Constructing Faithful Maps over Arbitrary Fields

Prerona Chatterjee

joint work with

Ramprasad Saptharishi

WACT 2018

March 8, 2018

Algebraic Independence

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.

Algebraic Independence

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.

Algebraic Independence

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.

Algebraic Independence

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.

Question: Can we test algebraic independence efficiently?

Checking Algebraic Independence

Working with Annihilating Polynomials [Kay09, GSS18]

Checking whether the constant term of all the annihilating polynomials is zero is NP-hard.

Checking Algebraic Independence

Working with Annihilating Polynomials [Kay09, GSS18]

Checking whether the constant term of all the annihilating polynomials is zero is NP-hard.

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

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

Checking Algebraic Independence

Working with Annihilating Polynomials [Kay09, GSS18]

Checking whether the constant term of all the annihilating polynomials is zero is NP-hard.

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

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

The Jacobian Criterion [Jac41]

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

Rank Preserving Maps

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.

Rank Preserving Maps

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

Rank Preserving Maps

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

Question: Can we construct faithful maps efficiently?

Rank Preserving Maps

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

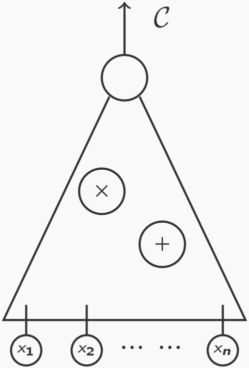
$$\varphi : \{x_1, x_2, \ldots, x_n\} \to \mathbb{F}[y_1, y_2, \ldots, y_k]$$

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

Question: Can we construct faithful maps efficiently?

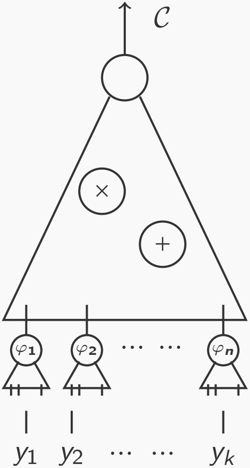
Bonus: Helps in polynomial identity testing.

Faithful Maps and Poly. Identity Testing [BMS11, ASSS12]



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

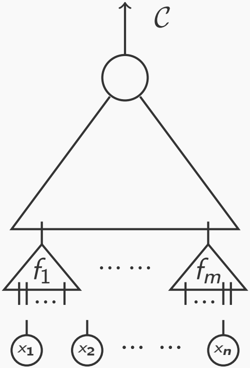
Faithful Maps and Poly. Identity Testing [BMS11, ASSS12]



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

PIT ≡ Variable substitution preserving non-zeroness

Faithful Maps and Poly. Identity Testing [BMS11, ASSS12]

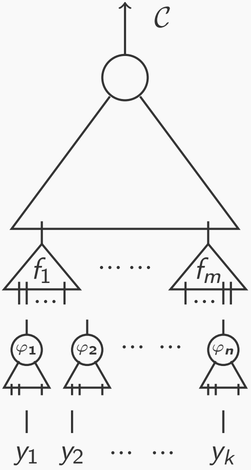


Check whether $\mathcal{C}$ computes the zero polynomial or not.

PIT ≡ Variable substitution preserving non-zeroness

$\mathcal{C} \equiv \mathcal{C}(f_1, f_2, \ldots, f_m)$: algebraic rank k

Faithful Maps and Poly. Identity Testing [BMS11, ASSS12]



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

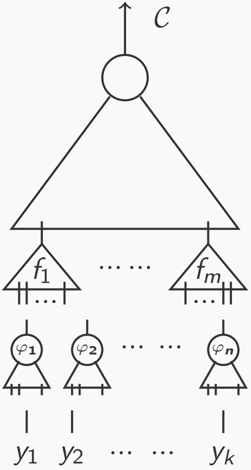
PIT ≡ Variable substitution preserving non-zeroness

$\mathcal{C} \equiv \mathcal{C}(f_1, f_2, \ldots, f_m)$: algebraic rank k

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

is a faithful map.

Faithful Maps and Poly. Identity Testing [BMS11, ASSS12]



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

PIT $\equiv$ Variable substitution preserving non-zeroness

$\mathcal{C} \equiv \mathcal{C}(f_1, f_2, \ldots, f_m)$: algebraic rank k

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

is a faithful map.

