Constructing Faithful Homomorphisms over Fields of Finite Characteristic

Prerona Chatterjee
Joint work with *Ramprasad Saptharishi*

Tata Institute of Fundamental Research, Mumbai

FST&TCS, IIT Bombay

December 11, 2019

Faithful Maps

In the vector space $\mathbb{R}^3$ over $\mathbb{R}$,

$$(1,0,1) \qquad (0,1,0) \qquad (1,2,1)$$

In the vector space $\mathbb{R}^3$ over $\mathbb{R}$,

$$1 \times (1, 0, 1) + 2 \times (0, 1, 0) - 1 \times (1, 2, 1) = 0$$

In the vector space $\mathbb{R}^3$ over $\mathbb{R}$,

$$(1, 0, 1) \qquad (0, 1, 0) \qquad (1, 2, 1)$$

are linearly dependent.

In the vector space $\mathbb{R}^3$ over $\mathbb{R}$,

$$(1, 0, 1) \qquad (0, 1, 0) \qquad (1, 2, 1)$$

are linearly dependent.

In the space of bi-variate polynomials over $\mathbb{C}$,

$$x^2 \qquad y^2 \qquad xy$$

In the vector space $\mathbb{R}^3$ over $\mathbb{R}$,

$$(1, 0, 1) \qquad (0, 1, 0) \qquad (1, 2, 1)$$

are linearly dependent.

In the space of bi-variate polynomials over $\mathbb{C}$,

$$x^2 \quad \times \quad y^2 \quad - \quad (xy)^2 \quad = \quad 0$$

In the vector space $\mathbb{R}^3$ over $\mathbb{R}$,

$$(1,0,1) \qquad (0,1,0) \qquad (1,2,1)$$

are linearly dependent.

In the space of bi-variate polynomials over $\mathbb{C}$,

$$x^2 \qquad y^2 \qquad xy$$

are algebraically dependent.

Definition: Suppose $\{f_1, \ldots, f_k\} \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n]$.

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 $A \in \mathbb{F}[y_1, \ldots, y_k]$

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

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

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.

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.

Note: The underlying field is very important.

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.

Note: The underlying field is very important. For any prime p,

$$x^p + y^p \qquad x + y$$

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.

Note: The underlying field is very important. For any prime p,

$$x^p + y^p \qquad x + y$$

- are algebraically independent over $\mathbb{C}$.

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.

Note: The underlying field is very important. For any prime p,

$$x^p + y^p \qquad x + y$$

- are algebraically independent over $\mathbb{C}$.
- are algebraically dependent over $\mathbb{F}_p$.

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.

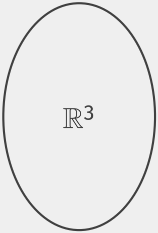
Note: The underlying field is very important. For any prime p,

$$x^p + y^p \qquad x + y$$

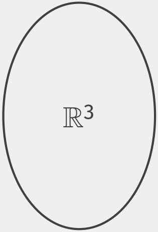
- are algebraically independent over $\mathbb{C}$.
- are algebraically dependent over $\mathbb{F}_p$. $[x^p + y^p = (x + y)^p]$

- Linear rank of $S = \{v_1, \ldots, v_m\} \subseteq \mathbb{V}$ is the size of the largest linearly independent subset of S.

Algebraic Rank



- Linear rank of $S = \{v_1, \ldots, v_m\} \subseteq \mathbb{V}$ is the size of the largest linearly independent subset of S.
- Linear rank of $\{(1,0,1),(0,1,0),(1,2,1)\}$ is 2.



- Linear rank of $S = \{v_1, \ldots, v_m\} \subseteq \mathbb{V}$ is the size of the largest linearly independent subset of S.
- Linear rank of $\{(1,0,1), (0,1,0), (1,2,1)\}$ is 2.

- Algebraic rank of $S = \{f_1, \ldots, f_m\} \subseteq \mathbb{F}[\mathbf{x}]$ is the size of the largest algebraically independent subset of S.

