# Paradigms for *bounded* topfanin depth-4 circuits

Pranjal Dutta (CMI & IIT Kanpur), Prateek Dwivedi (IIT K), Nitin Saxena (IIT K)

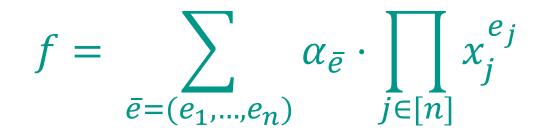




# **Polynomial Identity Testing**

#### **Multivariate Polynomials**

- $f(\bar{x}) \in \mathbb{F}[x_1, \dots, x_n]$
- deg f = d. Then,  $\sum_j e_j \le d$ .
- $\alpha_{\bar{e}}$  are field elements.



## $f(x_1, x_2, x_3) = 1 + x_1 + x_2 + x_3 + x_1 x_2 + x_1 x_3 + x_2 x_3 + x_1 x_2 x_3$ = $(1 + x_1)(1 + x_2)(1 + x_3)$

#### Polynomials: Ubiquitous object in Computer Science

- Graph Algorithm.
- Coding Theory.
- Cryptography.
- Computational Algebra.
- Circuit Complexity.
- Polynomial method in Combinatorics.

#### **Natural Operations**

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 g = f.

#### **Identity Testing**

For some polynomial g, test g = f.

- 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 =  $\binom{n+d}{d} \approx \text{EXP}(n, d)$ .

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

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

#### **Representing Multivariate Polynomials**

- Sparse Representation:  $\overline{\alpha}_{\overline{e}}$ .
  - Intuitive.

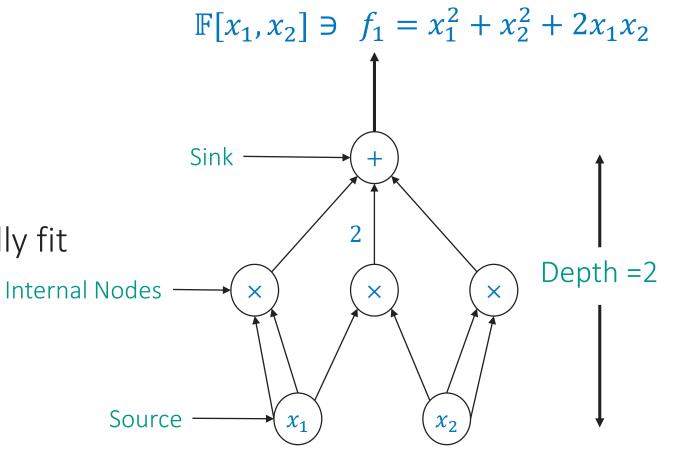


- Operations are easy (sum, product, etc)
- Due to exponential many monomials highly non-succinct.

$$f_1 = \sum_{S \subseteq [n]} \prod_{i \in S} x_i$$
  $f_2 = \prod_{i=[n]} (x_i + 1)$ 

#### **Representing Multivariate Polynomials**

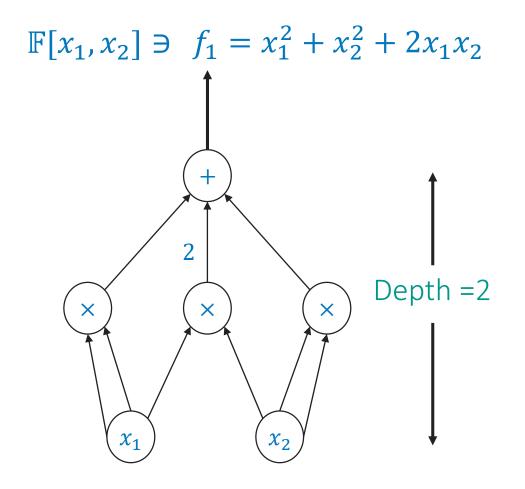
- Algebraic Circuits
  - Natural. Succinct.
  - Operations are easy.
  - Algebraic problems naturally fit into the framework.



