Deterministic identity testing paradigms for bounded top-fanin depth-4 circuits

Pranjal Dutta (NUS and Oxford), Prateek Dwivedi (IIT K), Nitin Saxena (IIT K)

Polynomial Identity Testing

- Blackbox
  - Quasi-poly time PIT for $\Sigma^{[O(1)]}\Pi\Sigma\Pi^{[O(1)]}$ and $\Sigma^{[O(1)]}\Pi\Sigma\wedge$ circuits.
- Whitebox
  - Poly time PIT for $\Sigma^{[O(1)]}\Pi\Sigma\wedge$ circuits.

Prelude

Natural Queries

Given a polynomial f,

- Evaluate it at $x_1 = a_1, \dots, x_n = a_n$.
- For some polynomial g, compute $f + g$ and $f \times g$.
- Find the factors of f.
- For some polynomial g, test $\mathrm{g} = \mathrm{f}$.

Identity Testing

For some polynomial g, test $\mathbf{g} = \mathrm{f}$.

$$f = \sum \alpha_{\bar{e}} \cdot \prod_{j\in[n]} x_j^{e_j}$$

$$g = \sum \beta_{\bar{e}} \cdot \prod_{j\in[n]} x_j^{e_j}$$

- Same coefficients, $\alpha_{\bar{e}} = \beta_{\bar{e}}$?
- Alternatively, check if all coefficients are zero in $f - g$.

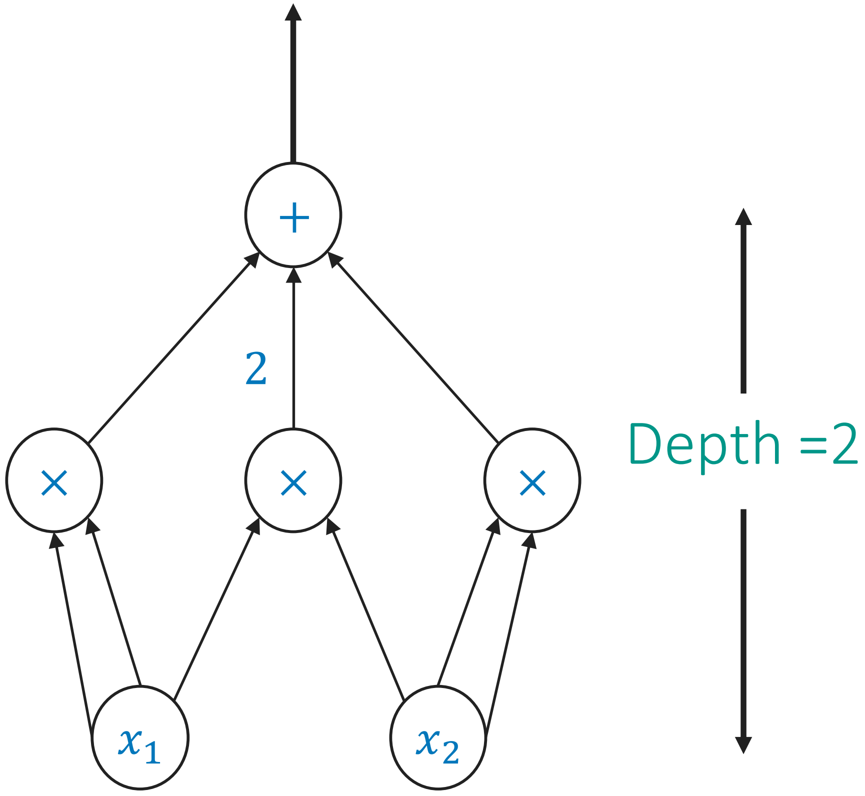
That's simple, but not efficient.

Number of coefficients $= \binom{n+d}{d} \approx \mathrm{EXP}(n, d)$.

Representing Multivariate Polynomials

- Algebraic Circuits
  - Intuitive. Succinct.
  - Operations are easy.
  - Most algebraic problems naturally fit into the framework.