Algebraic Rank

$\mathbb{R}^3$

- Linear rank of $S = \{v_1, \ldots, v_m\} \subseteq \mathbb{V}$ is the size of the largest linearly independent subset of S.
- Linear rank of $\{(1,0,1), (0,1,0), (1,2,1)\}$ is 2.

- Algebraic rank of $S = \{f_1, \ldots, f_m\} \subseteq \mathbb{F}[\mathbf{x}]$ is the size of the largest algebraically independent subset of S.
- Algebraic rank of $\{x^p + y^p, x + y\}$ is 1

$\mathbb{F}_p[x, y]$

Algebraic Rank

$\mathbb{R}^3$

- Linear rank of $S = \{v_1, \ldots, v_m\} \subseteq \mathbb{V}$ is the size of the largest linearly independent subset of S.
- Linear rank of $\{(1,0,1),(0,1,0),(1,2,1)\}$ is 2.

- Algebraic rank of $S = \{f_1, \ldots, f_m\} \subseteq \mathbb{F}[\mathbf{x}]$ is the size of the largest algebraically independent subset of S.
- Algebraic rank of $\{x^p + y^p, x + y\}$ is 2

$\mathbb{C}[x, y]$

Basis in Linear Algebra: Given a set of vectors $\{v_1, v_2, \ldots, v_m\}$ with linear rank k, there is a basis of size k.

Basis in Linear Algebra: Given a set of vectors $\{v_1, v_2, \ldots, v_m\}$ with linear rank k, there is a basis of size k.

Definition: Faithful Maps

Given a set of polynomials $\{f_1, f_2, \ldots, f_m\}$ with algebraic rank k, a map

$$\varphi : \{x_1, x_2, \ldots, x_n\} \to \mathbb{F}[y_1, y_2, \ldots, y_k]$$

is said to be a faithful map if the algebraic rank of $\{f_1 \circ \varphi, f_2 \circ \varphi, \ldots, f_m \circ \varphi\}$ is also k.

Basis in Linear Algebra: Given a set of vectors $\{v_1, v_2, \ldots, v_m\}$ with linear rank k, there is a basis of size k.

Definition: Faithful Maps

Given a set of polynomials $\{f_1, f_2, \ldots, f_m\}$ with algebraic rank k, a map
$$\varphi : \{x_1, x_2, \ldots, x_n\} \to \mathbb{F}[y_1, y_2, \ldots, y_k]$$
is said to be a faithful map if the algebraic rank of $\{f_1 \circ \varphi, f_2 \circ \varphi, \ldots, f_m \circ \varphi\}$ is also k.

Question: Can we construct faithful maps efficiently?

Basis in Linear Algebra: Given a set of vectors $\{v_1, v_2, \ldots, v_m\}$ with linear rank k, there is a basis of size k.

Definition: Faithful Maps

Given a set of polynomials $\{f_1, f_2, \ldots, f_m\}$ with algebraic rank k, a map

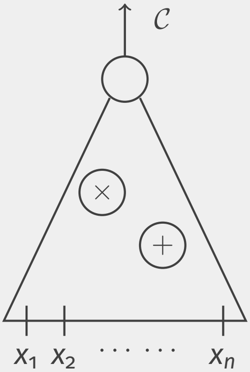
$$\varphi : \{x_1, x_2, \ldots, x_n\} \to \mathbb{F}[y_1, y_2, \ldots, y_k]$$

is said to be a faithful map if the algebraic rank of $\{f_1 \circ \varphi, f_2 \circ \varphi, \ldots, f_m \circ \varphi\}$ is also k.

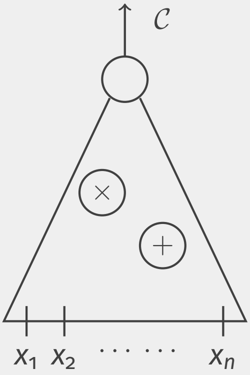
Question: Can we construct faithful maps efficiently?