Size = Number of gates = 6

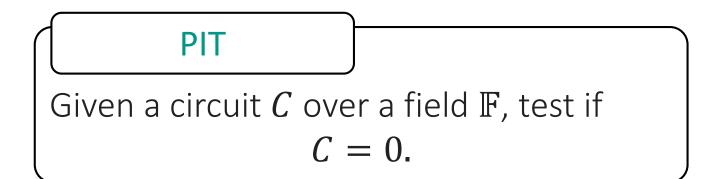
#### **Representing Multivariate Polynomials**

- Algebraic Circuits
  - Intuitive. Succinct.
  - Operations are easy.
  - Algebraic problems naturally fit into the framework.
  - PIT is efficient with *randomness*.

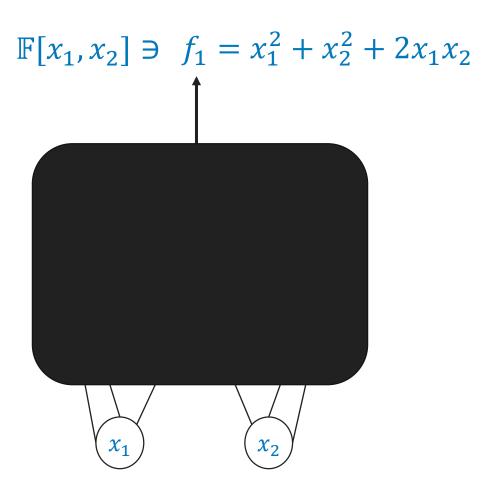


Size = Number of gates = 6

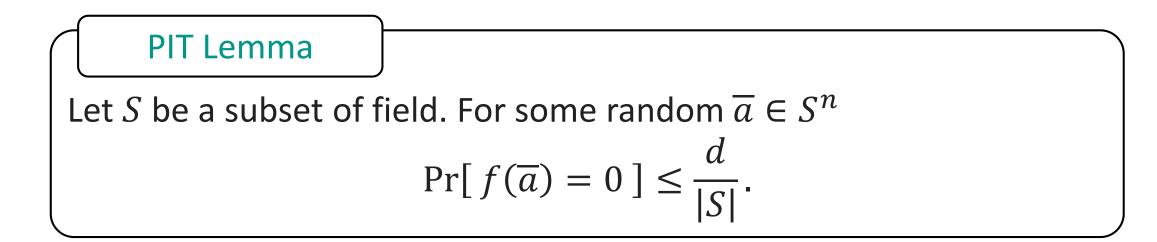
#### **Polynomial Identity Testing**



- Whitebox.
- Blackbox.



#### Efficient Randomized algorithm



- Randomized algorithm: Consider set S of size more than (d + 1).
- Also gives a  $poly(d^n)$  time deterministic algorithm.
- Can we do better?

#### Why do we care?

• Algorithms

#### PIT ↔ Perfect Matching

For a graph G(V, E) on n verticies,

Tutte Matrix T is a  $n \times n$  matrix:

$$T_{ij} = \begin{cases} x_{ij}, \text{ if } (i,j) \in E \text{ and } i < j \\ -x_{ij}, \text{ if } (i,j) \in E \text{ and } i > j \\ 0, \text{ otherwise} \end{cases}$$

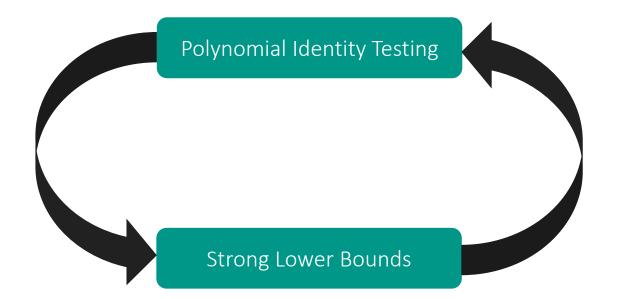
**Tutte's Characterisation** 

G has a perfect matching  $\Leftrightarrow \det T \neq 0$ 

- Determinant is a polynomial. Then testing det T = 0 is PIT.
- Gives a randomized parallel algorithm using PIT Lemma.

#### Why do we care?

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



#### $PIT \rightarrow Lower Bounds$

Kabanets and Impagliazzo (STOC'03)

PIT  $\in$  P  $\implies$  Either NEXP is not in P/poly or Permanent is hard.