$\mathbb{F}[x_1, x_2] \ni \ f_1 = x_1^2 + x_2^2 + 2x_1x_2$



Size = Number of gates = 4

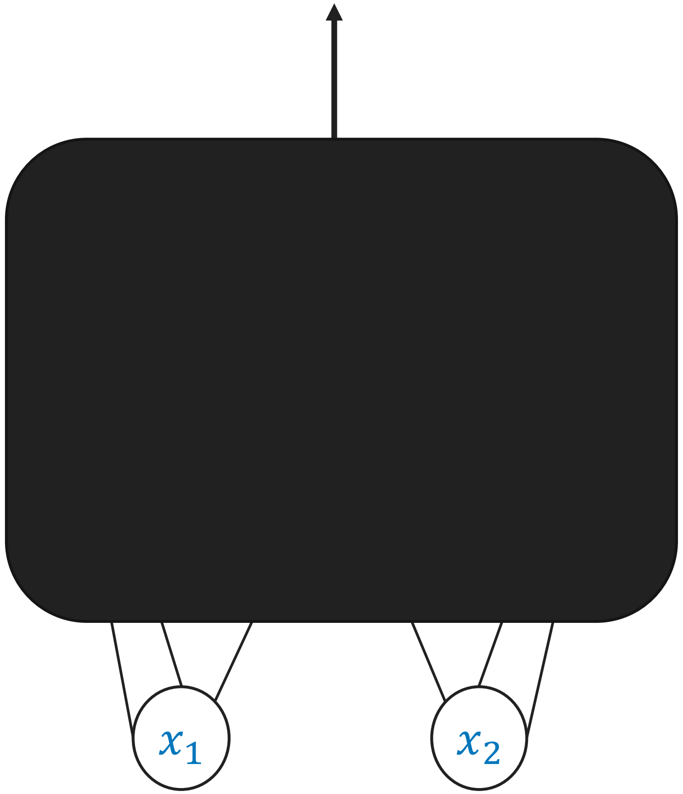
Polynomial Identity Testing

PIT

Given a circuit C over a field $\mathbb{F}$, test if $C = 0$.

- Whitebox.
- Blackbox.
  - PIT is efficient with randomness.

$$\mathbb{F}[x_1, x_2] \ni f_1 = x_1^2 + x_2^2 + 2x_1x_2$$



Efficient Randomized algorithm

PIT Lemma

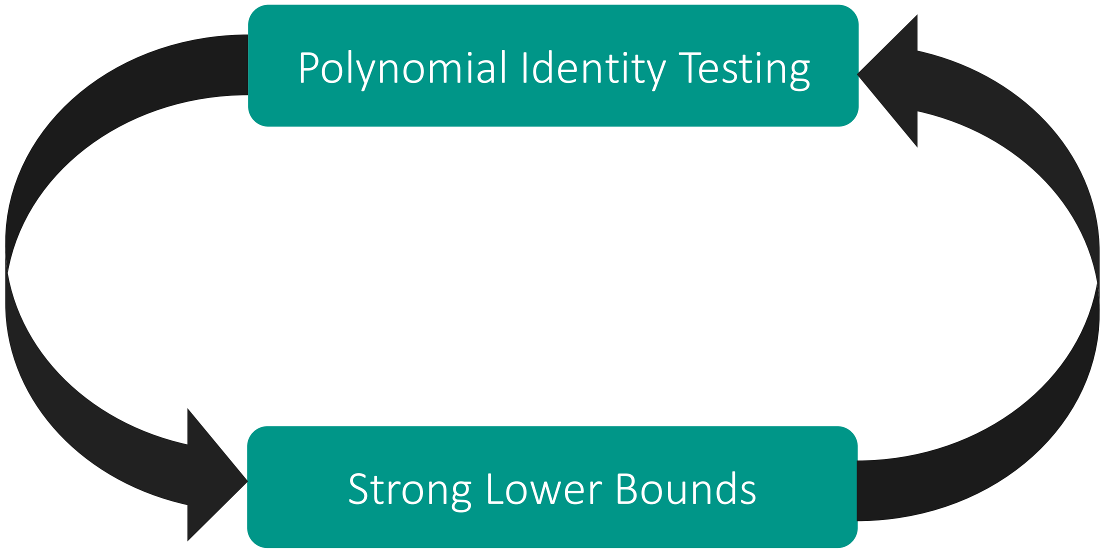
Let S be a subset of field. For $f \neq 0$ and some random $\overline{a} \in S^n$

$$\Pr[\, f(\overline{a}) = 0\,] \leq \frac{d}{|S|}.$$

- Randomized algorithm: Consider set S of size more than $(d+1)$.
- Also gives a $\mathbf{poly}(d^n)$ time deterministic algorithm.

