Constructing Faithful Maps over Arbitrary Fields

Prerona Chatterjee

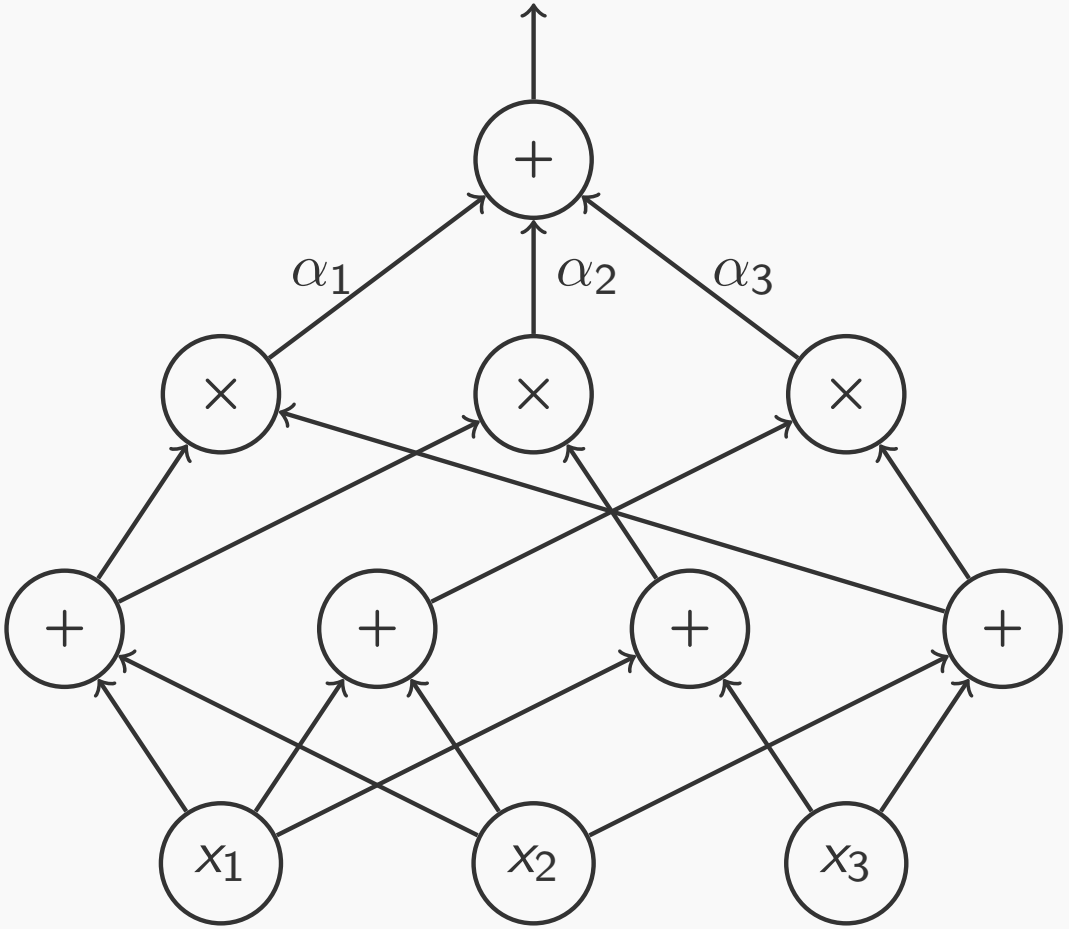
joint work with

Ramprasad Saptharishi

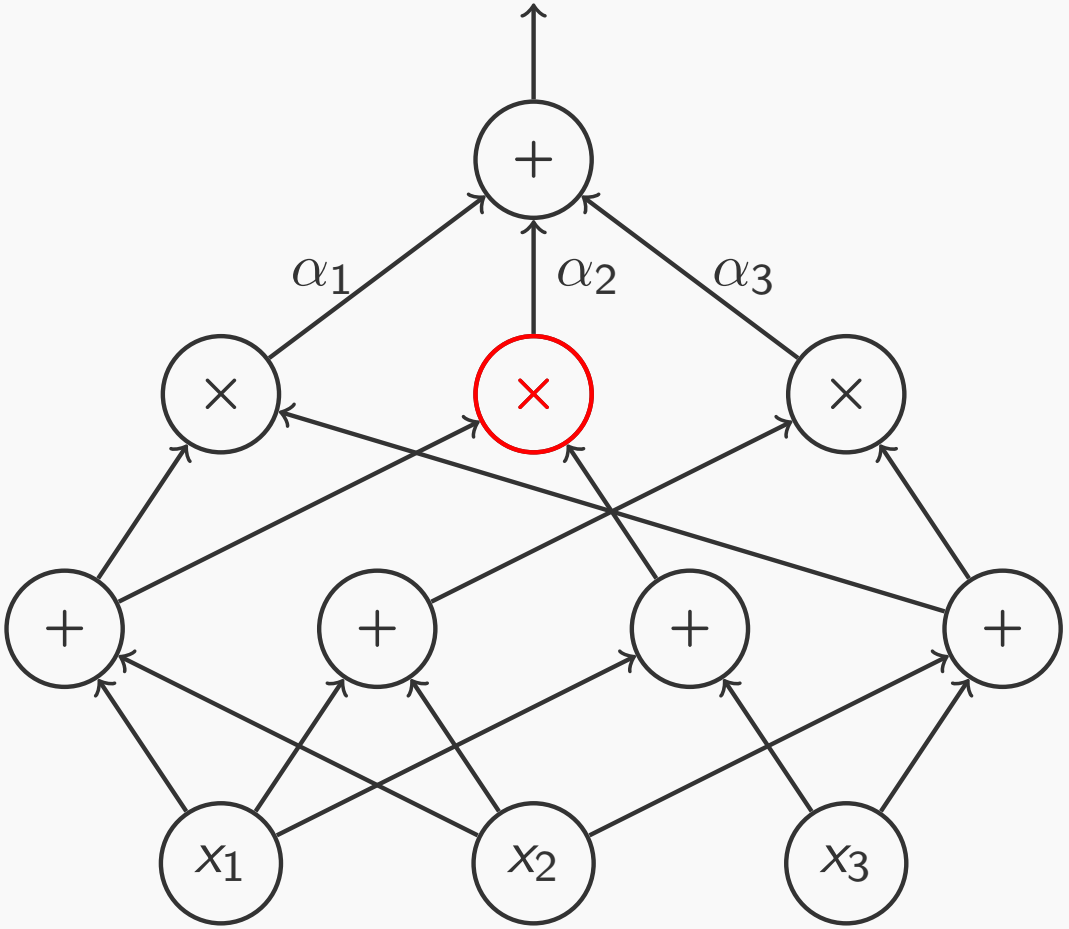
TIFR, Mumbai

February 16, 2018

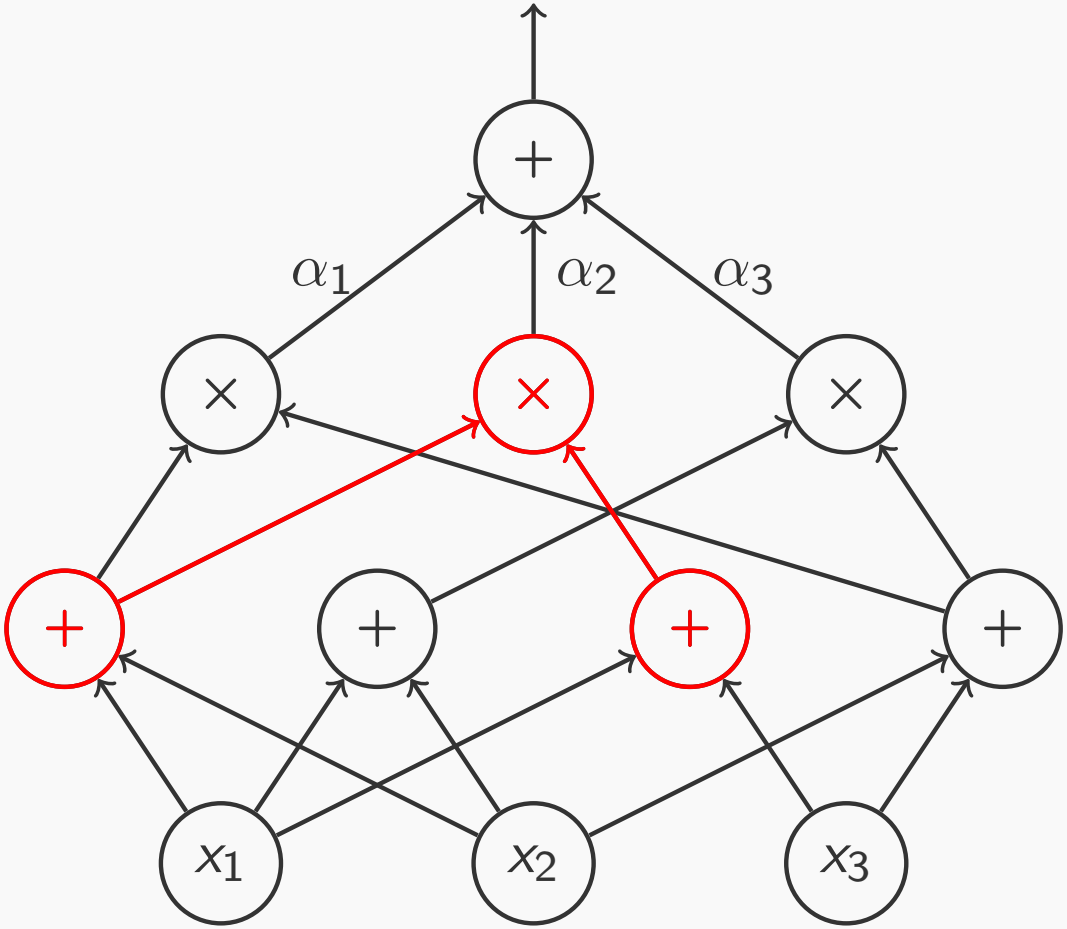
Algebraic Circuits and Polynomial Identity Testing