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

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

A Quick Survey

[Jac41]: Gave a criterion for checking Algebraic Independence over Characteristic zero fields.

A Quick Survey

[Jac41]: Gave a criterion for checking Algebraic Independence over Characteristic zero fields.

[BMS11]: Introduced the problem and the concept of faithful maps. Applied faithful maps to solve PIT when $f_1, f_2, \ldots, f_m$ are sparse.

A Quick Survey

[Jac41]: Gave a criterion for checking Algebraic Independence over Characteristic zero fields.

[BMS11]: Introduced the problem and the concept of faithful maps. Applied faithful maps to solve PIT when $f_1, f_2, \ldots, f_m$ are sparse.

[ASSS12]: Extended these techniques to a variety of other models.

A Quick Survey

[Jac41]: Gave a criterion for checking Algebraic Independence over Characteristic zero fields.

[BMS11]: Introduced the problem and the concept of faithful maps. Applied faithful maps to solve PIT when $f_1, f_2, \ldots, f_m$ are sparse.

[ASSS12]: Extended these techniques to a variety of other models.

[PSS16]: Gave a criterion for checking Algebraic Independence over arbitrary fields.

A Quick Survey

[Jac41]: Gave a criterion for checking Algebraic Independence over Characteristic zero fields.

[BMS11]: Introduced the problem and the concept of faithful maps. Applied faithful maps to solve PIT when $f_1, f_2, \ldots, f_m$ are sparse.

[ASSS12]: Extended these techniques to a variety of other models.

[PSS16]: Gave a criterion for checking Algebraic Independence over arbitrary fields.

This work: Construct Faithful Maps over arbitrary fields and extend results in [ASSS12] to other fields.

Constructing Faithful Maps over Characteristic Zero Fields

Fact: A random affine transformation is a faithful map

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

Constructing Faithful Maps over Characteristic Zero Fields

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?

Constructing Faithful Maps over Characteristic Zero Fields

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

$$\left[\quad \mathbf{J}_{\mathbf{y}}(\mathbf{f}(\varphi)) \quad \right]$$

Constructing Faithful Maps over Characteristic Zero Fields

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

$$\left[\quad \mathbf{J}_{\mathbf{y}}(\mathbf{f}(\varphi)) \quad \right] = \left[\quad \varphi(\mathbf{J}_{\mathbf{x}}(\mathbf{f})) \quad \right] \times \left[\quad M_{\varphi} \quad \right]$$

Constructing Faithful 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 Faithful 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. $\text{rank}(\mathbf{J_x}(\mathbf{f})) = \text{rank}(\varphi(\mathbf{J_x}(\mathbf{f})))$: a_is are responsible for this

Constructing Faithful Maps over Characteristic Zero Fields

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

$$\left[\quad \mathbf{J_y}(\mathbf{f}(\varphi)) \quad \right] = \left[\quad \varphi(\mathbf{J_x}(\mathbf{f})) \quad \right] \times \left[\quad M_\varphi \quad \right]$$

What we need: φ such that

1. $\text{rank}(\mathbf{J_x}(\mathbf{f})) = \text{rank}(\varphi(\mathbf{J_x}(\mathbf{f})))$: a_is are responsible for this
2. M_φ preserves rank

A Rank Preserving Matrix and a Faithful Map [BMS11]

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

Chain Rule $\Rightarrow M_\varphi[i, j] = s_{ij}$

A Rank Preserving Matrix and a Faithful Map [BMS11]

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

Chain Rule $\Rightarrow M_\varphi[i, j] = s_{ij}$

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

A Rank Preserving Matrix and a Faithful Map [BMS11]

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

Chain Rule $\Rightarrow M_\varphi[i,j] = s_{ij}$

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

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

A Rank Preserving Matrix and a Faithful Map [BMS11]

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

Chain Rule $\Rightarrow M_\varphi[i,j] = s_{ij}$

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

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

[GR05]: Vandermonde type matrices preserve rank.

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

A Rank Preserving Matrix and a Faithful Map [BMS11]

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

Chain Rule $\Rightarrow M_\varphi[i,j] = s_{ij}$

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

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

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

[GR05]: Vandermonde type matrices preserve rank.

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

What 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.

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

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

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

Characteristic Zero: $\mathbf{J}$ has full rank $\Leftarrow$ $\mathbf{J}$ 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.