- "hard" means it requires super polynomial size algebraic circuits.
- Connects derandomizing PIT with Boolean/Algebraic Lower Bounds.
- Wishful thinking: PIT relates to Permanent hardness?
- Heintz and Schnorr (STOC'80), and later Agrawal (FSTTCS'05), showed PIT ∈ P implies there is a PSPACE computable polynomials which is very hard.

# State of Affairs



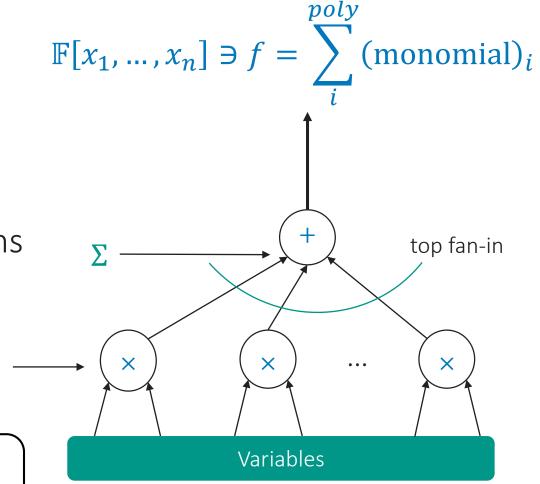
- Nothing better than exponential known for **general** algebraic circuits.
- **Constant depth** circuits in **SUBEXP** algorithm.

[Limaye,Srinivasan,Tavenas FOCS'21]

• Efficient algorithm are there for very restricted circuits.

#### Depth-2 circuits: Sparse Polynomials

- Monomials only polynomial in n.
- Whitebox is easy.
- Blackbox is easy as well due to Klivans and Spielman (2001).



Sparse PIT (KS, STOC'01)

For  $\Sigma\Pi$  circuit of size-*s* and sparsity-*m* PIT is possible in poly(*s*,*m*).