Bonus: Helps in polynomial identity testing.

Given: Circuit $\mathcal{C}$ that computes an n-variate, degree d polynomial
Goal: Check whether $\mathcal{C} \cong$ Zero Polynomial.



Given: Circuit $\mathcal{C}$ that computes an n-variate, degree d polynomial
Goal: Check whether $\mathcal{C} \cong$ Zero Polynomial.

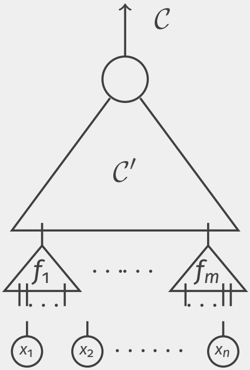


Trivial Upperbound: $(d+1)^n$

Approach: Reduce no. of variables
Keep degree under control
Preserve non-zeroness

Polynomial Identity Testing

Given: Circuit $\mathcal{C}$ that computes an n-variate, degree d polynomial
Goal: Check whether $\mathcal{C} \cong$ Zero Polynomial.



Trivial Upperbound: $(d+1)^n$

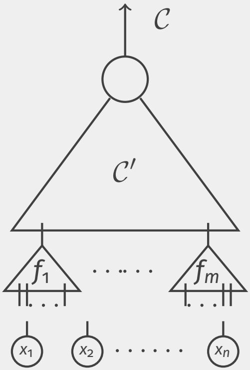
Approach: Reduce no. of variables
Keep degree under control
Preserve non-zeroness

Special Case: $\mathcal{C} = \mathcal{C}'(f_1, f_2, \ldots, f_m)$ where

algebraic rank of $\{f_1, \ldots, f_m\} = k$, and

$$k \ll n$$

Given: Circuit $\mathcal{C}$ that computes an n-variate, degree d polynomial
Goal: Check whether $\mathcal{C} \cong$ Zero Polynomial.



Trivial Upperbound: $(d+1)^n$

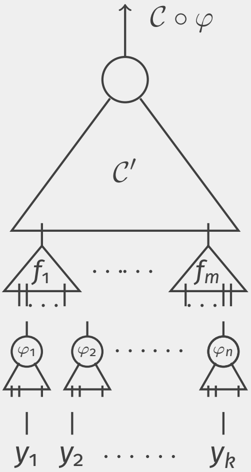
Approach: Reduce no. of variables
Keep degree under control
Preserve non-zeroness

Special Case: $\mathcal{C} = \mathcal{C}'(f_1, f_2, \ldots, f_m)$ where

algebraic rank of $\{f_1, \ldots, f_m\} = k$, and

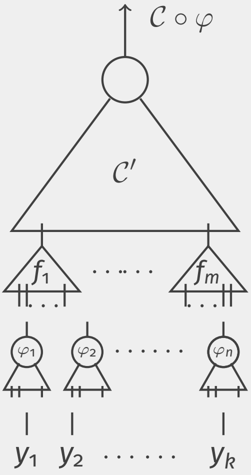
$$k \ll n$$

Q: Can the upperbound be made $\approx (d+1)^k$?



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

Faithful Maps and PIT [BMS13, ASSS16]

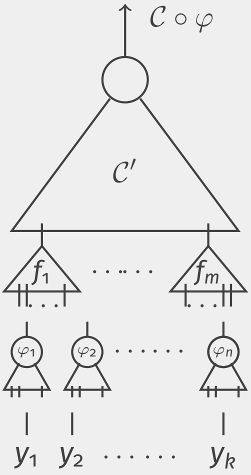


Property required: $\mathcal{C} \neq 0 \implies \mathcal{C} \circ \varphi \neq 0$

If $k = m$ and $\mathcal{C}' \neq 0$,

$$\mathcal{C}'(f_1, \ldots, f_k) \neq 0$$

Faithful Maps and PIT [BMS13, ASSS16]