Why do we care?

- Algorithms
- Complexity Theory
- Lower Bounds
  - PIT is intrinsically connected to proving circuit lower bounds.



State of Affairs

Status Quo

- Nothing better than exponential known for general algebraic circuits.
- Constant depth circuits in SUBEXP algorithm. [LST21]
- Efficient algorithm are there for very restricted circuits.

[LST21] Nutan Limaye, Srikanth Srinivasan, Sébastien Tavenas

Depth-4 circuits

$$\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$$

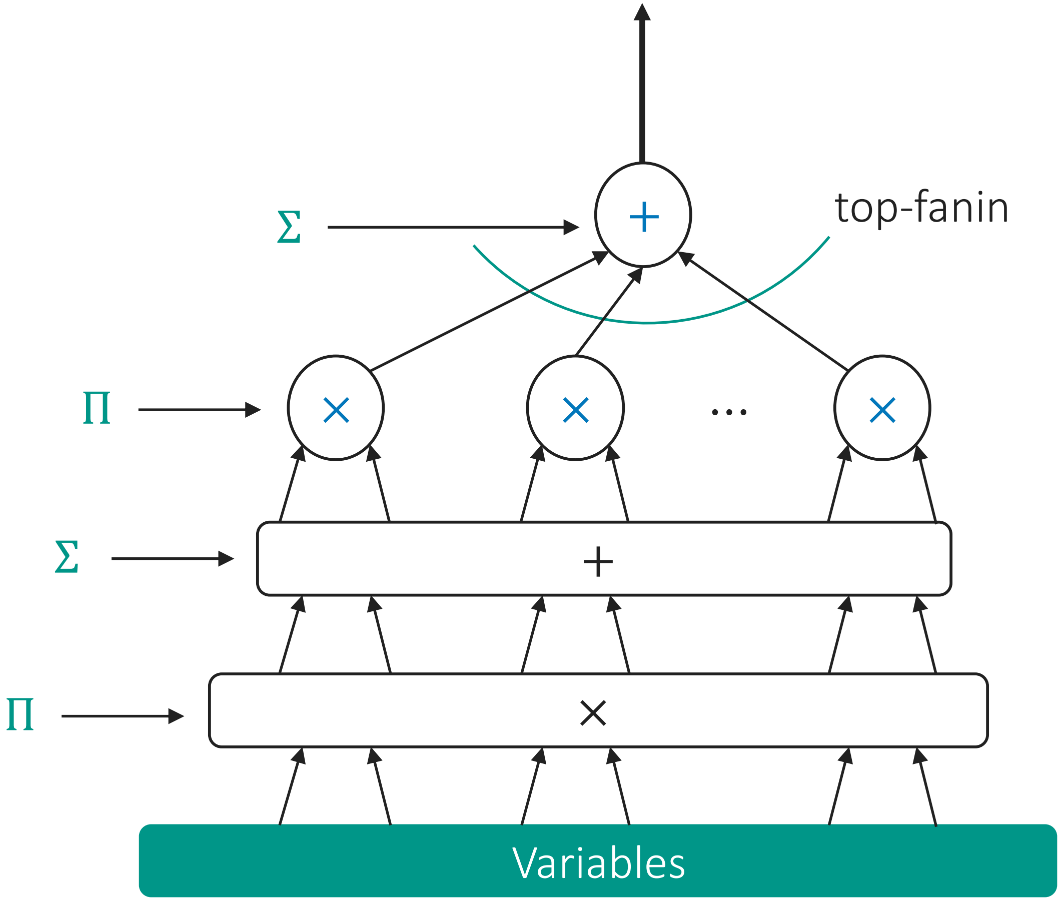
$$\mathbb{F}[x_1, \dots, x_n] \ni f = \sum_i^k \prod_j (\text{sparse polynomial})_{ij}$$

The restriction is special!

Agrawal-Vinay

$\Sigma\Pi\Sigma\Pi$ PIT is **almost** as hard as the general case.