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

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

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

Characteristic Zero: $\mathbf{J}$ has full rank $\Leftarrow$ $\mathbf{J}$ has an inverse

Finite Characteristic: Entries in "inverse" have denominators that are partial derivatives of some annihilators, which can become zero.

Looking Further in the Taylor Expansion [PSS16]

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

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

Looking Further in the Taylor Expansion [PSS16]

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

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

[PSS16]: Look at Taylor expansions up to the "inseparable degree".

Looking Further in the Taylor Expansion [PSS16]

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

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

[PSS16]: Look at Taylor expansions up to the "inseparable degree".

Definition: A new Operator

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

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

Looking Further in the Taylor Expansion [PSS16]

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

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

[PSS16]: Look at Taylor expansions up to the "inseparable degree".

Definition: A new Operator

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

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

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

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

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

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

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

The Goal

What we know:

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

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

The Goal

What we know:

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

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

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 $u_1, u_2, \dots, u_k \in \mathcal{I}_t(\varphi)$

Constructing Faithful 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 Faithful 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 Faithful 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. $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi)) = \varphi(\mathcal{H}(\mathbf{f}, \mathbf{v})) \times M_\varphi$: Chain Rule

Constructing Faithful 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. $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi)) = \varphi(\mathcal{H}(\mathbf{f}, \mathbf{v})) \times M_\varphi$: Chain Rule
3. $\text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})) = \text{rank}(\varphi(\mathcal{H}(\mathbf{f}, \mathbf{v})))$: a_is are responsible for this

Constructing Faithful 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. $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi)) = \varphi(\mathcal{H}(\mathbf{f}, \mathbf{v})) \times M_\varphi$: Chain Rule
3. $\text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})) = \text{rank}(\varphi(\mathcal{H}(\mathbf{f}, \mathbf{v})))$: a_is are responsible for this
4. M_φ preserves rank

The Matrix Decomposition

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

The Matrix Decomposition

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

where

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

What makes Vandermonde type matrices work?

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

What makes Vandermonde type matrices work?

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

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

What makes Vandermonde type matrices work?

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

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

What makes Vandermonde type matrices work?

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

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

What makes Vandermonde type matrices work?

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

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

What makes Vandermonde type matrices work?

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

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

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

What makes Vandermonde type matrices work?

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

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

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

What makes Vandermonde type matrices work?

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

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

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

What makes Vandermonde type matrices work?

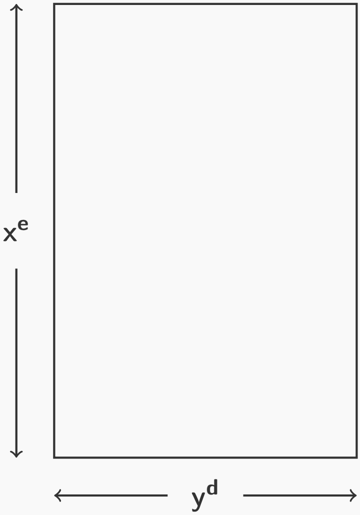
Cauchy-Binet: $\det(AM) = \sum_{B \subseteq \{x_i\},\ |B|=k} \det(A_B)\det(M_B)$.

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

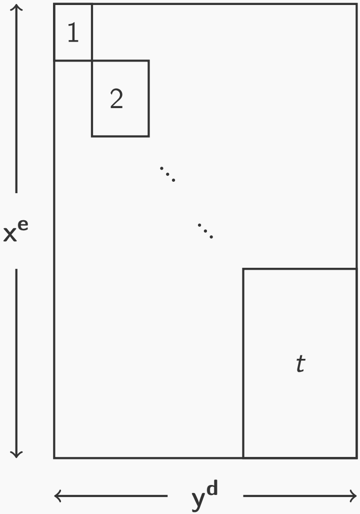
$\mathrm{wt}(x_i)$ is distinct for each i