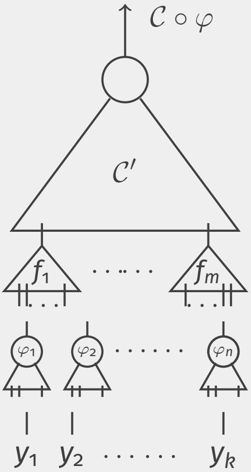
Property required: $\mathcal{C} \neq 0 \implies \mathcal{C} \circ \varphi \neq 0$

If $k = m$ and $\mathcal{C}' \neq 0$,

$$\mathcal{C}'(f_1, \ldots, f_k) \neq 0$$

Since φ is faithful,

$$\mathcal{C} \circ \varphi = \mathcal{C}'(f_1 \circ \varphi, \ldots, f_k \circ \varphi) \neq 0$$



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

If $k = m$ and $\mathcal{C}' \neq 0$,

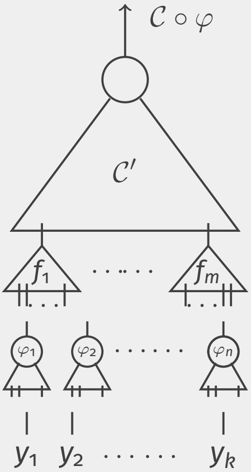
$$\mathcal{C}'(f_1, \ldots, f_k) \neq 0$$

Since φ is faithful,

$$\mathcal{C} \circ \varphi = \mathcal{C}'(f_1 \circ \varphi, \ldots, f_k \circ \varphi) \neq 0$$

Thus,

$$\mathcal{C} \neq 0 \implies \mathcal{C} \circ \varphi \neq 0$$



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

If $k = m$ and $\mathcal{C}' \neq 0$,

$$\mathcal{C}'(f_1, \ldots, f_k) \neq 0$$

Since φ is faithful,

$$\mathcal{C} \circ \varphi = \mathcal{C}'(f_1 \circ \varphi, \ldots, f_k \circ \varphi) \neq 0$$

Thus,

$$\mathcal{C} \neq 0 \implies \mathcal{C} \circ \varphi \neq 0$$

Fact: Even when $k < m$, if φ is faithful,

$$\mathcal{C} \neq 0 \implies \mathcal{C} \circ \varphi \neq 0$$

Constructing Faithful Maps

The Question

Given a set of polynomials $\{f_1, f_2, \ldots, f_m\} \subseteq \mathbb{F}[x_1, \ldots, x_n]$, we want to construct a map

$$\varphi : \{x_1, x_2, \ldots, x_n\} \to \mathbb{F}[y_1, y_2, \ldots, y_k]$$

such that

$$\mathrm{algrank}(f_1(\varphi), f_2(\varphi), \ldots, f_m(\varphi)) = \mathrm{algrank}(f_1, f_2, \ldots, f_m)$$

Given a set of polynomials $\{f_1, f_2, \ldots, f_m\} \subseteq \mathbb{F}[x_1, \ldots, x_n]$, we want to construct a map

$$\varphi : \{x_1, x_2, \ldots, x_n\} \to \mathbb{F}[y_1, y_2, \ldots, y_k]$$

such that

$$\text{algrank}(f_1(\varphi), f_2(\varphi), \ldots, f_m(\varphi)) = \text{algrank}(f_1, f_2, \ldots, f_m)$$

Fact: A random affine transformation is a faithful map

$$\varphi : x_i = \sum_{j=1}^{k} s_{ij} y_j + a_i$$

The Question

Given a set of polynomials $\{f_1, f_2, \ldots, f_m\} \subseteq \mathbb{F}[x_1, \ldots, x_n]$, we want to construct a map

$$\varphi : \{x_1, x_2, \ldots, x_n\} \to \mathbb{F}[y_1, y_2, \ldots, y_k]$$

such that

$$\mathrm{algrank}(f_1(\varphi), f_2(\varphi), \ldots, f_m(\varphi)) = \mathrm{algrank}(f_1, f_2, \ldots, f_m)$$

Fact: A random affine transformation is a faithful map

$$\varphi : x_i = \sum_{j=1}^{k} s_{ij} y_j + a_i$$

Question: Can we construct faithful maps deterministically?