Algebraic Circuits and Polynomial Identity Testing

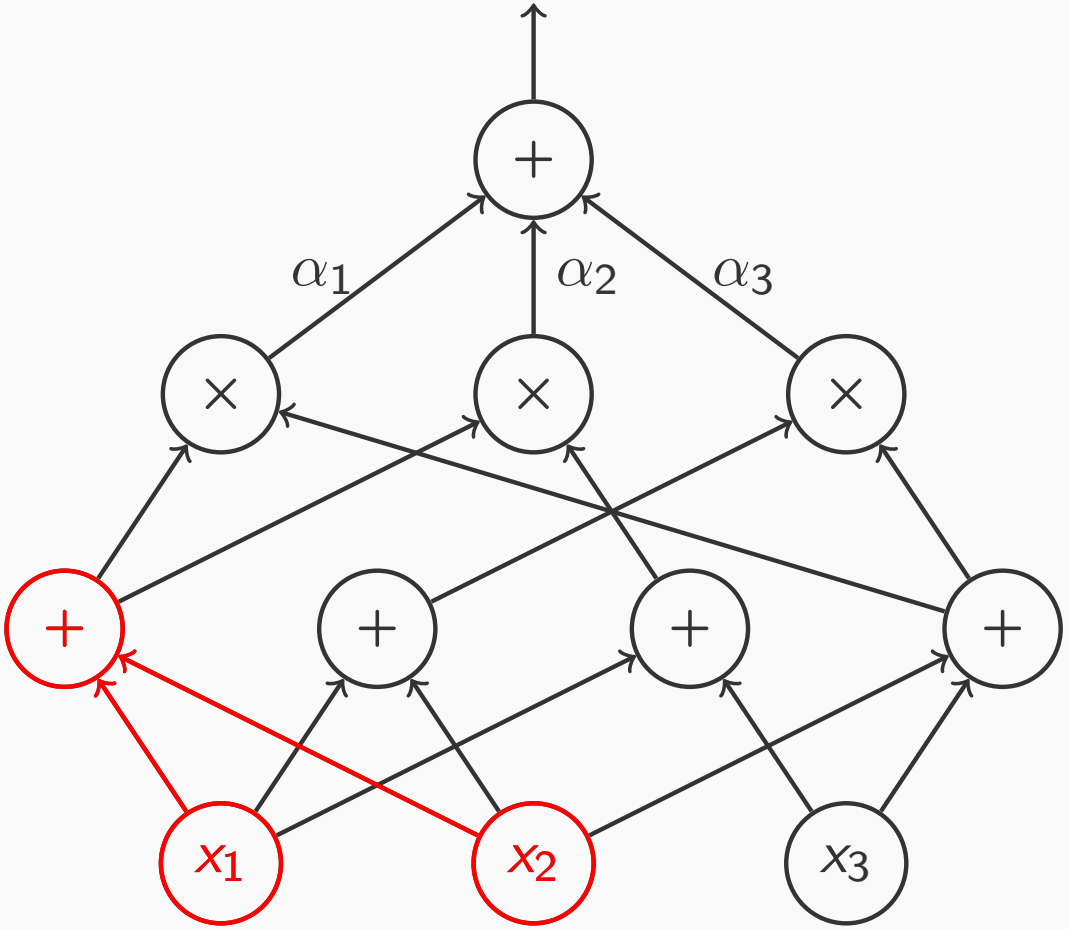


Algebraic Circuits and Polynomial Identity Testing



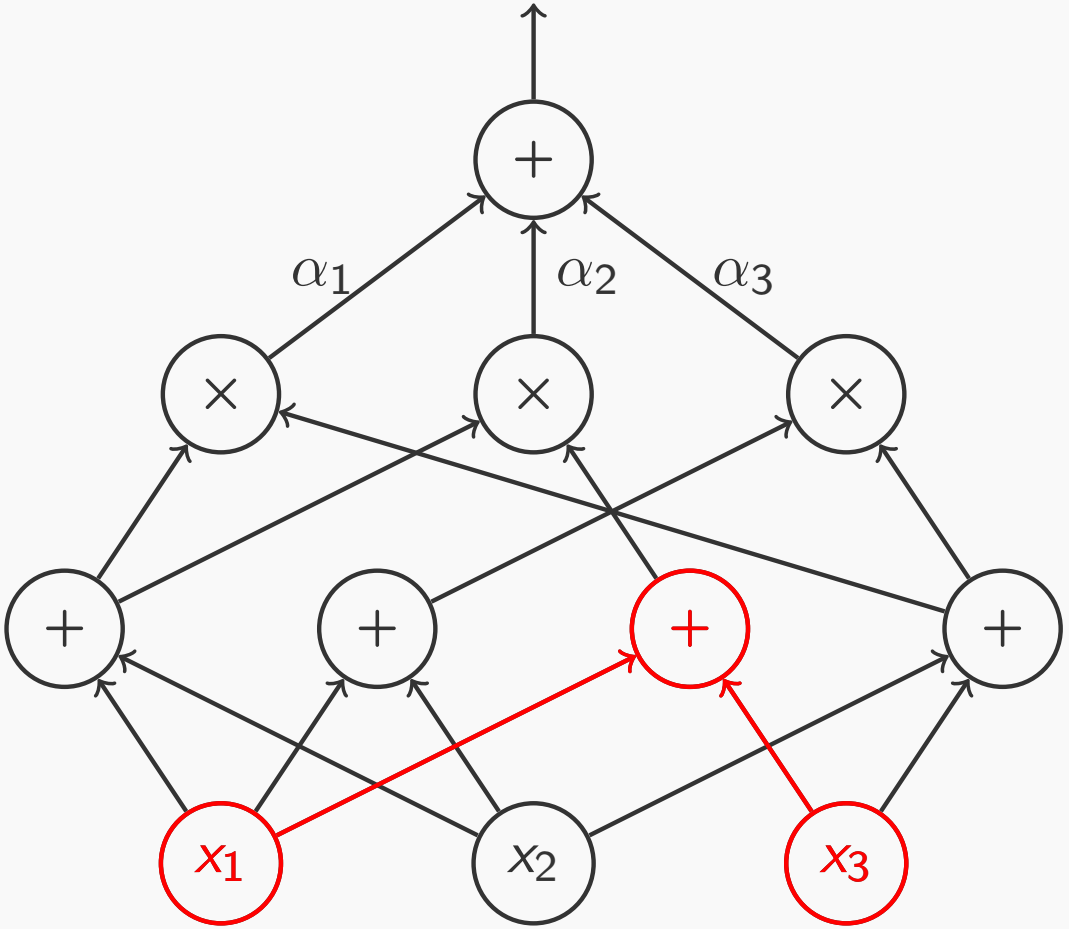
$$()\cdot()$$

Algebraic Circuits and Polynomial Identity Testing



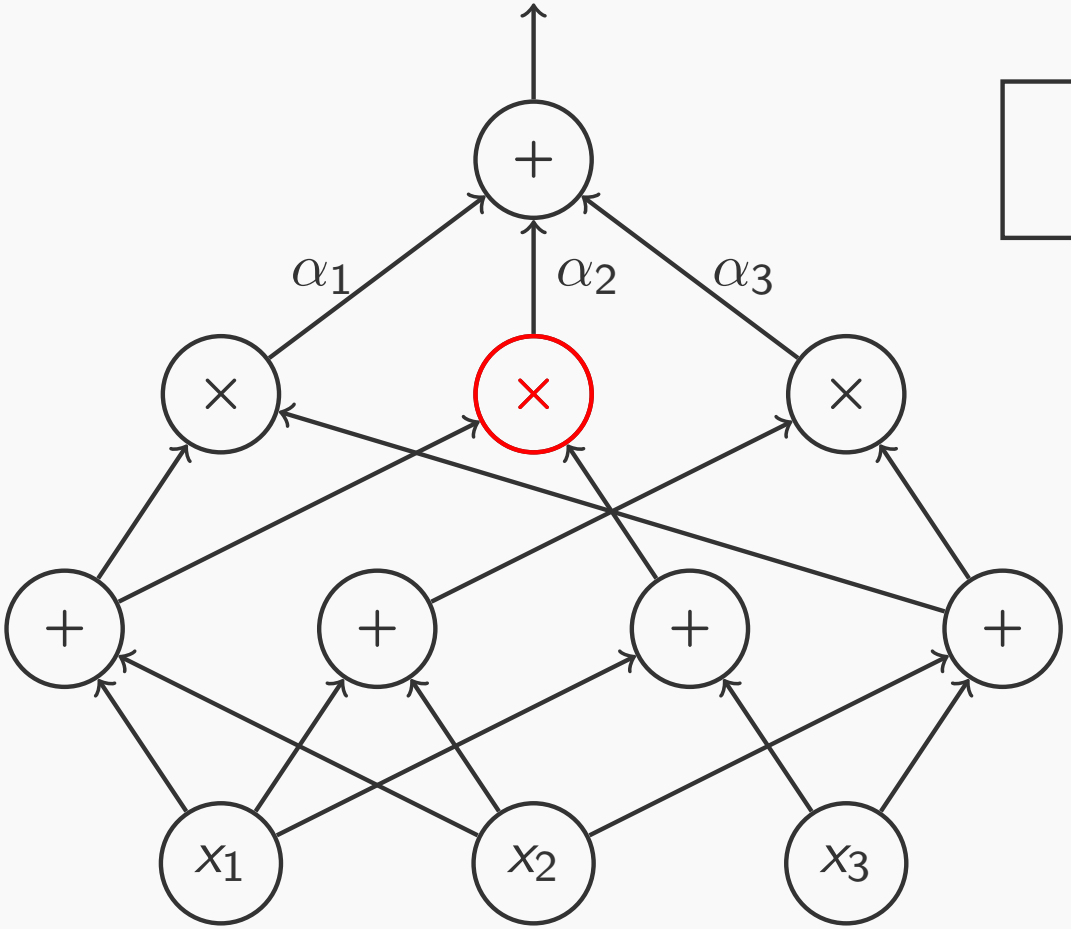
$$(x_1 + x_2) \cdot ()$$

Algebraic Circuits and Polynomial Identity Testing



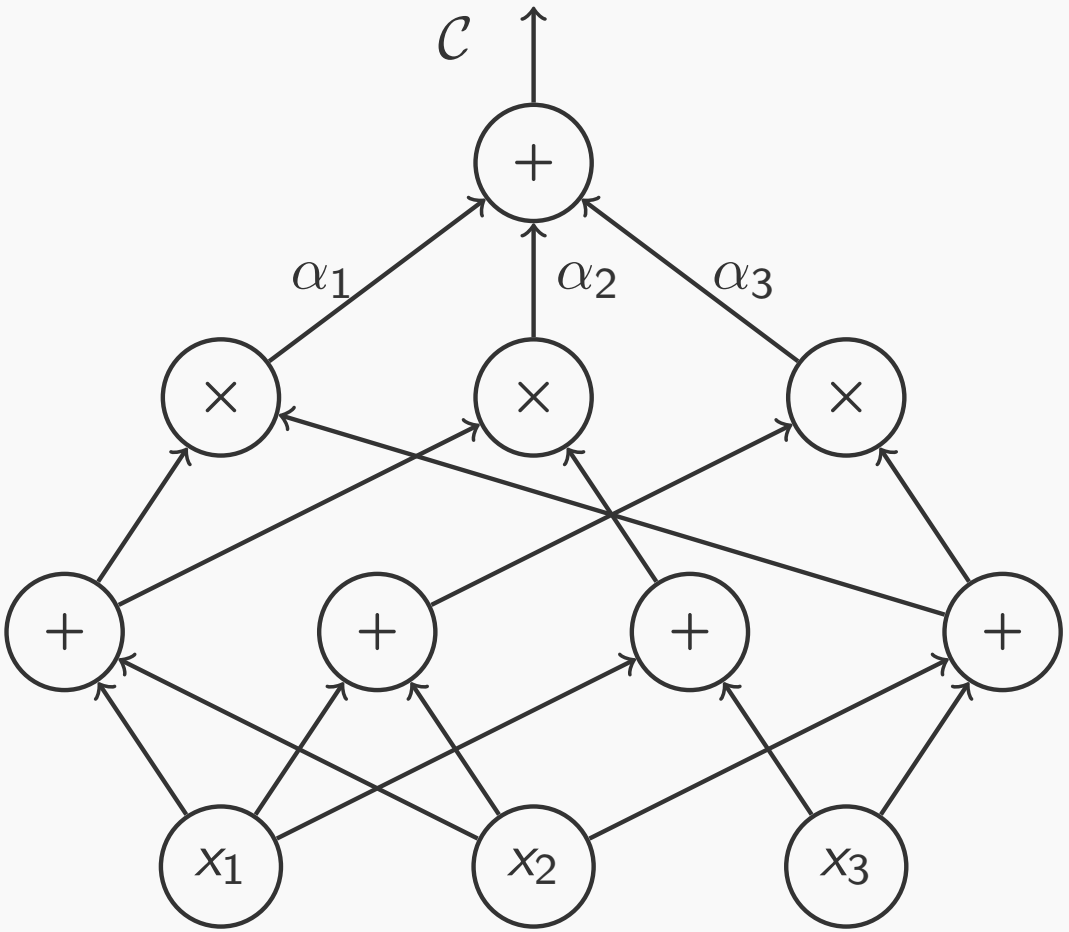
$$(x_1 + x_2) \cdot (x_1 + x_3)$$

