Towards Algebraic Independence based PITs over Arbitrary fields

Prerona Chatterjee

TIFR, Mumbai

December 08, 2017

A little about 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.

A little about 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,

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

A little about 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,

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

- [Kay09] The minimal "annihilating polynomial" is "hard".

Checking Algebraic Independence efficiently

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 efficiently

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

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

The Jacobian Criterion

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

How it helps in solving PITs

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.

How it helps in solving PITs

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 PIT Question: Given a circuit $\mathcal{C}$, check whether it computes the identically zero polynomial.

How it helps in solving PITs

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 PIT Question: Given a circuit $\mathcal{C}$, check whether it computes the identically zero polynomial.

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

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

The Strategy

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

The Strategy

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

$$\left[\quad \mathbf{J_y}(\mathbf{f}(\varphi)) \quad \right]$$

The Strategy

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

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

The Strategy

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

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

What we need: φ such that

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

The Strategy

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

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

What we need: φ such that

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

The Strategy

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

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

What we need: φ such that

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

Rank Extractors

Definition: Rank Extractors

An n-rowed matrix M is said to be a rank extractor if for every $m \times n$ matrix A, $\text{rank}(A) = \text{rank}(AM)$.

Rank Extractors

Definition: Rank Extractors

An n-rowed matrix M is said to be a rank extractor if for every $m \times n$ matrix A, $\text{rank}(A) = \text{rank}(AM)$.

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

Rank Extractors

Definition: Rank Extractors

An n-rowed matrix M is said to be a rank extractor if for every $m \times n$ matrix A, $\text{rank}(A) = \text{rank}(AM)$.

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

Rank Extractors

Definition: Rank Extractors

An n-rowed matrix M is said to be a rank extractor if for every $m \times n$ matrix A, $\text{rank}(A) = \text{rank}(AM)$.

$$\begin{bmatrix} \quad A' \quad \end{bmatrix} \times \begin{bmatrix} \\ M_s \\ \\ \end{bmatrix} = \begin{bmatrix} A' M_s \end{bmatrix}$$

A Faithful map

$$\begin{matrix} x_1 \\ x_2 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ x_n \end{matrix} \begin{bmatrix} & & \\ & M & \\ & & \end{bmatrix}$$

A Faithful map

$$\begin{matrix} x_1 \\ x_2 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ x_n \end{matrix} \left[\begin{matrix} \\ \\ \quad M \quad \\ \\ \\ \end{matrix} \right]$$

Binet-Cauchy:

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

A Faithful map

$$\begin{matrix} x_1 \\ x_2 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ x_n \end{matrix} \begin{bmatrix} \\ \\ \\ \quad M \quad \\ \\ \\ \\ \end{bmatrix}$$

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.

A Faithful map

$$\begin{matrix} x_1 \\ x_2 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ x_n \end{matrix} \begin{bmatrix} & & \\ & M & \\ & & \end{bmatrix}$$

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.

A Faithful map

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

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 minors cleverly: $\mathrm{wt}(B) = \deg_s(\det(M_B))$.

A Faithful 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 minors cleverly: $\mathrm{wt}(B) = \deg_s(\det(M_B))$.

A Faithful 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 minors cleverly: $\mathrm{wt}(B) = \deg_s(\det(M_B))$.

A Faithful 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.

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

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

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

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

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

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

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

The Criterion over Arbitrary fields

Definition: A new Operator

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

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

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

The [PSS16] Criterion

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

$\{f_1, f_2, \ldots, f_m\}$ 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

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

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

What we want to show

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

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 $v_1, v_2, \dots, v_k \in \mathcal{I}_t$.

The Strategy

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

The Strategy

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

Sufficient Properties

1. Every u must have a v

The Strategy

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

Sufficient Properties

1. **Every u must have a v:** There is a natural pre-image.

The Strategy

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

Sufficient Properties

1. **Every u must have a v:** There is a natural pre-image.
2. $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi)) = \mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi} \times M_{\varphi}$

The Strategy

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

Sufficient Properties

1. **Every u must have a v:** There is a natural pre-image.
2. $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi)) = \mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi} \times M_{\varphi}$: True in general.