- Nothing better than SUBEXP is known.
- Poly (and quasi-poly) time algorithms are found with various *restrictions*



[AV08] Manindra Agrawal V. Vinay

PIT on Depth Restricted Circuits

$$\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$$

- Promising model.
- Poly (and quasi-poly) time algorithms are found with various *restrictions* on the depth-4 model.
- Bounded top and bottom fanin.

Paper	Restriction	PIT
Saxena and Seshadhri	$\delta = 1$	$\mathrm{poly}(n, d^k)$
Beecken, Mittmann and Saxena	Bounded trdeg	$\mathrm{poly}(s^k)$ *(k=trdeg bound)*
Agarwal, Saha, Saptharishi and Saxena	Bounded top-fanin, multilinear	$\mathrm{poly}\left(s^{k^2}\right)$
Kumar and Saraf	Low individual deg	$\mathrm{QP}(n)$
	Bounded local trdeg and bottom fanin	$\mathrm{QP}(n)$
Peleg and Shpilka	$k = 3, \delta = 2$	$\mathrm{poly}(n, d)$

Results

Blackbox PIT of $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ circuits

Theorem [DuttaDSaxena21]

For constant k, δ there is a quasi-poly time blackbox PIT algorithm for $\Sigma^{[\mathrm{k}]}\Pi\Sigma\Pi^{[\delta]}$ circuits.

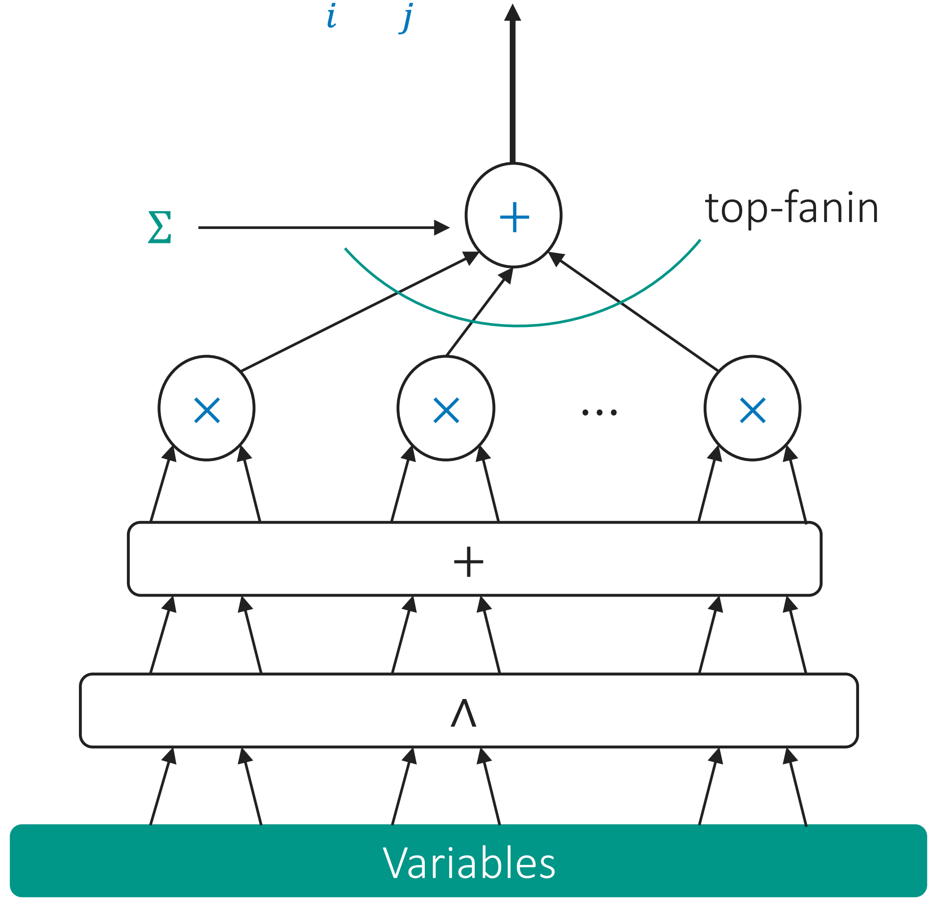
- For size s circuit we give $s^{O(\delta^2 \cdot k \cdot log\ s)}$ time deterministic algorithm.
- The algorithm is quasi-poly even up to $k, \delta = \mathrm{poly}(\log s)$.

