If  $B = (\mathbf{x}^{e_1}, \mathbf{x}^{e_2}, \dots, \mathbf{x}^{e_k})$ ,

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

# A RANK PRESERVING MATRIX

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

# A RANK PRESERVING MATRIX

$$\begin{array}{c} \uparrow \\ k \\ \downarrow \end{array} \left[ \begin{array}{c} \\ \\ \\ \end{array} \right] A \left[ \begin{array}{c} \\ \\ \\ \end{array} \right] \times \left[ \begin{array}{c} \\ \\ \\ \end{array} \right] M \left[ \begin{array}{c} \\ \\ \\ \end{array} \right] = \left[ \begin{array}{c} \\ \\ \\ \end{array} \right] AM \left[ \begin{array}{c} \\ \\ \\ \end{array} \right]$$

$\longleftarrow > k \longrightarrow$

# A RANK PRESERVING MATRIX

$$\begin{array}{c} \uparrow \\ k \\ \downarrow \end{array} \left[ \begin{array}{c} \\ \\ \\ \end{array} \right] \begin{array}{c} \\ \\ \\ \end{array} \left[ \begin{array}{c} \\ \\ \\ \end{array} \right] \times \left[ \begin{array}{c} \\ \\ \\ \end{array} \right] \begin{array}{c} \\ \\ \\ \end{array} \left[ \begin{array}{c} \\ \\ \\ \end{array} \right] = \left[ \begin{array}{c} \\ \\ \\ \end{array} \right] \begin{array}{c} \\ \\ \\ \end{array} \left[ \begin{array}{c} \\ \\ \\ \end{array} \right]$$

$\longleftarrow > k \longrightarrow$

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

# A RANK PRESERVING MATRIX

$$\begin{array}{c} \uparrow \\ k \\ \downarrow \end{array} \left[ \begin{array}{c} \boxed{A} \end{array} \right] \times \left[ \begin{array}{c} M \end{array} \right] = \left[ \begin{array}{c} AM \end{array} \right]$$

$\leftarrow > k \rightarrow$

**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

$$\begin{array}{c} \uparrow \\ k \\ \downarrow \end{array} \left[ \begin{array}{|c|} \hline A \\ \hline \end{array} \right] \times \left[ \begin{array}{|c|} \hline M' \\ \hline \end{array} \right] = \left[ \begin{array}{|c|} \hline AM' \\ \hline \end{array} \right]$$

$\leftarrow k \rightarrow$

**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  $\deg_S(\det(M'_{B_0})) = \text{wt}(B_0)$

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

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

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

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

**About**  $\text{wt}$ :

- $\text{wt}$  "hashes" the monomials in question  
⇒ there is a unique  $B$  of maximum weight.

## A FEW DETAILS

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

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

**About**  $\text{wt}$ :

- $\text{wt}$  "hashes" the monomials in question  
⇒ 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

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

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

# A FAITHFUL MAP OVER ARBITRARY FIELDS

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

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

## 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

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

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

## 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

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

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

## 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.  $\text{rank}(\varphi_z(\mathcal{H}(\mathbf{f}, \mathbf{v}))) = \text{rank}(\varphi_z(\mathcal{H}(\mathbf{f}, \mathbf{v})) \times M_\varphi)$



# A FAITHFUL MAP OVER ARBITRARY FIELDS

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

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

## 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.  $\text{rank}(\varphi_z(\mathcal{H}(\mathbf{f}, \mathbf{v}))) = \text{rank}(\varphi_z(\mathcal{H}(\mathbf{f}, \mathbf{v})) \times M_\varphi)$
4.  $\text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})) = \text{rank}(\varphi_z(\mathcal{H}(\mathbf{f}, \mathbf{v})))$

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!**