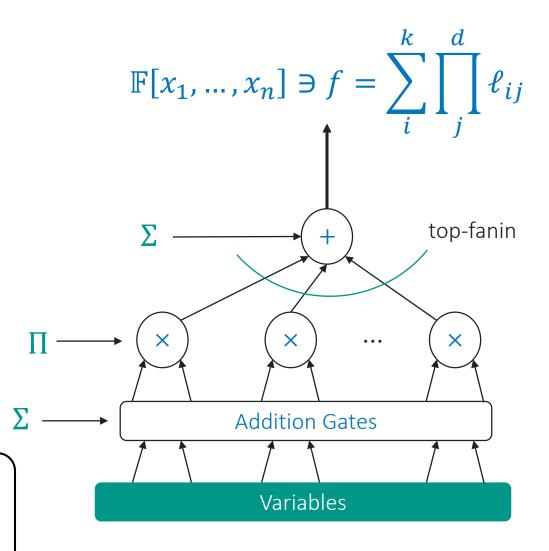
#### **Depth-3 circuits**

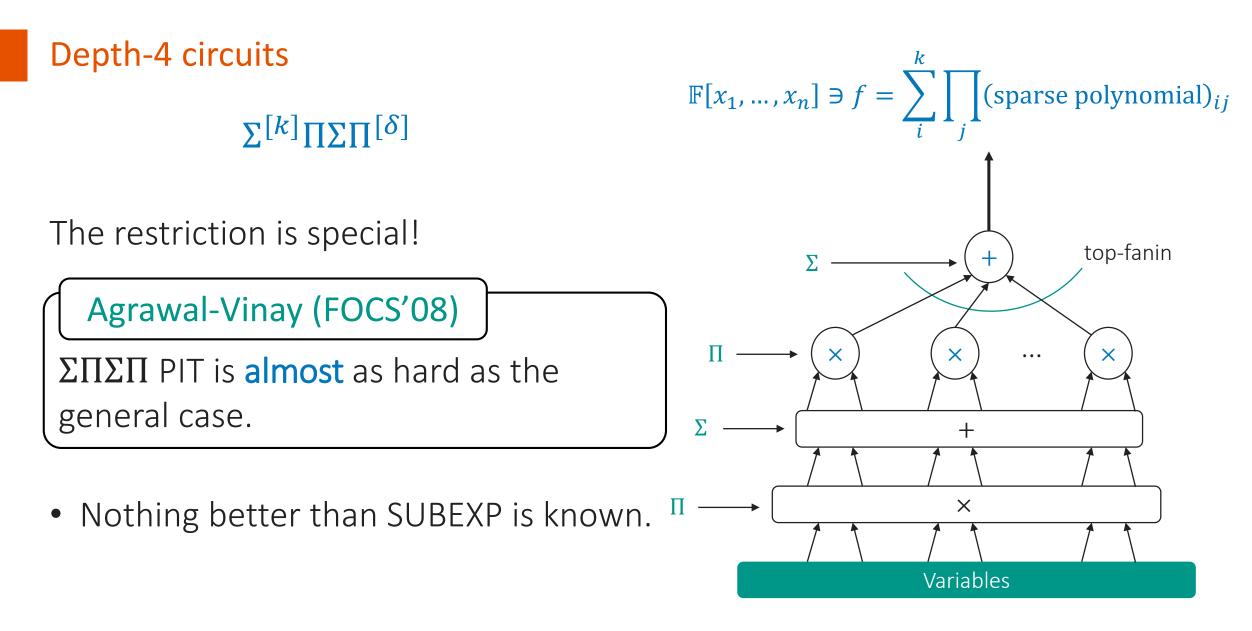
- Sum of product of *linear terms*.
- SUBEXP algorithm due to LST21.
- There is poly-time blackbox PIT algorithm when *k* is constant due to

Saxena and Seshadhri (2011).

 $Σ^{[k]}ΠΣ$  PIT (SS, STOC'11)

For a size-s circuit PIT algorithm runs in  $poly(s, d^k)$ 

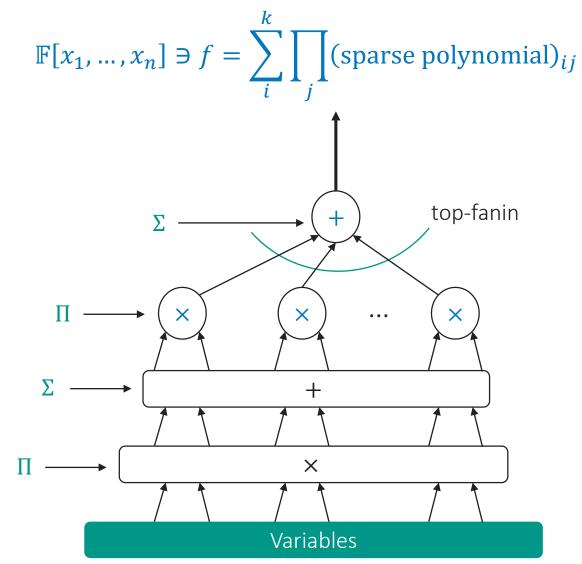




#### Depth-4 circuits

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

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



<sup>[</sup>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.
- One such restriction we consider is *bounded top and bottom fanin*.

Paper	Restriction	PIT
Saxena and Seshadhri (STOC'11)	$\delta = 1$	poly(n, d <sup>k</sup> )
Beecken, Mittmann and Saxena (ICALP'11)	Bounded trdeg	poly(s <sup>k</sup> ) (k=trdeg bound)
Agarwal, Saha, Saptharishi and Saxena (STOC'12)	Bounded top- fanin, multilinear	$\operatorname{poly}(s^{k^2})$
Kumar and Saraf (CCC'16)	Low individual deg	QP(n)
	Bounded local trdeg and bottom fanin	QP(n)
Peleg and Shpilka (STOC'21)	$k = 3, \delta = 2$	poly(n, d)

# New Developments

Theorem 1 [Dutta,Dwivedi,S CCC'21]