PIT on $\Sigma^{[k]}\Pi\Sigma\wedge$ circuits

$$\Sigma^{[k]}\Pi\Sigma\wedge$$

- Sum of product of sum of **univariates**.
- Deterministic PIT was open since 2013 [SSS13].

$$\mathbb{F}[x_1,\dots,x_n] \ni f = \sum_{i}^{k}\prod_{j}\left(g_{ij1}(x_1)+\cdots+g_{ijn}(x_n)\right)$$



[SSS13] Chandan Saha, Ramprasad Saptharishi, Nitin Saxena

Blackbox PIT of $\Sigma^{[k]}\Pi\Sigma\wedge$ circuits

Theorem [DuttaDSaxena21]

For constant k there is a quasi-poly time blackbox PIT algorithm for $\Sigma^{[k]}\Pi\Sigma\wedge$ circuits.

- For size s circuit we give $s^{O(k \cdot log\ log\ s)}$ time deterministic algorithm.
- Faster than our $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ PIT algo.

Whitebox PIT of $\Sigma^{[k]}\Pi\Sigma\wedge$ circuits

Theorem [DuttaDSaxena21]

For constant k there is a poly time whitebox PIT algorithm for $\Sigma^{[\mathrm{k}]}\Pi\Sigma\wedge$ circuits.

- For size s circuit we give $s^{O(k\cdot 7^k)}$ time deterministic algorithm.

Proof Overview

DiDI Technique on $\Sigma^{[k]}\Pi\Sigma\wedge$ circuits

Problem ($\Sigma^{[k]}\Pi\Sigma\wedge$ PIT)

Test

$$f = T_1 + T_2 + \cdots T_k \stackrel{?}{=} 0$$

where $T_i \in \Pi\Sigma\wedge$ of $\deg \leq d$.

- Divide and Derive inductively. Top $\Pi \to \wedge$.
- Primal Idea: $g(X) \neq 0 \iff g'(X) \neq 0 \; or \; g(0) \neq 0$
- $\Sigma\wedge\Sigma\wedge$ has a poly-time whitebox PIT.

Design a homomorphism $\Psi: \mathbb{F}[\bar{x}] \to \mathbb{F}[\bar{x}, z]$ manifesting '*nice*' property.

↓

Divide and Derive to reduce to $k-1$ case.

↓

⋮

↓

PIT on $k = 1$ is easy.

Jacobian hits for $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ blackbox PIT

Problem

Test

$$f = T_1 + T_2 + \cdots T_k \overset{?}{=} 0$$

Where $T_i = \prod_j g_{ij} \in \Pi\Sigma\Pi^{[\delta]}$ of degree at most d and size s.

- Faithful map Φ follows from Hitting set of $\Sigma\wedge\Sigma\Pi^{[\delta]}$-circuit.
- $\Phi(f)$ is essentially k variate.

Design a homomorphism
$\Psi: \mathbb{F}[\bar{x}] \to \mathbb{F}[\bar{x}, z]$
manifesting '*nice*' property.

↓

Fixing $\bar{x}$ suitably using 'nice' property
$\Psi': \mathbb{F}[\bar{x}] \to \mathbb{F}[z]$
such that it preserves rank of *Jacobian*.

↓

Extend Ψ' to a *faithful* map
$\Phi: \mathbb{F}[\bar{x}] \to \mathbb{F}[z, y_1, \ldots y_k, t]$

↓

Use PIT Lemma for final Hitting Set of
$\Phi(f)$

**Agarwal, Saha, Saptharishi and Saxena*

Open Problems

Open Problems

- Design a poly-time algorithm for $\Sigma \wedge \Sigma\Pi^{[\delta]}$-circuits.
  - It will place PIT of $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ in P.
- Solve PIT for $\Sigma^{[k]}\Pi\Sigma \wedge^{[2]}$ - sum of product of sum of bivariate fed into top product gate.
- Improve the dependence on k for $\Sigma^{[k]}\Pi\Sigma \wedge$ whitebox PIT.
  - Currently it is exponential in k.