Characteristic Zero Fields [BMS13, ASSS16]

Step 1: Capture algebraic rank via linear rank

Step 1: Capture algebraic rank via linear rank

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

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

Step 1: Capture algebraic rank via linear rank

For $\{f_1, f_2, \ldots, f_m\} \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n]$ 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 [Jac41]

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.

Step 1: Capture algebraic rank via linear rank of the Jacobian

For $\{f_1, f_2, \ldots, f_m\} \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n]$ 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 [Jac41]

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.

Step 2: Start with a generic linear transformation

$$\varphi : x_i = \sum_{j=1}^{k} s_{ij} y_j + a_i$$

Step 2: Start with a generic linear transformation

$$\varphi : x_i = \sum_{j=1}^{k} s_{ij} y_j + a_i$$

$$\begin{bmatrix} \\ \mathbf{J_y}(\mathbf{f}(\varphi)) \\ \\ \end{bmatrix}$$

Step 2: Start with a generic linear transformation

$$\varphi : x_i = \sum_{j=1}^{k} s_{ij} y_j + a_i$$

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

Step 2: Start with a generic linear transformation

$$\varphi : x_i = \sum_{j=1}^{k} s_{ij} y_j + a_i$$

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

What we need: φ such that

- $\mathrm{rank}(\mathbf{J_x}(\mathbf{f})) = \mathrm{rank}(\varphi(\mathbf{J_x}(\mathbf{f})))$

Step 2: Start with a generic linear transformation

$$\varphi : x_i = \sum_{j=1}^{k} s_{ij} y_j + a_i$$

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

What we need: φ such that

- $\mathrm{rank}(\mathbf{J_x}(\mathbf{f})) = \mathrm{rank}(\varphi(\mathbf{J_x}(\mathbf{f})))$: Can be done if f_is are structured

Step 2: Start with a generic linear transformation

$$\varphi : x_i = \sum_{j=1}^{k} s_{ij} y_j + a_i$$

$$\begin{bmatrix} \\ \mathbf{J}_{\mathbf{y}}(\mathbf{f}(\varphi)) \\ \\ \end{bmatrix} = \begin{bmatrix} \\ \varphi(\mathbf{J}_{\mathbf{x}}(\mathbf{f})) \\ \\ \end{bmatrix} \times \begin{bmatrix} \\ \\ M_\varphi \\ \\ \\ \end{bmatrix}$$

What we need: φ such that

- $\mathrm{rank}(\mathbf{J}_{\mathbf{x}}(\mathbf{f})) = \mathrm{rank}(\varphi(\mathbf{J}_{\mathbf{x}}(\mathbf{f})))$: Can be done if f_is are structured
- M_φ preserves rank

Step 2: Start with a generic linear transformation

$$\varphi : x_i = \sum_{j=1}^{k} s_{ij} y_j + a_i$$

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

What we need: φ such that

- $\mathrm{rank}(\mathbf{J_x}(\mathbf{f})) = \mathrm{rank}(\varphi(\mathbf{J_x}(\mathbf{f})))$: Can be done if f_is are structured
- M_φ preserves rank : True if $\left\{ M_\varphi[i,j] = s^{ij} \right\}$ . . . . [GR05]

Step 2: Start with a generic linear transformation

$$\varphi : x_i = \sum_{j=1}^{k} s^{ij} y_j + a_i$$

$$\begin{bmatrix} \\ \mathbf{J}_{\mathbf{y}}(\mathbf{f}(\varphi)) \\ \\ \end{bmatrix} = \begin{bmatrix} \\ \varphi(\mathbf{J}_{\mathbf{x}}(\mathbf{f})) \\ \\ \end{bmatrix} \times \begin{bmatrix} \\ \\ M_\varphi \\ \\ \\ \end{bmatrix}$$

What we need: φ such that

- $\mathrm{rank}(\mathbf{J}_{\mathbf{x}}(\mathbf{f})) = \mathrm{rank}(\varphi(\mathbf{J}_{\mathbf{x}}(\mathbf{f})))$: Can be done if f_is are structured
- M_φ preserves rank : True if $\left\{ M_\varphi[i,j] = s^{ij} \right\}$ . . . . [GR05]

What happens over Finite Characteristic Fields?