The Strategy

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

Sufficient Properties

1. **Every u must have a v:** There is a natural pre-image.
2. $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi)) = \mathcal{H}(\mathbf{f}, \mathbf{v})|_\varphi \times M_\varphi$: True in general.

$$\left[\quad \mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi)) \quad \right] = \left[\quad \mathcal{H}(\mathbf{f}, \mathbf{v})|_\varphi \quad \right] \times \left[\quad M_\varphi \quad \right]$$

The Strategy

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

Sufficient Properties

1. $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{u}) = \mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi))$ for some appropriate $\mathbf{v}$.
2. $\mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi} \times M_{\varphi}$ is a sub-matrix of $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi))$
3. $\text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi}) = \text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi} \times M_{\varphi})$

The Strategy

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

Sufficient Properties

1. $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{u}) = \mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi))$ for some appropriate $\mathbf{v}$.
2. $\mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi} \times M_{\varphi}$ is a sub-matrix of $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi))$
3. $\text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi}) = \text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi} \times M_{\varphi})$:

$$\underbrace{\begin{bmatrix} \\ M_{\varphi} \\ \\ \end{bmatrix}}_{\text{labelled by monomials of degree up to } t \text{ in } \mathbf{y}}$$

The Strategy

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

Sufficient Properties

1. $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{u}) = \mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi))$ for some appropriate $\mathbf{v}$.
2. $\mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi} \times M_{\varphi}$ is a sub-matrix of $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi))$
3. $\text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi}) = \text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi} \times M_{\varphi}) \; : \; \text{wt}(x_i) = i$

$$\underbrace{\begin{bmatrix} \\ M_{\varphi} \\ \\ \end{bmatrix}}_{\text{labelled by monomials of degree up to } t \text{ in } \mathbf{y}}$$

Not Block Vandermonde type

The Strategy

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

Sufficient Properties

1. $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{u}) = \mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi))$ for some appropriate $\mathbf{v}$.
2. $\mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi} \times M_{\varphi}$ is a sub-matrix of $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi))$
3. $\text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi}) = \text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi} \times M_{\varphi})$: $\text{wt}(x_i) = (t+1)^i$

$$\underbrace{\begin{bmatrix} \\ M_{\varphi} \\ \\ \end{bmatrix}}$$

Block Vandermonde type

labelled by "pure" monomials of degree up to t in $\mathbf{y}$

The Strategy

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

Properties

1. $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{u}) = \mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi))$ for some appropriate $\mathbf{v}$.
2. $\mathcal{H}(\mathbf{f}, \mathbf{v})|_\varphi \times M_\varphi$ is a sub-matrix of $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi))$
3. $\text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})|_\varphi) = \text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})|_\varphi \times M_\varphi) \ : \ \text{wt}(x_i) = (t+1)^i$

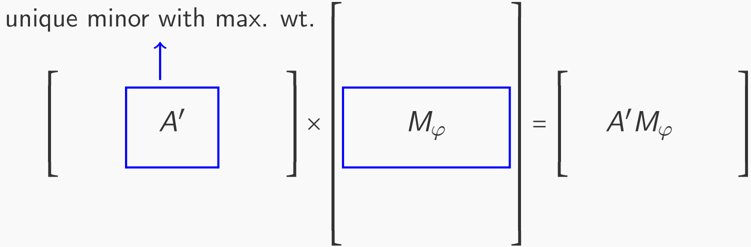
$$\overbrace{\begin{bmatrix} \quad A' \quad \end{bmatrix}}^{\text{labelled by } \mathbf{x}^{\mathbf{e}}} \times \begin{bmatrix} \quad M_\varphi \quad \end{bmatrix} = \begin{bmatrix} \quad A' M_\varphi \quad \end{bmatrix}$$

The Strategy

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

Properties

1. $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{u}) = \mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi))$ for some appropriate $\mathbf{v}$.
2. $\mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi} \times M_{\varphi}$ is a sub-matrix of $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi))$
3. $\text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi}) = \text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi} \times M_{\varphi}) \;:\; \text{wt}(x_i) = (t+1)^i$