Hitting Set

Definition [Hitting Set]

A set $\mathcal{H} \subseteq \mathbb{F}^n$ which certifies the non-zeroness of class $\mathcal{C}$ of polynomials.

$$\forall f \neq 0 \in \mathcal{C}, \qquad \exists \bar{a} \in \mathcal{H} : f(\bar{a}) \neq 0$$

- Blackbox PIT $\leftrightarrow$ Hitting Set.

Trivial Hitting Set

Lemma [Trivial Hitting Set]

For a class of n-variate, deg d polynomials, there exists an explicit hitting set of size $\mathbf{poly}(d^n)$

- Suffices when $n = O(1)$.
- Offers a general framework for PIT algorithms.
  - Design a variable reducing non-zeroness preserving map.

Recapitulation of $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ blackbox PIT

Problem

Test

$$f = T_1 + T_2 + \cdots T_k \overset{?}{=} 0$$

Where $T_i = \prod_j g_{ij} \in \Pi\Sigma\Pi^{[\delta]}$ of degree at most d and size s.

Design a homomorphism $\Psi: \mathbb{F}[\bar{x}] \to \mathbb{F}[\bar{x}, z]$ manifesting nice property.

Fixing $\bar{x}$ suitably using 'nice' property $\Psi': \mathbb{F}[\bar{x}] \to \mathbb{F}[z]$ such that it preserves rank of Jacobian.

Extend Ψ' to a faithful map $\Phi: \mathbb{F}[\bar{x}] \to \mathbb{F}[z, \bar{y}, t]$

Use PIT Lemma for final Hitting Set of $\Phi(f)$

Faithful homomorphism

- Set of polynomials $\bar{T} = \{T_1, \dots, T_m\}$ in $\mathbb{F}[\bar{x}]$ are *algebraically dependent* if there is an non-zero *annihilator* A such that $A(\bar{T}\ ) = 0$.
- Transcendence Degree (trdeg): Size of the largest subset of $S \subseteq \bar{T}$ which is alg. independent.
  - S is called the *Transcendence Basis*.

Faithful homomorphism

Definition [Faithful hom.]

$\Phi: \mathbb{F}[\bar{x}] \to \mathbb{F}[\bar{y}]$ such that

$$\mathrm{trdeg}_{\mathbb{F}}\,(\bar{T}) = \mathrm{trdeg}_{\mathbb{F}}\big(\Phi(\bar{T})\big).$$

Theorem [Faithful is useful]

For any $C \in \mathbb{F}[y_1, \dots, y_k]$,

$$C(\bar{T}) = 0 \iff C\big(\Phi(\bar{T})\big) = 0.$$

Recapitulation of $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ blackbox PIT

Problem

Test

$$f = T_1 + T_2 + \cdots T_k \stackrel{?}{=} 0$$

Where $T_i = \prod_j g_{ij} \in \Pi\Sigma\Pi^{[\delta]}$ of degree at most d and size s.

Design a homomorphism
$\Psi: \mathbb{F}[\bar{x}] \to \mathbb{F}[\bar{x}, z]$
manifesting '*nice*' property.

Fixing $\bar{x}$ suitably using 'nice' property
$\Psi': \mathbb{F}[\bar{x}] \to \mathbb{F}[z]$
such that it preserves rank of *Jacobian*.

Extend Ψ' to a *faithful* map
$\Phi: \mathbb{F}[\bar{x}] \to \mathbb{F}[z, \bar{y}, t]$

Use PIT Lemma for final Hitting Set of
$\Phi(f)$

Jacobian Hits (Again)

- Jacobian $\mathcal{J}_{\bar{x}}(\bar{T})$ is a $k \times n$ matrix.

$$\mathcal{J}_{\bar{x}}(\bar{T}) = \left(\partial_{x_j}(T_i)\right)_{k\times n} = \begin{bmatrix} \partial_{x_1}(T_1) & \cdots & \partial_{x_n}(T_1) \\ \vdots & \ddots & \vdots \\ \partial_{x_1}(T_m) & \cdots & \partial_{x\_n}(T_k) \end{bmatrix}$$

- Linear rank captures the alg. rank.