What happens over Finite Characteristic Fields?

The Jacobian Criterion is **false** over finite characteristic fields.

The Jacobian Criterion is **false** over finite characteristic fields.

Taylor Expansion

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

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

The Jacobian Criterion is **false** over finite characteristic fields.

Taylor Expansion

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

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

[PSS18]: Look up till the inseparable degree in the expansion.

The Jacobian Criterion is **false** over finite characteristic fields.

Taylor Expansion

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

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

[PSS18]: Look up till the inseparable degree in the expansion.

Definition: A new Operator

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

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

The Jacobian Criterion is **false** over finite characteristic fields.

Taylor Expansion

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

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

[PSS18]: Look up till the inseparable degree in the expansion.

Definition: A new Operator

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

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

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

$f_1, f_2, \ldots, f_k \in \mathbb{F}[\mathbf{x}]$ are algebraically independent if and only if for every $(v_1, v_2, \ldots, v_k)$ with v_is in $\mathcal{I}_t$,

$f_1, f_2, \ldots, f_k \in \mathbb{F}[\mathbf{x}]$ are algebraically independent if and only if for every $(v_1, v_2, \ldots, v_k)$ with v_is in $\mathcal{I}_t$,

$$\mathcal{H}(\mathbf{f}, \mathbf{v}) = \begin{bmatrix} \ldots & \mathcal{H}_t(f_1) + v_1 & \ldots \\ \ldots & \mathcal{H}_t(f_2) + v_2 & \ldots \\ & \vdots & \\ \ldots & \mathcal{H}_t(f_k) + v_k & \ldots \end{bmatrix}$$

Alternate Criterion for the General Case [PSS18]

$f_1, f_2, \ldots, f_k \in \mathbb{F}[\mathbf{x}]$ are algebraically independent if and only if for every $(v_1, v_2, \ldots, v_k)$ with v_is in $\mathcal{I}_t$,

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

Alternate Criterion for the General Case [PSS18]

$f_1, f_2, \ldots, f_k \in \mathbb{F}[\mathbf{x}]$ are algebraically independent if and only if for every $(v_1, v_2, \ldots, v_k)$ with v_is in $\mathcal{I}_t$,

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

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

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

Our Result

Suspose

- $\circ$ $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$
- $\circ$ algebraic rank of $\{f_1, \ldots, f_m\} = k$
- $\circ$ inseparable degree of $\{f_1, \ldots, f_m\} = t$

Suppose
- $\circ\ f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$
- $\circ$ algebraic rank of $\{f_1, \ldots, f_m\} = k$
- $\circ$ inseparable degree of $\{f_1, \ldots, f_m\} = t$

Then, we can construct

$$\Phi : \mathbb{F}[\mathbf{x}] \to \mathbb{F}(s)[y_0, y_1, \ldots, y_k]$$

Our Result

Suppose

- $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$
- algebraic rank of $\{f_1, \ldots, f_m\} = k$
- inseparable degree of $\{f_1, \ldots, f_m\} = t$

Then, we can construct

$$\Phi : \mathbb{F}[\mathbf{x}] \to \mathbb{F}(s)[y_0, y_1, \ldots, y_k]$$

such that

$$\mathrm{algrank}_{\mathbb{F}}(f_1 \circ \Phi, \ldots, f_m \circ \Phi) = k$$

Our Result

Suppose
- $\circ\ f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$
- $\circ$ algebraic rank of $\{f_1, \ldots, f_m\} = k$
- $\circ$ inseparable degree of $\{f_1, \ldots, f_m\} = t$

Then, we can construct

$$\Phi : \mathbb{F}[\mathbf{x}] \to \mathbb{F}(s)[y_0, y_1, \ldots, y_k]$$

such that

$$\mathrm{algrank}_{\mathbb{F}}(f_1 \circ \Phi, \ldots, f_m \circ \Phi) = k$$

whenever

- each of the f_i's are sparse polynomials,
- each of the f_i's are products of variable disjoint, multilinear, sparse polynomials.