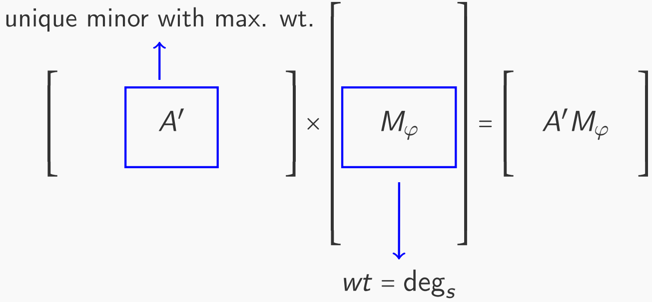


The Strategy

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

Properties

1. $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{u}) = \mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi))$ for some appropriate $\mathbf{v}$.
2. $\mathcal{H}(\mathbf{f}, \mathbf{v})|_\varphi \times M_\varphi$ is a sub-matrix of $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi))$
3. $\text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})|_\varphi) = \text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})|_\varphi \times M_\varphi)$: $\text{wt}(x_i) = (t+1)^i$



The Strategy

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

where t is the inseparable degree.

Properties

1. $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{u}) = \mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi))$ for some appropriate $\mathbf{v}$.
2. $\mathcal{H}(\mathbf{f}, \mathbf{v})|_\varphi \times M_\varphi$ is a sub-matrix of $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi))$
3. $\text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})|_\varphi) = \text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})|_\varphi \times M_\varphi)$
4. $\text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})) = \text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})|_\varphi)$

The Strategy

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

where t is the inseparable degree.

Properties

1. $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{u}) = \mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi))$ for some appropriate $\mathbf{v}$.
2. $\mathcal{H}(\mathbf{f}, \mathbf{v})|_\varphi \times M_\varphi$ is a sub-matrix of $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi))$
3. $\text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})|_\varphi) = \text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})|_\varphi \times M_\varphi)$
4. $\text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})) = \text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})|_\varphi)$: Can be handled by choosing the a_is correctly

The Map

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

where t is the inseparable degree.

The 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. $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{u}) = \mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi))$ for some appropriate $\mathbf{v}$.
2. $\mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi} \times M_{\varphi}$ is a sub-matrix of $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi))$.
3. $\text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi}) = \text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi} \times M_{\varphi})$.
4. $\text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})) = \text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi})$.

The 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. $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{u}) = \mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi))$ for some appropriate $\mathbf{v}$.
2. $\mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi} \times M_{\varphi}$ is a sub-matrix of $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi))$.
3. $\text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi}) = \text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi} \times M_{\varphi})$.
4. $\text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})) = \text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi})$.

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

The 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. $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{u}) = \mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi))$ for some appropriate $\mathbf{v}$.
2. $\mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi} \times M_{\varphi}$ is a sub-matrix of $\mathcal{H}(\mathbf{f}(\varphi), \mathbf{v}(\varphi))$.
3. $\text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi}) = \text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi} \times M_{\varphi})$.
4. $\text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})) = \text{rank}(\mathcal{H}(\mathbf{f}, \mathbf{v})|_{\varphi})$.

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

Choice of $\mathbf{a}$: Depends on the model under consideration.

An Application

Theorem: Extension of [BMS11]

If $\{f_1, f_2, \ldots, f_m\} \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ is a set of sparse polynomials with transcendence degree k and inseparable degree t, then there is a $n^{\text{poly}(k,t)}$ time PIT for circuits of the type $\mathcal{C}(f_1, f_2, \ldots, f_m)$.

Thus if k, t were constant, we have a poly(n)-time PIT.

An Application

Theorem: Extension of [BMS11]

If $\{f_1, f_2, \ldots, f_m\} \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ is a set of sparse polynomials with transcendence degree k and inseparable degree t, then there is a $n^{\text{poly}(k,t)}$ time PIT for circuits of the type $\mathcal{C}(f_1, f_2, \ldots, f_m)$.

Thus if k, t were constant, we have a poly(n)-time PIT.

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

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.

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.