Theorem [Beecken Mittmann Saxena]

Jacobian Criterion: For large $\mathrm{char}\ \mathbb{F}$,

$$\mathrm{trdeg}_{\mathbb{F}}\,(\bar{T}) = \mathrm{rank}_{\mathbb{F}(\bar{x})}\mathcal{J}_{\bar{x}}(\bar{T})$$

Jacobian Hits (Again)

- Jacobian offers the recipe of *faithful* map.
- Let $\Psi': \mathbb{F}[\bar{x}] \to \mathbb{F}[\bar{z}]$ such that

$$\mathrm{rank}_{\mathbb{F}(\bar{x})}\mathcal{J}_{\bar{x}}(\bar{T}) = \mathrm{rank}_{\mathbb{F}(\bar{z})}\Psi'\big(\mathcal{J}_{\bar{x}}(\bar{T})\big).$$

Theorem [ASSS16*]

For large $\mathbf{char}\ \mathbb{F}$, the map $\Phi: \mathbb{F}[\bar{x}] \to \mathbb{F}[z, \bar{y}, t]$ *defined as*

$$x_i \to \left(\sum_j y_j\, t^{ij}\right) + \Psi'(x_i)$$

is *faithful* for $T_1, \ldots T_k$.

**Agarwal, Saha, Saptharishi and Saxena*

Recapitulation of $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ blackbox PIT

Problem

Test

$$f = T_1 + T_2 + \cdots T_k \stackrel{?}{=} 0$$

Where $T_i = \prod_j g_{ij} \in \Pi\Sigma\Pi^{[\delta]}$ of degree at most d and size s.

Design a homomorphism
$\Psi: \mathbb{F}[\bar{x}] \to \mathbb{F}[\bar{x}, z]$
manifesting '*nice*' property.

Fixing $\bar{x}$ suitably using 'nice' property
$\Psi': \mathbb{F}[\bar{x}] \to \mathbb{F}[z]$
such that it preserves rank of *Jacobian*.

Extend Ψ' to a *faithful* map
$\Phi: \mathbb{F}[\bar{x}] \to \mathbb{F}[z, \bar{y}, t]$

Use PIT Lemma for final Hitting Set of
$\Phi(f)$

Homomorphism Ψ

$$\mathcal{J}_{\bar{x}}(\bar{T}) = \left(\partial_{x_j}(T_i)\right)_{k\times k}$$

- Let $T_1, \ldots, T_k$ is the tr-basis.
- Let $J_{\bar{x}}(\bar{T}) = \mathrm{Det}\, \mathcal{J}_{\bar{x}}(\bar{T})$,
  - To preserve rank, ensure determinant is non-zero.
  - $T_i = \prod_j g_{ij}$ and $L(T_i) = \{g_{ij} | j\}$.

$$J_{\bar{x}}(\bar{T}) = T_1 \ldots T_k \sum_{g_1 \in L(T_1), \ldots g_k \in L(T_k)} \frac{J_{\bar{x}}(g_1, \ldots, g_k)}{g_1 \cdots g_k}$$

Homomorphism Ψ

- Consider an $\bar{\alpha} = (a_1, \ldots, a_n) \subseteq \mathbb{F}^n$ such that $g(\bar{\alpha}) \neq 0$ for all $g \in \bigcup_i L(T_i)$. Find it using PIT for sparse polynomials.
- Define $\Psi: \mathbb{F}[\bar{x}] \to \mathbb{F}[\bar{x}, z]$ such that

$$x_i \mapsto z \cdot x_i + a_i.$$

$$\Psi(J_{\bar{x}}(\bar{T})) = \Psi(T_1 \ldots T_k) \underbrace{\boxed{\sum_{(\cdot)} \frac{\Psi(J_{\bar{x}}(g_1, \ldots, g_k))}{\Psi(g_1 \cdots g_k)}}}_{F}$$

Homomorphism Ψ

Define $\mathcal{R} = \mathbb{F}[z_1]/\langle z_1^D \rangle$ where $D = \deg(f) + 1$.

Claim

Over $\mathcal{R}[\bar{x}]$,

- $J_{\bar{x}}(\bar{T}) = 0 \Leftrightarrow \Psi(J_{\bar{x}}(\bar{T})) = 0$.
- $\Psi(J_{\bar{x}}(\bar{T})) = 0 \ \Leftrightarrow F = 0$.