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

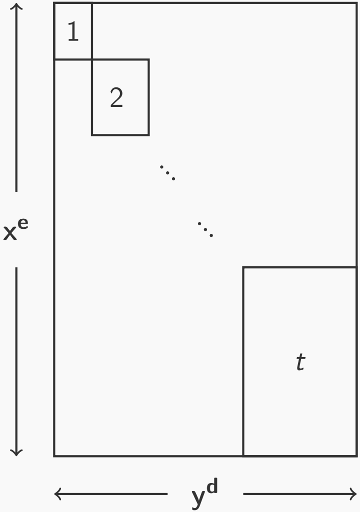
The Current Matrix



The Current Matrix

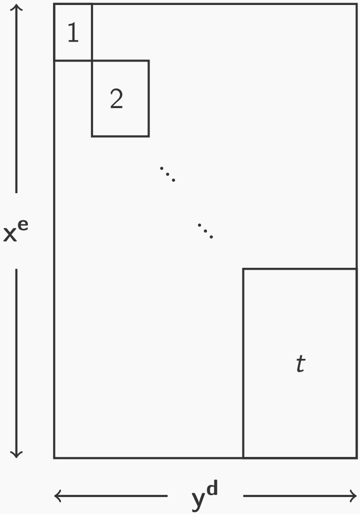


The Current Matrix



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

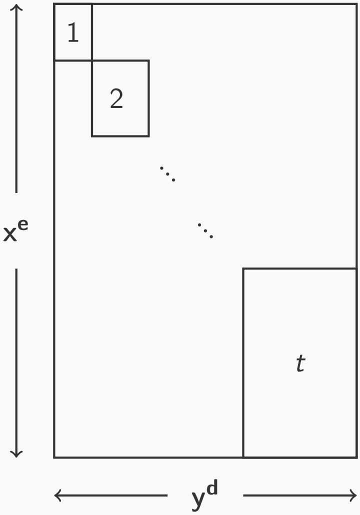
The Current Matrix



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

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

The Current Matrix

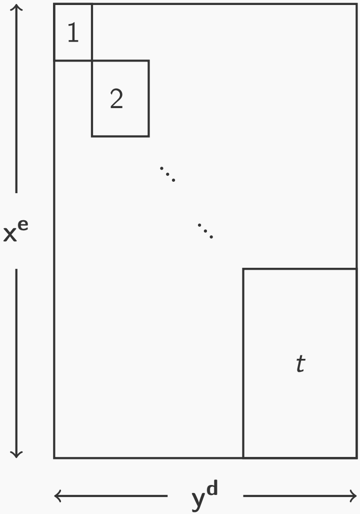


$$M_\varphi(\mathbf{x}^{\mathbf{e}}, \mathbf{y}^{\mathbf{d}}) = \mathrm{coeff}_{\mathbf{y}^{\mathbf{d}}}(\varphi(\mathbf{x}^{\mathbf{e}}))$$

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

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

The Current Matrix



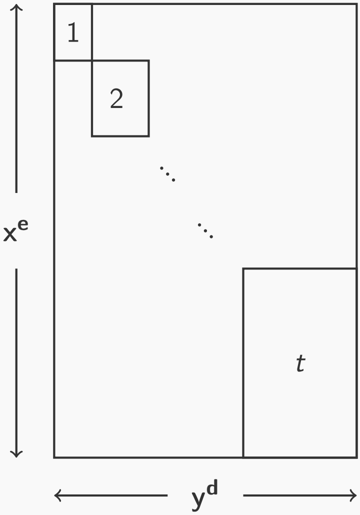
$$M_\varphi(\mathbf{x^e}, \mathbf{y^d}) = \text{coeff}_{\mathbf{y^d}}(\varphi(\mathbf{x^e}))$$

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

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

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

The Current Matrix



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

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

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

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

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

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

A Rank Preserving Matrix

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

A Rank Preserving Matrix

$$\overset{\uparrow}{\underset{\downarrow}{k}} \begin{bmatrix} \quad & A & \quad \end{bmatrix} \times \underbrace{\begin{bmatrix} \\ \quad & M & \quad \\ \\ \end{bmatrix}}_{\longleftarrow \; > k \; \longrightarrow} = \begin{bmatrix} \quad & AM & \quad \end{bmatrix}$$