Algebraic Circuits and Polynomial Identity Testing



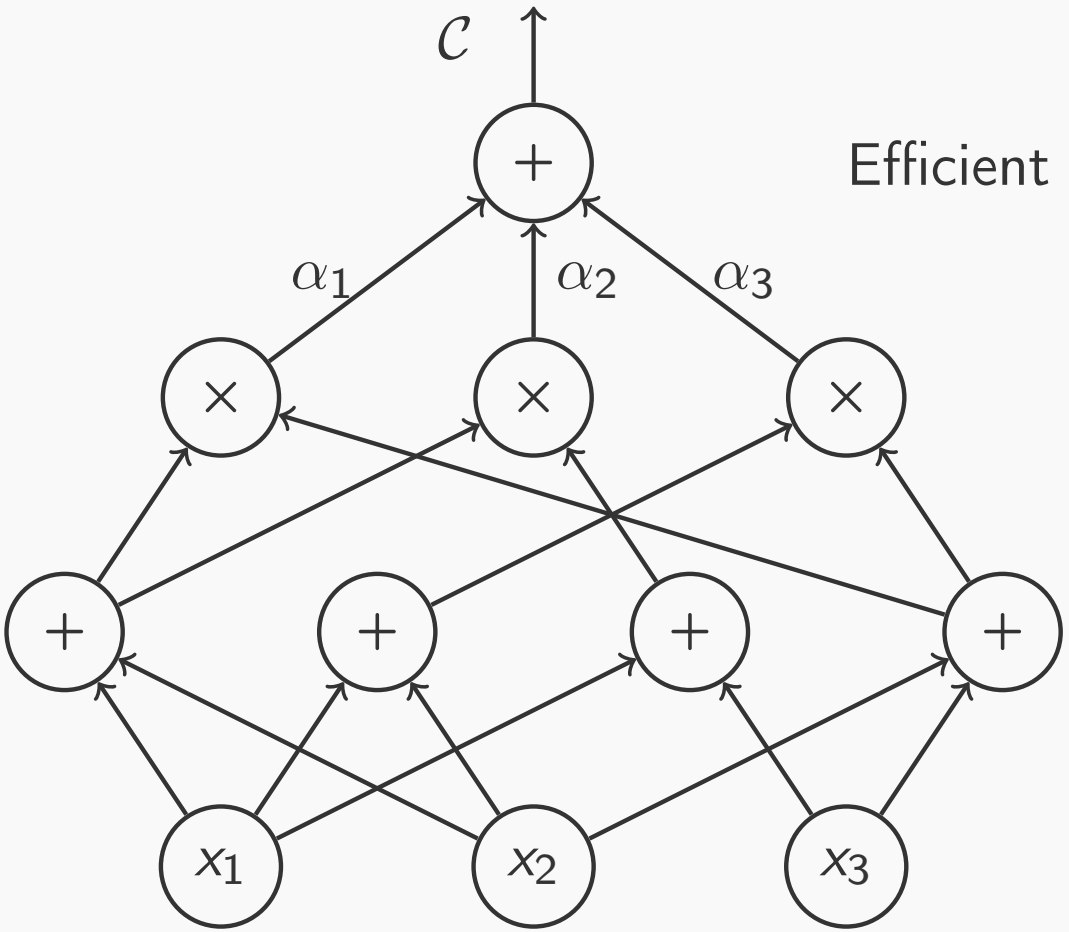
$$(x_1 + x_2) \cdot (x_1 + x_3)$$

Algebraic Circuits and Polynomial Identity Testing



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

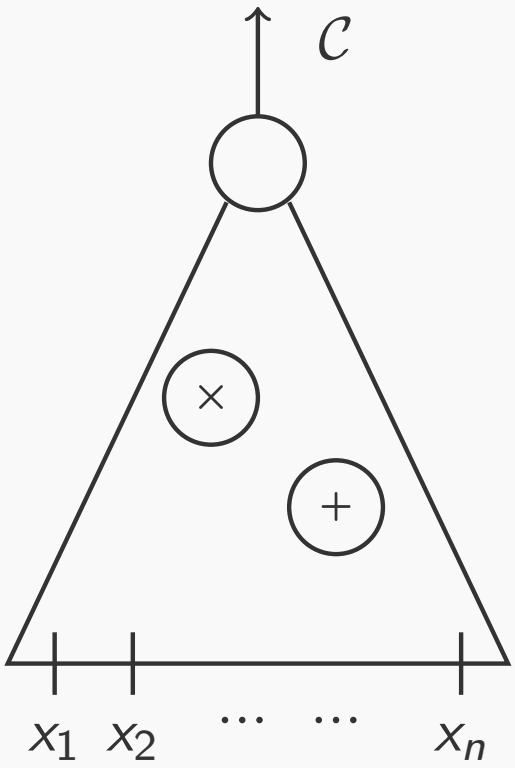
Algebraic Circuits and Polynomial Identity Testing



Efficient deterministic PIT not known for general circuits

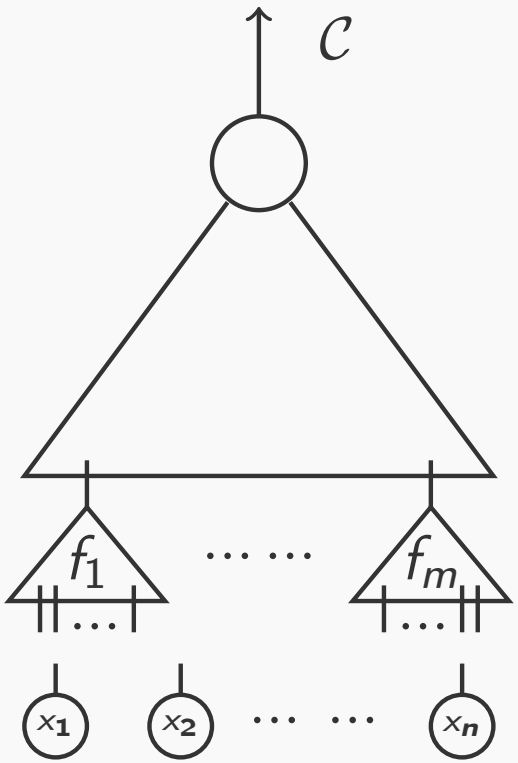
$$\mathcal{C} \stackrel{?}{=} 0$$