Step 1: Capture algebraic rank via linear rank of the PSS-Jacobian

Step 1: Capture algebraic rank via linear rank of the PSS-Jacobian

Step 2: For a *generic linear map* $\Phi : \mathbf{x} \to \mathbb{F}(s)[y_1, \ldots, y_k]$,
write **PSS** $\mathbf{J_y}(\mathbf{f} \circ \Phi)$ in terms of **PSS** $\mathbf{J_x}(\mathbf{f})$.

Step 1: Capture algebraic rank via linear rank of the PSS-Jacobian

Step 2: For a *generic linear map* $\Phi : \mathbf{x} \to \mathbb{F}(s)[y_1, \ldots, y_k]$, write **PSS** $\mathbf{J_y}(\mathbf{f} \circ \Phi)$ in terms of **PSS** $\mathbf{J_x}(\mathbf{f})$. This can be described succinctly as

$$\textbf{PSS } \mathbf{J_y}(f \circ \Phi) = \Phi(\textbf{PSS } \mathbf{J_x}(\mathbf{f})) \cdot M_\Phi .$$

Step 1: Capture algebraic rank via linear rank of the PSS-Jacobian

Step 2: For a *generic linear map* $\Phi : \mathbf{x} \to \mathbb{F}(s)[y_1, \ldots, y_k]$, write $\textbf{PSS}\ \mathbf{J_y}(\mathbf{f} \circ \Phi)$ in terms of $\textbf{PSS}\ \mathbf{J_x}(\mathbf{f})$. This can be described succinctly as

$$\textbf{PSS}\ \mathbf{J_y}(f \circ \Phi) = \Phi(\textbf{PSS}\ \mathbf{J_x}(\mathbf{f})) \cdot M_\Phi .$$

What we need: Φ such that

- $\mathrm{rank}(\Phi(\textbf{PSS}\ \mathbf{J_x}(\mathbf{f}))) = \mathrm{rank}(\textbf{PSS}\ \mathbf{J_x}(\mathbf{f}))$: Can be done if $\mathbf{f}$'s are some structured polynomials (for example, sparse).

Step 1: Capture algebraic rank via linear rank of the PSS-Jacobian

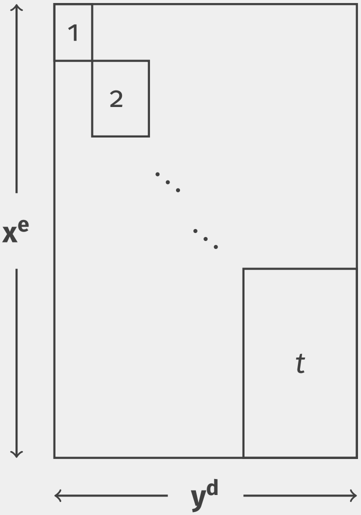
Step 2: For a *generic linear map* $\Phi : \mathbf{x} \to \mathbb{F}(s)[y_1, \ldots, y_k]$, write **PSS** $\mathbf{J_y}(\mathbf{f} \circ \Phi)$ in terms of **PSS** $\mathbf{J_x}(\mathbf{f})$. This can be described succinctly as

$$\textbf{PSS } \mathbf{J_y}(f \circ \Phi) = \Phi(\textbf{PSS } \mathbf{J_x}(\mathbf{f})) \cdot M_\Phi.$$