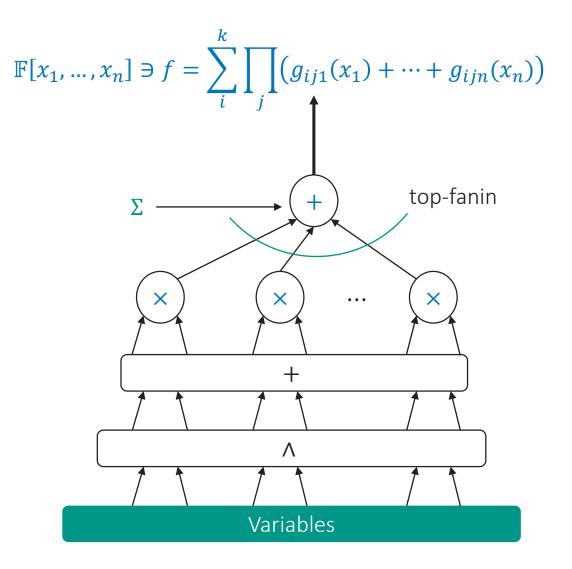
For constant  $k, \delta$  there is a quasi-poly time blackbox PIT algorithm for  $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$  circuits.

- 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  $k, \delta = poly(\log s)$ .

## 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 [Saha,Saptharishi,S, Comp.Compl.'13].



[SSS13] Chandan Saha, Ramprasad Saptharishi, Nitin Saxena

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

Theorem 2 [Dutta,Dwivedi,S CCC'21]

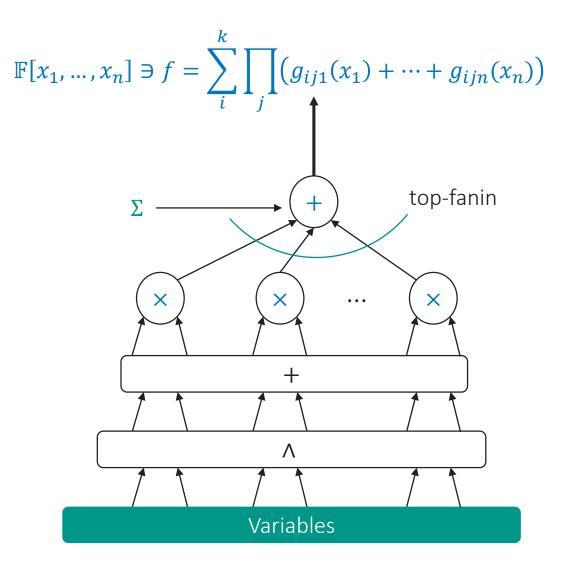
For constant k there is a quasi-poly time blackbox PIT algorithm for  $\Sigma^{[k]}\Pi\Sigma \wedge \text{circuits}$ .

- For size *s* circuit we take  $s^{O(k \cdot \log \log s)}$  time.
- Similar proof, but faster than our  $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$  PIT algo.

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

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

- Sum of product of sum of **univariates**.
- $k \leq 2$  was already solved in [SSS13].
- But k > 2 was open!



[SSS13] Chandan Saha, Ramprasad Saptharishi, Nitin Saxena

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

Theorem 3 [Dutta, Dwivedi, S CCC'21]

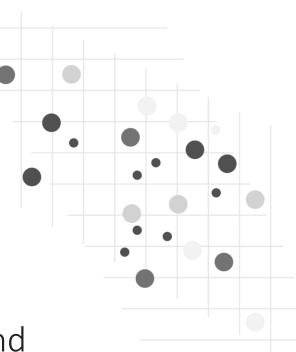
For constant k there is a poly time whitebox PIT algorithm for  $\Sigma^{[k]}\Pi\Sigma \wedge \text{circuits}$ .

- For size *s* circuit we take  $s^{O(k \cdot 7^k)}$  time.
- Introducing **DiDI**-technique (**Di**vide **D**erive Induct).
  - Inductive. Top  $\Pi \rightarrow \Lambda$ .
  - Robust enough to give blackbox algorithm. But worse time complexity.

# Conclusion

#### Conclusion

- Introduced PIT and Algebraic Circuits.
- Discussed connection of PIT with algorithms and lower bounds.
- Three new PIT algorithms: Blackbox PIT of  $\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}$  and  $\Sigma^{[k]}\Pi\Sigma \Lambda$ . And Whitebox PIT of  $\Sigma^{[k]}\Pi\Sigma \Lambda$ .