Polynomial Identity Testing and Faithful Maps



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

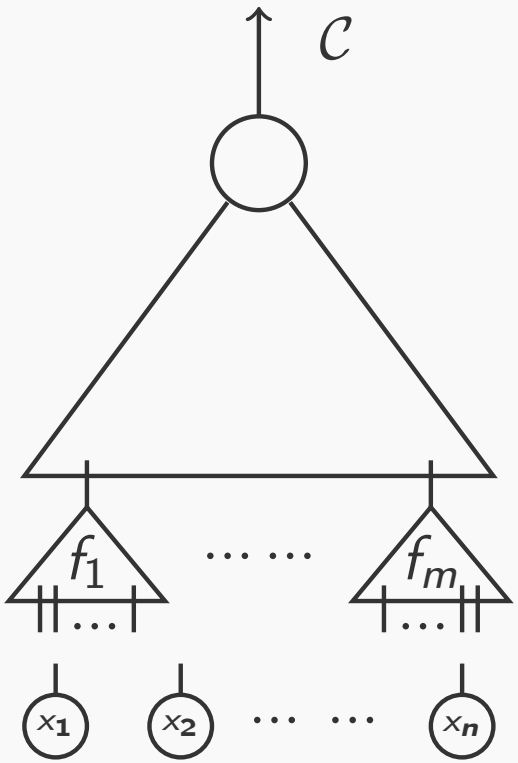
Polynomial Identity Testing and Faithful Maps



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

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

Polynomial Identity Testing and Faithful Maps

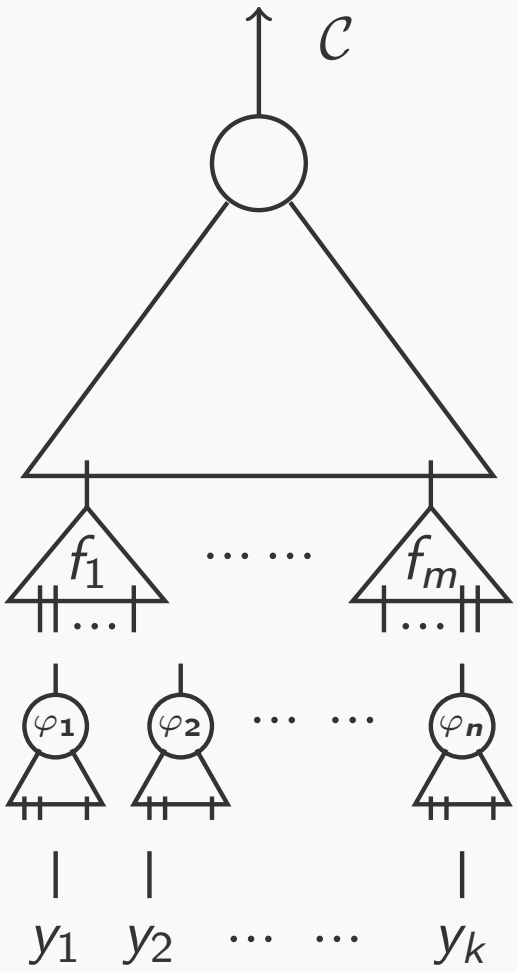


Check whether $\mathcal{C}$ computes the zero polynomial or not.