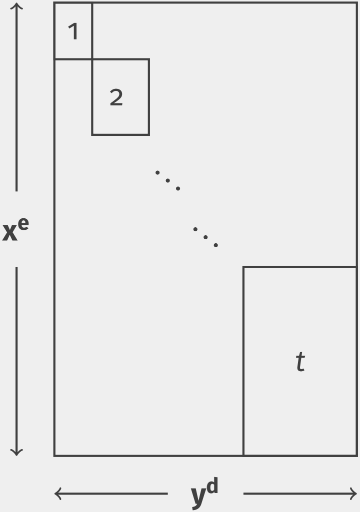
What we need: Φ such that

- $\mathrm{rank}(\Phi(\textbf{PSS } \mathbf{J_x}(\mathbf{f}))) = \mathrm{rank}(\textbf{PSS } \mathbf{J_x}(\mathbf{f}))$: Can be done if **f**'s are some structured polynomials (for example, sparse).
- M_Φ preserves rank. That is,

$$\mathrm{rank}(\Phi(\textbf{PSS } \mathbf{J_x}(\mathbf{f})) \cdot M_\Phi) = \mathrm{rank}(\Phi(\textbf{PSS } \mathbf{J_x}(\mathbf{f}))).$$

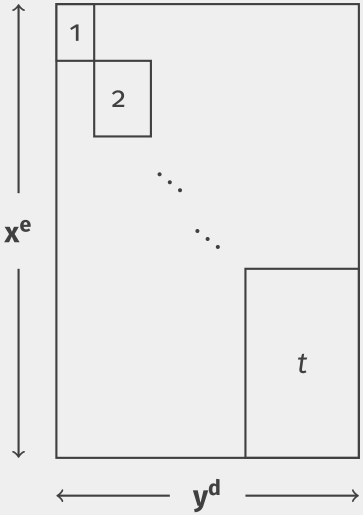


$$M_\Phi(\mathbf{x^e}, \mathbf{y^d}) = \text{coeff}_{\mathbf{y^d}}(\Phi(\mathbf{x^e}))$$



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

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

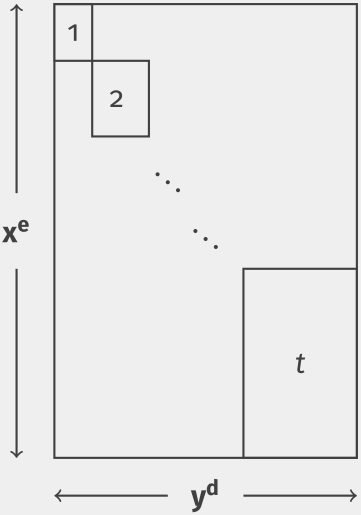


$$M_\Phi(\mathbf{x}^{\mathbf{e}}, \mathbf{y}^{\mathbf{d}}) = \mathrm{coeff}_{\mathbf{y}^{\mathbf{d}}}(\Phi(\mathbf{x}^{\mathbf{e}}))$$

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

For the correct definition of wt(i), things work out.

The Faithful Map



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

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

For the correct definition of $\mathrm{wt}(i)$, things work out.

$$\Phi(x_i) = a_i \cdot y_0 + \sum_{j \in [k]} s^{\mathrm{wt}(i)j} \cdot y_j$$

1. Construct $\mathbb{F}(s)$-Faithful maps over arbitrary fields.

1. Construct $\mathbb{F}(s)$-Faithful maps over arbitrary fields.
2. Improve the dependence on "inseparable degree".

Open Threads

1. Construct $\mathbb{F}(s)$-Faithful maps over arbitrary fields.
2. Improve the dependence on "inseparable degree".
3. [GSS'18]: Different characterisation for Algebraic dependence - not algorithmic but has no dependence on "inseparable degree"

   Can we get PIT applications out of it?

1. Construct $\mathbb{F}(s)$-Faithful maps over arbitrary fields.
2. Improve the dependence on "inseparable degree".
3. [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!