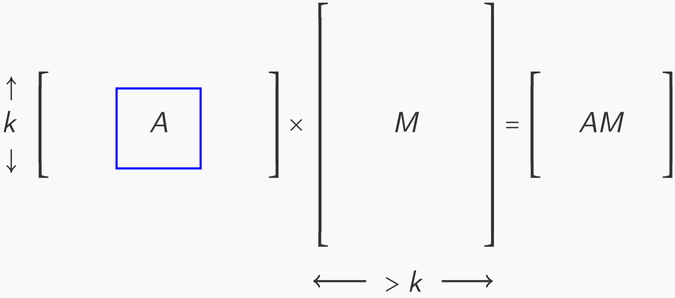
A Rank Preserving Matrix

$$k \left[\quad A \quad \right] \times \left[\quad M \quad \right] = \left[\quad AM \quad \right]$$

$$\longleftarrow \; > k \; \longrightarrow$$

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

A Rank Preserving Matrix

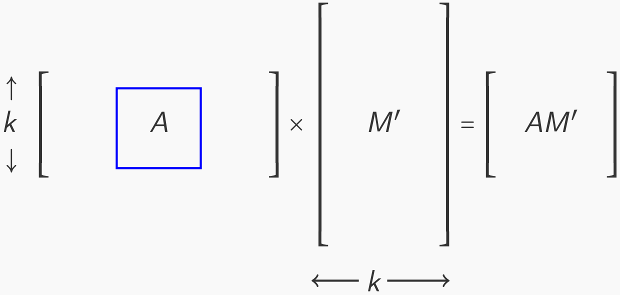


What we want: k columns of AM that are linearly independent.

Proof Strategy:

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

A Rank Preserving Matrix



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

Proof Strategy:

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

A few details

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

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

A few details

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

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

About wt:

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

A few details

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

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

About wt:

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

About M'

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

A Faithful Map over Arbitrary Fields

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

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

A Faithful Map over Arbitrary Fields

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

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

Properties

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

A Faithful Map over Arbitrary Fields

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

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

Properties

1. For every $\mathbf{u}$, 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 $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi))$

A Faithful Map over Arbitrary Fields

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

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

Properties

1. For every $\mathbf{u}$, 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. $\mathrm{rank}(\varphi(\mathcal{H}(\mathbf{f}, \mathbf{v}))) = \mathrm{rank}(\varphi(\mathcal{H}(\mathbf{f}, \mathbf{v})) \times M_\varphi)$

A Faithful Map over Arbitrary Fields

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

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

Properties

1. For every $\mathbf{u}$, 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. $\mathrm{rank}(\varphi(\mathcal{H}(\mathbf{f}, \mathbf{v}))) = \mathrm{rank}(\varphi(\mathcal{H}(\mathbf{f}, \mathbf{v})) \times M_\varphi)$
4. $\mathrm{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})) = \mathrm{rank}(\varphi(\mathcal{H}(\mathbf{f}, \mathbf{v})))$

An Instantiation

Theorem

Let $f_1, f_2, \ldots, f_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ *be s-sparse polynomials such that* $\text{algrank}(f_1, f_2, \ldots, f_m) = k$ *and the inseparable degree is* t*.*
If t *and* k *are bounded by a constant, then, there is an explicit deterministic construction of a faithful homomorphisms in* $\text{poly}(n, m, s)$ *time.*

An Instantiation

Theorem

Let $f_1, f_2, \ldots, f_m \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ be s-sparse polynomials such that $\text{algrank}(f_1, f_2, \ldots, f_m) = k$ and the inseparable degree is t. If t and k are bounded by a constant, then, there is an explicit deterministic construction of a faithful homomorphisms in $\text{poly}(n, m, s)$ time.

Explicit faithful homomorphisms can also be constructed efficiently for other models studied in [ASSS12] when we have similar inseparable degree bounds.

Open Threads

1. Improve the dependence on "inseparable degree".

Open Threads

1. Improve the dependence on "inseparable degree".

2. [GSS18]: 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. [GSS18]: Different characterisation for Algebraic dependence - not algorithmic but has no dependence on "inseparable degree"

   Can we get PIT applications out of it?

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.
In *Automata, Languages and Programming - 38th International Colloquium, ICALP 2011, Zurich, Switzerland, July 4-8, 2011, Proceedings, Part II*, pages 137–148, 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

Zeyu Guo, Nitin Saxena, and Amit Sinhababu.
Algebraic dependencies and PSPACE algorithms in approximative complexity.
CoRR, abs/1801.09275, 2018.

C.G.J. Jacobi.
De determinantibus functionalibus.
Journal für die reine und angewandte Mathematik, 22:319–359, 1841.

Neeraj Kayal.
The complexity of the annihilating polynomial.
In *Proceedings of the 24th Annual IEEE Conference on Computational Complexity, CCC 2009, Paris, France, 15-18 July 2009*, pages 184–193, 2009.

References III

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.