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

Only k of them are "relevant"

Polynomial Identity Testing and Faithful Maps



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

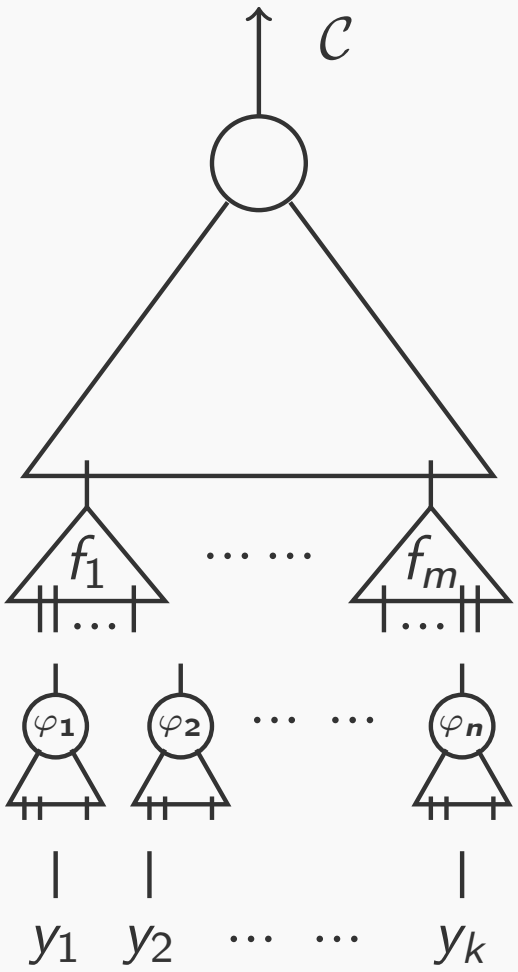
$\mathcal{C} = \mathcal{C}(f_1, f_2, \ldots, f_m)$

Only k of them are "relevant"

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

is a "good" map

Polynomial Identity Testing and Faithful Maps



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"

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

is a "good" map

$\mathcal{C}(f_1, f_2, \ldots, f_m) \neq 0$ if and only if

$(\mathcal{C}(f_1(\varphi), f_2(\varphi), \ldots f_m(\varphi))) \neq 0.$

How many are "Relevant"?

Definition: Algebraic Independence

A given set of polynomials $\{f_1, f_2, \ldots, f_m\} \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n]$ is said to be algebraically dependent if there is a non-zero polynomial combination of these that is zero.

Otherwise, they are said to be algebraically independent.

How many are "Relevant"?

Definition: Algebraic Independence

A given set of polynomials $\{f_1, f_2, \ldots, f_m\} \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n]$ is said to be algebraically dependent if there is a non-zero polynomial combination of these that is zero.

Otherwise, they are said to be algebraically independent.

For a set of polynomials $\{f_1, f_2, \ldots, f_m\}$, the family of all algebraically independent subsets form a matroid.

Thus, $\text{algrank}(f_1, f_2, \ldots, f_m)$ is well defined.

Checking for Relevance over Characteristic Zero fields

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

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

Checking for Relevance over Characteristic Zero fields

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

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

The Jacobian Criterion

If $\mathbb{F}$ has characteristic zero, $\{f_1, f_2, \ldots, f_m\}$ is algebraically independent if and only if its Jacobian matrix is full rank.

"Good" Maps

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 $\{f_1(\varphi), f_2(\varphi), \ldots, f_m(\varphi)\}$ is also k.

"Good" Maps

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 $\{f_1(\varphi), f_2(\varphi), \ldots, f_m(\varphi)\}$ is also k.

The Connection [BMS11, ASSS12]: Given a set of polynomials $\{f_1, f_2, \ldots, f_m\}$ and a faithful map φ; for any circuit $\mathcal{C}(z_1, \ldots, z_m)$,

$$\mathcal{C}(f_1, f_2, \ldots, f_m) \neq 0 \Leftrightarrow (\mathcal{C}(f_1(\varphi), f_2(\varphi), \ldots f_m(\varphi))) \neq 0.$$

Constructing Good Maps over Characteristic Zero Fields

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

Constructing Good Maps over Characteristic Zero Fields

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

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

Constructing Good Maps over Characteristic Zero Fields

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

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

Constructing Good Maps over Characteristic Zero Fields

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

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

What we need: φ such that

1. $\text{rank}(\mathbf{J_x}(\mathbf{f})) = \text{rank}(\varphi(\mathbf{J_x}(\mathbf{f})))$

Constructing Good Maps over Characteristic Zero Fields

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

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

What we need: φ such that

1. $\text{rank}(\mathbf{J_x}(\mathbf{f})) = \text{rank}(\varphi(\mathbf{J_x}(\mathbf{f})))$: Can be handled by choosing a_is correctly.

Constructing Good Maps over Characteristic Zero Fields

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

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

What we need: φ such that

1. $\text{rank}(\mathbf{J_x}(\mathbf{f})) = \text{rank}(\varphi(\mathbf{J_x}(\mathbf{f})))$
2. $\text{rank}(\varphi(\mathbf{J_x}(\mathbf{f}))) = \text{rank}(\varphi(\mathbf{J_x}(\mathbf{f})) \times M_\varphi)$

How we need M_φ to behave

For every $m \times n$ matrix A, $\text{rank}(A) = \text{rank}(AM_\varphi)$.

How we need M_φ to behave

For every $m \times n$ matrix A, $\mathrm{rank}(A) = \mathrm{rank}(AM_\varphi)$.

$$\left[\begin{array}{c} \\ A \\ \\ \end{array}\right]_{m \times n}$$

How we need M_φ to behave

For every $m \times n$ matrix A, $\mathrm{rank}(A) = \mathrm{rank}(AM_\varphi)$.

$$\begin{bmatrix} & A' & \end{bmatrix}_{k \times n}$$

How we need M_φ to behave

For every $m \times n$ matrix A, $\operatorname{rank}(A) = \operatorname{rank}(AM_\varphi)$.

$$\begin{bmatrix} & A' & \end{bmatrix} \times \begin{bmatrix} & M_\varphi & \end{bmatrix} = \begin{bmatrix} & A'M_\varphi & \end{bmatrix}$$

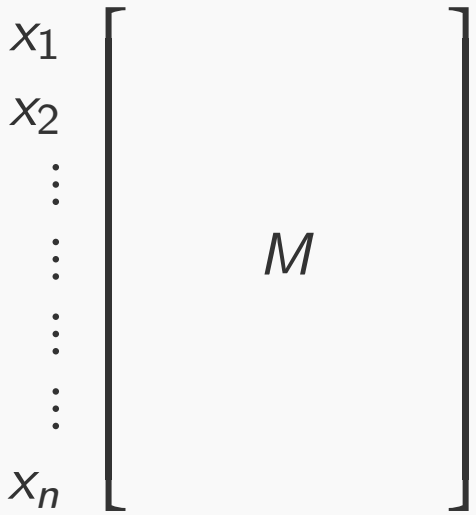
How we need M_φ to behave

For every $m \times n$ matrix A, $\text{rank}(A) = \text{rank}(AM_\varphi)$.