- Since $J_{\bar{x}}(\bar{T}) \neq 0$, then $F \neq 0$ over $\mathcal{R}[\bar{x}]$.
- Construct a set $H' \subseteq \mathbb{F}^n$: $\Psi\big(J_{\bar{x}}(\bar{T})\big)\big|_{\bar{x}=\bar{a}} \neq 0$ for some $\bar{a} \in H'$.
- For this we construct a hitting-set for F.

Recapitulation of $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ blackbox PIT

Problem

Test

$$f = T_1 + T_2 + \cdots T_k \stackrel{?}{=} 0$$

Where $T_i = \prod_j g_{ij} \in \Pi\Sigma\Pi^{[\delta]}$ of degree at most d and size s.

Design a homomorphism
$\Psi\colon \mathbb{F}[\bar{x}] \to \mathbb{F}[\bar{x}, z]$
manifesting '*nice*' property.

↓

Fixing $\bar{x}$ suitably using 'nice' property
$\Psi'\colon \mathbb{F}[\bar{x}] \to \mathbb{F}[z]$
such that it preserves rank of *Jacobian*.

↓

Extend Ψ' to a *faithful* map
$\Phi\colon \mathbb{F}[\bar{x}] \to \mathbb{F}[z, \bar{y}, t]$

↓

Use PIT Lemma for final Hitting Set of
$\Phi(f)$

Towards extending Ψ to Ψ'

$$\Psi(J_{\bar{x}}(\bar{T})) = \Psi(T_1 \ldots T_k) \underbrace{\boxed{\sum_{(\cdot)} \frac{\Psi(J_{\bar{x}}(g_1, \ldots, g_k))}{\Psi(g_1 \cdots g_k)}}}_{\mathrm{F}}$$

Claim [Nice Property]

Over $\mathcal{R}[\bar{x}]$, F can be computed by $\Sigma\wedge\Sigma\Pi^{[\delta]}$-circuit of size $(s \cdot 3^{\delta})^{O(k)}$.

- $F = P(\bar{x}, z)/Q$ where $Q \in \mathbb{F}$.
- Degree of P wrt z remains polynomially bounded.

$\Sigma\wedge\Sigma\Pi^{[\delta]}$ - sum of powers of (degree δ) sparse polynomials.

Towards extending Ψ to Ψ'

- Essentially, H' will be the hitting-set for 'small' size $\Sigma \wedge \Sigma\Pi^{[\delta]}$.
- [Forbes15] gave the hitting set for the class.
- Use that to conclude that $\bar{b} \in H' \subseteq \mathbb{F}^n$ such that $P(\bar{b}, \bar{z}) \neq 0$ is of size $s^{O(\delta^2 \cdot k \cdot \log s)}$.
- H' fixes $\bar{x}$ in Ψ and gives $\Psi' : \mathbb{F}[\bar{x}] \to \mathbb{F}[z]$

$$x_i \mapsto z \cdot b_i + a_i.$$

Recapitulation of $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$ blackbox PIT

Problem

Test

$$f = T_1 + T_2 + \cdots T_k \stackrel{?}{=} 0$$

Where $T_i = \prod_j g_{ij} \in \Pi\Sigma\Pi^{[\delta]}$ of degree at most d and size s.

- Faithful map Φ follows from Hitting set of $\Sigma \wedge \Sigma\Pi^{[\delta]}$-circuit.
- Therefore, $\Phi(f)$ is essentially $k+3$ variate.

Design a homomorphism
$\Psi: \mathbb{F}[\bar{x}] \rightarrow \mathbb{F}[\bar{x}, z]$
manifesting '*nice*' property.

↓

Fixing $\bar{x}$ suitably using 'nice' property
$\Psi': \mathbb{F}[\bar{x}] \rightarrow \mathbb{F}[z]$
such that it preserves rank of *Jacobian*.

↓

Extend Ψ' to a *faithful* map
$\Phi: \mathbb{F}[\bar{x}] \rightarrow \mathbb{F}[z, y_1, \ldots y_k, t]$

↓

Use PIT Lemma for final Hitting Set of
$\Phi(f)$