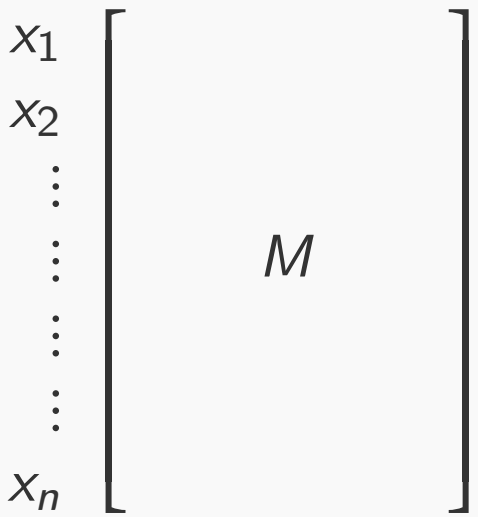
$$\begin{bmatrix} & A' & \end{bmatrix} \times \begin{bmatrix} & M_\varphi & \end{bmatrix} = \begin{bmatrix} & A'M_\varphi & \end{bmatrix}$$

Family of matrices or one matrix parameterised by s: $\left\{M_{\varphi(s)}\right\}_{s \in \mathcal{F}}$

A Good Map



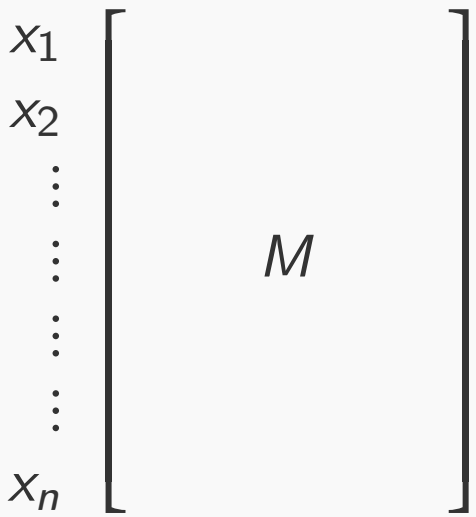
A Good Map



Binet-Cauchy:

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

A Good Map



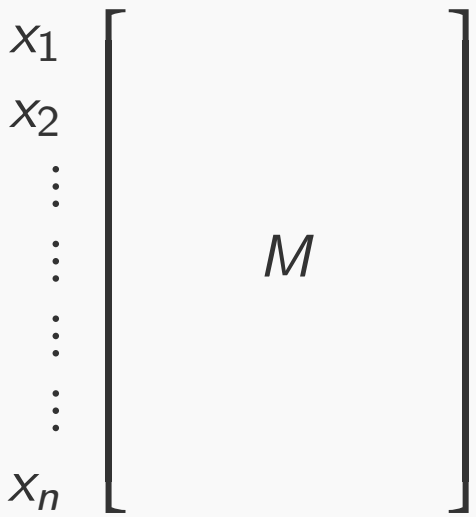
Binet-Cauchy:

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

Sufficient Properties

1. Every $k \times k$ minor is full rank.

A Good Map



Binet-Cauchy:

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

Sufficient Properties

1. Every $k \times k$ minor is full rank.
2. From among the Bs for which $\det(A_B) \neq 0$, there is a unique B for which the $\deg_s(\det(M_B))$ is maximum.

A Good Map

$$\begin{matrix} x_1 \\ x_2 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ x_n \end{matrix} \begin{bmatrix} s^{\mathrm{wt}(1)} \\ s^{\mathrm{wt}(2)} \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ s^{\mathrm{wt}(n)} \end{bmatrix}$$

Binet-Cauchy:

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

Sufficient Properties

1. Every $k \times k$ minor is full rank.
2. From among the Bs for which $\det(A_B) \neq 0$, there is a unique B for which the $\deg_s(\det(M_B))$ is maximum.

- Define $\mathrm{wt}(x_i)$ such that the weight of each row is distinct.

A Good Map

$$\begin{matrix} x_1 \\ x_2 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ x_n \end{matrix} \begin{bmatrix} s^{\mathrm{wt}(1)} \\ s^{\mathrm{wt}(2)} \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ s^{\mathrm{wt}(n)} \end{bmatrix}$$

Binet-Cauchy:

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

Sufficient Properties

1. Every $k \times k$ minor is full rank.
2. From among the Bs for which $\det(A_B) \neq 0$, there is a unique B for which the $\deg_s(\det(M_B))$ is maximum.

- Define $\mathrm{wt}(x_i)$ such that the weight of each row is distinct.
- Extend definition to sub-matrices cleverly such that $\mathrm{wt}(B) = \deg_s(\det(M_B))$.

A Good Map

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

Binet-Cauchy:

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

Sufficient Properties

1. Every $k \times k$ minor is full rank.
2. From among the Bs for which $\det(A_B) \neq 0$, there is a unique B for which the $\deg_s(\det(M_B))$ is maximum.

- Define $\mathrm{wt}(x_i)$ such that the weight of each row is distinct.
- Extend definition to sub-matrices cleverly such that $\mathrm{wt}(B) = \deg_s(\det(M_B))$.

A Good Map

[GR05]: Vandermonde type matrices are rank extractors.

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

Binet-Cauchy:

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

Sufficient Properties

1. Every $k \times k$ minor is full rank.
2. From among the Bs for which $\det(A_B) \neq 0$, there is a unique B for which the $\deg_s(\det(M_B))$ is maximum.

- Define $\mathrm{wt}(x_i)$ such that the weight of each row is distinct.
- Extend definition to sub-matrices cleverly such that $\mathrm{wt}(B) = \deg_s(\det(M_B))$.

A Good Map

[GR05]: Vandermonde type matrices are rank extractors.

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

Binet-Cauchy:

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

Sufficient Properties

1. Every $k \times k$ minor is full rank.
2. From among the Bs for which $\det(A_B) \neq 0$, there is a unique B for which the $\deg_s(\det(M_B))$ is maximum.

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

Failure of the Jacobian Criterion over Arbitrary fields

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

Failure of the Jacobian Criterion over Arbitrary fields

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

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

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

Failure of the Jacobian Criterion over Arbitrary fields

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

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

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

Reason: $(x, f_1, f_2) : A_x(\alpha, \beta, \gamma)$

Failure of the Jacobian Criterion over Arbitrary fields

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

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

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

Reason: $(x, f_1, f_2) : A_x(\alpha, \beta, \gamma)$ $\qquad$ $(y, f_1, f_2) : A_y(\alpha, \beta, \gamma)$

Failure of the Jacobian Criterion over Arbitrary fields

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

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

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

Reason: $(x, f_1, f_2) : A_x(\alpha, \beta, \gamma) \qquad (y, f_1, f_2) : A_y(\alpha, \beta, \gamma)$

$$\partial_\alpha(A_x) = 0 = \partial_\alpha(A_y)$$

Failure of the Jacobian Criterion over Arbitrary fields

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

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

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

Reason: $(x, f_1, f_2) : A_x(\alpha, \beta, \gamma) \qquad (y, f_1, f_2) : A_y(\alpha, \beta, \gamma)$

$$\partial_\alpha(A_x) = 0 = \partial_\alpha(A_y)$$

$$A_x(\alpha, \beta, \gamma) = A'_x(\alpha^{p^{k_1}}, \beta, \gamma), A_y(\alpha, \beta, \gamma) = A'_y(\alpha^{p^{k_2}}, \beta, \gamma)$$

Failure of the Jacobian Criterion over Arbitrary fields

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

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

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

Reason: $(x, f_1, f_2) : A_x(\alpha, \beta, \gamma) \qquad (y, f_1, f_2) : A_y(\alpha, \beta, \gamma)$

$$\partial_\alpha(A_x) = 0 = \partial_\alpha(A_y)$$

$$A_x(\alpha, \beta, \gamma) = A'_x(\alpha^{p^{k_1}}, \beta, \gamma), A_y(\alpha, \beta, \gamma) = A'_y(\alpha^{p^{k_2}}, \beta, \gamma)$$

For $k = \max\{k_1, k_2\}$, p^k : Inseparable degree of $\{f_1, f_2\}$.

Hasse derivatives

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

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

Hasse derivatives

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

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

For $f = x^p$, $f(x+z) - f(z) = x^p$ over $\mathbb{F}_p$.

Hasse derivatives

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

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

For $f = x^p$, $f(x+z) - f(z) = x^p$ over $\mathbb{F}_p$.

Consider Hasse Derivatives:

$$\partial^h_{x^p}(x^p) = \frac{1}{p!} \times p! = 1$$

Hasse derivatives

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

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

For $f = x^p$, $f(x+z) - f(z) = x^p$ over $\mathbb{F}_p$.

Consider Hasse Derivatives:

$$\partial^h_{x^p}(x^p) = \frac{1}{p!} \times p! = 1$$

In general, the Hasse derivative of f with respect to $\mathbf{x}^\mathbf{e}$ is the coefficient of $\mathbf{x}^\mathbf{e}$ in $f(\mathbf{x}+\mathbf{z}) - f(\mathbf{z})$.

The Criterion over Arbitrary fields

Definition: A new Operator

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

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

The Criterion over Arbitrary fields

Definition: 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 Criterion over Arbitrary fields

Definition: 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 [PSS16] 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 $\mathcal{I}_t$ is some fixed ideal of $\mathbb{F}(\mathbf{z})[x_1, x_2, \ldots, x_n]$.

Alternate Statement for the [PSS16] 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 $\mathcal{I}_t$,

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

What we want to show

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

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

What we want to show

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

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

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

has full rank for every $v_1, v_2, \dots, v_k \in \mathcal{I}_t$.

Constructing Good Maps over Arbitrary Fields

$$\varphi : x_i \to \sum_{j=1}^{k} s_{ij} y_j + a_i y_0 \text{ and } z_i \to \sum_{j=1}^{k} s_{ij} w_j + a_i w_0$$

Constructing Good Maps over Arbitrary Fields

$$\varphi : x_i \to \sum_{j=1}^{k} s_{ij} y_j + a_i y_0 \text{ and } z_i \to \sum_{j=1}^{k} s_{ij} w_j + a_i w_0$$

Sufficient Properties

1. For every $\mathbf{u}$, there is a $\mathbf{v}$ for which $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{u}) = \mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi))$

Constructing Good Maps over Arbitrary Fields

$$\varphi : x_i \to \sum_{j=1}^{k} s_{ij} y_j + a_i y_0 \text{ and } z_i \to \sum_{j=1}^{k} s_{ij} w_j + a_i w_0$$

Sufficient Properties

1. For every $\mathbf{u}$, there is a $\mathbf{v}$ for which $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{u}) = \mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi))$
2. $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi)) = \varphi(\mathcal{H}(\mathbf{f}, \mathbf{v})) \times M_\varphi$

Constructing Good Maps over Arbitrary Fields

$$\varphi : x_i \to \sum_{j=1}^{k} s_{ij} y_j + a_i y_0 \text{ and } z_i \to \sum_{j=1}^{k} s_{ij} w_j + a_i w_0$$

Sufficient Properties

1. For every $\mathbf{u}$, there is a $\mathbf{v}$ for which $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{u}) = \mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi))$
2. $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi)) = \varphi(\mathcal{H}(\mathbf{f}, \mathbf{v})) \times M_\varphi$
3. $\text{rank}(\varphi(\mathcal{H}(\mathbf{f}, \mathbf{v}))) = \text{rank}(\varphi(\mathcal{H}(\mathbf{f}, \mathbf{v})) \times M_\varphi)$

Constructing Good Maps over Arbitrary Fields

$$\varphi : x_i \to \sum_{j=1}^{k} s_{ij} y_j + a_i y_0 \text{ and } z_i \to \sum_{j=1}^{k} s_{ij} w_j + a_i w_0$$

Sufficient Properties

1. For every $\mathbf{u}$, there is a $\mathbf{v}$ for which $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{u}) = \mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi))$
2. $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi)) = \varphi(\mathcal{H}(\mathbf{f}, \mathbf{v})) \times M_\varphi$
3. $\text{rank}(\varphi(\mathcal{H}(\mathbf{f}, \mathbf{v}))) = \text{rank}(\varphi(\mathcal{H}(\mathbf{f}, \mathbf{v})) \times M_\varphi)$
4. $\text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})) = \text{rank}(\varphi(\mathcal{H}(\mathbf{f}, \mathbf{v})))$

M_φ preserves rank

$$\varphi : x_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} y_j + a_i y_0 \text{ and } z_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} w_j + a_i w_0$$

M_φ preserves rank

$$\varphi : x_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} y_j + a_i y_0 \text{ and } z_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} w_j + a_i w_0$$

$$\overbrace{\begin{bmatrix} \varphi(\mathcal{H}(\mathbf{f}, \mathbf{v})) \end{bmatrix}}^{\text{labelled by } \mathbf{x}^{\mathbf{e}}} \times \underbrace{\begin{bmatrix} M_\varphi \end{bmatrix}}_{\text{labelled by } \mathbf{y}^{\mathbf{d}}}$$

M_φ preserves rank

$$\varphi : x_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} y_j + a_i y_0 \text{ and } z_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} w_j + a_i w_0$$

$$\overbrace{\begin{bmatrix} \varphi(\mathcal{H}(\mathbf{f}, \mathbf{v})) \end{bmatrix}}^{\text{labelled by } \mathbf{x}^{\mathbf{e}}} \times \underbrace{\begin{bmatrix} M_\varphi \end{bmatrix}}_{\text{labelled by } \mathbf{y}^{\mathbf{d}}}$$

where

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

M_φ preserves rank

$$\varphi : x_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} y_j + a_i y_0 \text{ and } z_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} w_j + a_i w_0$$

$$\overbrace{\begin{bmatrix} \varphi(\mathcal{H}(\mathbf{f}, \mathbf{v})) \end{bmatrix}}^{\text{labelled by } \mathbf{x^e}} \times \underbrace{\begin{bmatrix} M_\varphi \end{bmatrix}}_{\text{labelled by } \mathbf{y^d}} : \text{Block Diagonal}$$

M_φ preserves rank

$$\varphi : x_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} y_j + a_i y_0 \text{ and } z_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} w_j + a_i w_0$$

$$\overbrace{\begin{bmatrix} \varphi(\mathcal{H}(\mathbf{f}, \mathbf{v})) \end{bmatrix}}^{\text{labelled by } \mathbf{x^e}} \times \underbrace{\begin{bmatrix} M_\varphi \end{bmatrix}}_{\text{labelled by } \mathbf{y^d}} : \text{Block Diagonal}$$

Goal: Make each block Vandermonde type.

M_φ preserves rank

$$\varphi : x_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} y_j + a_i y_0 \text{ and } z_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} w_j + a_i w_0$$

$$\overbrace{\begin{bmatrix} \varphi(\mathcal{H}(\mathbf{f}, \mathbf{v})) \end{bmatrix}}^{\text{labelled by } \mathbf{x^e}} \times \underbrace{\begin{bmatrix} M_\varphi \end{bmatrix}}_{\text{labelled by } \mathbf{y^d}} : \text{Block Diagonal}$$

Goal: Make each block Vandermonde type. Not true!!

M_φ preserves rank

$$\varphi : x_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} y_j + a_i y_0 \text{ and } z_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} w_j + a_i w_0$$

$$\overbrace{\begin{bmatrix} \varphi(\mathcal{H}(\mathbf{f}, \mathbf{v})) \end{bmatrix}}^{\text{labelled by } \mathbf{x}^{\mathbf{e}}} \times \underbrace{\begin{bmatrix} \tilde{M}_\varphi \end{bmatrix}}_{\text{labelled by } y_i^{d_i}}$$

M_φ preserves rank

$$\varphi : x_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} y_j + a_i y_0 \text{ and } z_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} w_j + a_i w_0$$

$$\overbrace{\begin{bmatrix} \varphi(\mathcal{H}(\mathbf{f}, \mathbf{v})) \end{bmatrix}}^{\text{labelled by } \mathbf{x}^{\mathbf{e}}} \times \underbrace{\begin{bmatrix} \tilde{M}_\varphi \end{bmatrix}}_{\text{labelled by } y_i^{d_i}}$$

$\mathrm{wt}(\mathbf{x}^{\mathbf{e}}) = \sum_{i=1}^{n} e_i \,\mathrm{wt}(i)$ is such that each $\mathbf{x}^{\mathbf{e}}$ gets a distinct weight.

M_φ preserves rank

$$\varphi : x_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} y_j + a_i y_0 \text{ and } z_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} w_j + a_i w_0$$

$$\overbrace{\left[\varphi(\mathcal{H}(\mathbf{f},\mathbf{v}))\right]}^{\text{labelled by } \mathbf{x}^{\mathbf{e}}} \times \underbrace{\left[\tilde{M}_\varphi\right]}_{\text{labelled by } y_i^{d_i}} : \text{Block Vandermonde type}$$

$\mathrm{wt}(\mathbf{x}^{\mathbf{e}}) = \sum_{i=1}^{n} e_i \,\mathrm{wt}(i)$ is such that each $\mathbf{x}^{\mathbf{e}}$ gets a distinct weight.

M_φ preserves rank

$$\varphi : x_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} y_j + a_i y_0 \text{ and } z_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} w_j + a_i w_0$$

unique minor with max. wt.

$$\begin{bmatrix} \varphi(\mathcal{H}(\mathbf{f}, \mathbf{v})) \end{bmatrix} \times \begin{bmatrix} \tilde{M}_\varphi \end{bmatrix}$$

$\mathrm{wt}(\mathbf{x}^{\mathbf{e}}) = \sum_{i=1}^{n} e_i \,\mathrm{wt}(i)$ is such that each $\mathbf{x}^{\mathbf{e}}$ gets a distinct weight.

Extend wt to sub-matrices cleverly.

M_φ preserves rank

$$\varphi : x_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} y_j + a_i y_0 \text{ and } z_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} w_j + a_i w_0$$

unique minor with max. wt.

$$\begin{bmatrix} \varphi(\mathcal{H}(\mathbf{f}, \mathbf{v})) \end{bmatrix} \times \begin{bmatrix} M'_\varphi \end{bmatrix}$$

$wt = \deg_s$

$\mathrm{wt}(\mathbf{x}^{\mathbf{e}}) = \sum_{i=1}^{n} e_i \,\mathrm{wt}(i)$ is such that each $\mathbf{x}^{\mathbf{e}}$ gets a distinct weight.

Extend wt to sub-matrices cleverly.

Choose a submatrix of M_φ cleverly

M_φ preserves rank

$$\varphi : x_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} y_j + a_i y_0 \text{ and } z_i \to \sum_{j=1}^{k} s^{\mathrm{wt}(i)j} w_j + a_i w_0$$

unique minor with max. wt.

$$\left[\varphi(\mathcal{H}(\mathbf{f}, \mathbf{v})) \right] \times \left[M'_\varphi \right]$$

$wt = \deg_s$

$\mathrm{wt}(\mathbf{x}^{\mathbf{e}}) = \sum_{i=1}^{n} e_i \,\mathrm{wt}(i)$ is such that each $\mathbf{x}^{\mathbf{e}}$ gets a distinct weight.

By Binet-Cauchy formula,

$$\det(\varphi(\mathcal{H}(\mathbf{f}, \mathbf{v})) \cdot M'_\varphi) \neq 0.$$

The Good Map

$$\varphi : x_i \to \sum_{j=1}^{k} s^{j(t+1)^i \bmod p} y_j + a_i \text{ and } z_i \to \sum_{j=1}^{k} s^{j(t+1)^i \bmod p} w_j + a_i.$$

where t is the inseparable degree.

The Good Map

$$\varphi : x_i \to \sum_{j=1}^{k} s^{j(t+1)^i \bmod p} y_j + a_i \text{ and } z_i \to \sum_{j=1}^{k} s^{j(t+1)^i \bmod p} w_j + a_i.$$

where t is the inseparable degree.

Properties

1. For every $\mathbf{u}$, there is a $\mathbf{v}$ for which $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{u}) = \mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi))$

The Good Map

$$\varphi : x_i \to \sum_{j=1}^{k} s^{j(t+1)^i \bmod p} y_j + a_i \text{ and } z_i \to \sum_{j=1}^{k} s^{j(t+1)^i \bmod p} w_j + a_i.$$

where t is the inseparable degree.

Properties

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

The Good Map

$$\varphi : x_i \to \sum_{j=1}^{k} s^{j(t+1)^i \bmod p} y_j + a_i \text{ and } z_i \to \sum_{j=1}^{k} s^{j(t+1)^i \bmod p} w_j + a_i.$$

where t is the inseparable degree.

Properties

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

The Good Map

$$\varphi : x_i \to \sum_{j=1}^{k} s^{j(t+1)^i \bmod p} y_j + a_i \text{ and } z_i \to \sum_{j=1}^{k} s^{j(t+1)^i \bmod p} w_j + a_i.$$

where t is the inseparable degree.

Properties

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

The Good Map

$$\varphi : x_i \to \sum_{j=1}^{k} s^{j(t+1)^i \bmod p} y_j + a_i \text{ and } z_i \to \sum_{j=1}^{k} s^{j(t+1)^i \bmod p} w_j + a_i.$$

where t is the inseparable degree.

Properties

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

Size bounds: $p = O(n^{3t})$, $s = O(p)$.

The Good Map

$$\varphi : x_i \to \sum_{j=1}^{k} s^{j(t+1)^i \bmod p} y_j + a_i \text{ and } z_i \to \sum_{j=1}^{k} s^{j(t+1)^i \bmod p} w_j + a_i.$$

where t is the inseparable degree.

Properties

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

Size bounds: $p = O(n^{3t})$, $s = O(p)$.

Choice of a: Depends on the model under consideration.

Applications to PIT

Concept of faithful maps used to solve PIT in following settings:

1. $\mathcal{C}(f_1, f_2, \ldots, f_m)$, where f_i are sparse polynomials.
2. Depth-4 multi-linear circuits with bounded top fan-in.

Applications to PIT

Concept of faithful maps used to solve PIT in following settings:

1. $\mathcal{C}(f_1, f_2, \ldots, f_m)$, where f_i are sparse polynomials.
2. Depth-4 multi-linear circuits with bounded top fan-in.

More to come....

Applications to PIT

Concept of faithful maps used to solve PIT in following settings:

1. $\mathcal{C}(f_1, f_2, \ldots, f_m)$, where f_i are sparse polynomials.
2. Depth-4 multi-linear circuits with bounded top fan-in.

More to come.... hopefully!! :)

Applications to PIT

Concept of faithful maps used to solve PIT in following settings:

1. $\mathcal{C}(f_1, f_2, \ldots, f_m)$, where f_i are sparse polynomials.
2. Depth-4 multi-linear circuits with bounded top fan-in.

More to come.... hopefully!! :)

Thank you!!

References I

Manindra Agrawal, Chandan Saha, Ramprasad Saptharishi, and Nitin Saxena.
Jacobian hits circuits: hitting-sets, lower bounds for depth-d occur-k formulas & depth-3 transcendence degree-k circuits.
In *Proceedings of the 44th Symposium on Theory of Computing Conference, STOC 2012, New York, NY, USA, May 19 - 22, 2012*, pages 599–614, 2012.

Malte Beecken, Johannes Mittmann, and Nitin Saxena.
Algebraic independence and blackbox identity testing.
CoRR, abs/1102.2789, 2011.

Ariel Gabizon and Ran Raz.
Deterministic extractors for affine sources over large fields.
In *46th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2005), 23-25 October 2005, Pittsburgh, PA, USA, Proceedings*, pages 407–418, 2005.

References II

Anurag Pandey, Nitin Saxena, and Amit Sinhababu.
Algebraic independence over positive characteristic: New criterion and applications to locally low algebraic rank circuits.
In *41st International Symposium on Mathematical Foundations of Computer Science, MFCS 2016, August 22-26, 2016 - Kraków, Poland*, pages 74:1–74:15, 2016.