#### **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  $\Sigma^{[k]}\Pi\Sigma \Lambda^{[2]}$  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.

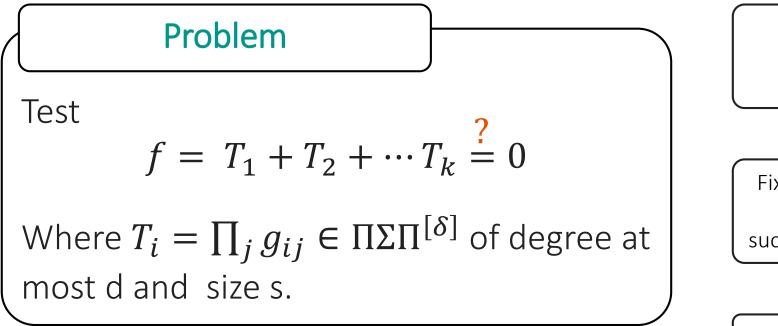


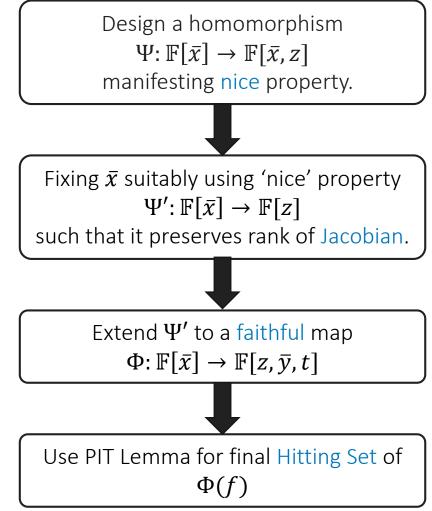
**Proof Overview** 

- Now: Jacobian for blackbox PIT

- Monday: Alternate approach (DiDI)

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







Definition [Hitting Set]

A set  $\mathcal H$  which certifies the non-zeroness of class  $\mathcal C$  of polynomials.

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

• Blackbox PIT  $\leftrightarrow$  Hitting Set.

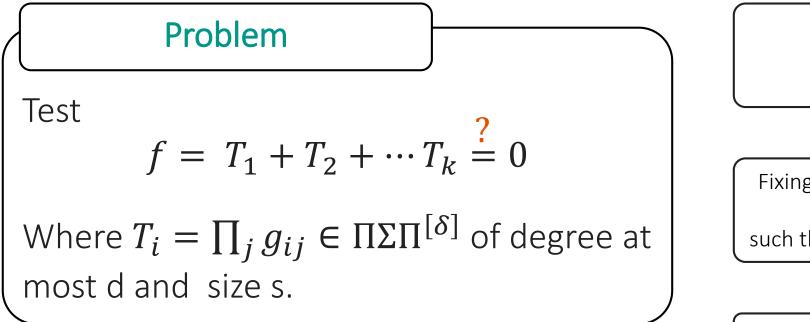


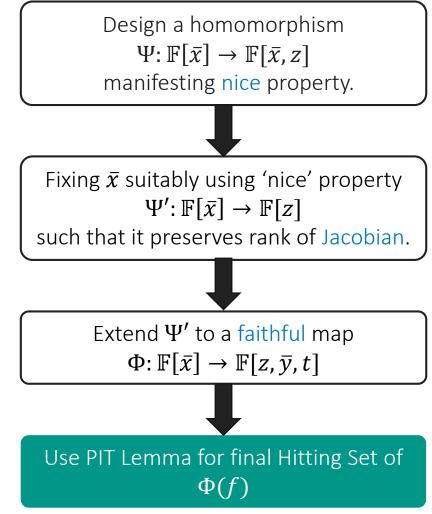
#### Lemma [Trivial Hitting Set]

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

- 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





# Faithful homomorphism

• Set of polynomials  $\overline{T} = \{T_1, \dots, T_m\}$  in  $\mathbb{F}[\overline{x}]$  are *algebraically* 

*dependent* if there is an non-zero *annihilator* A such that  $A(\overline{T}) = 0$ .

- Transcendence Degree (trdeg): Size of the largest subset of  $S \subseteq \overline{T}$  which is alg. independent.
  - S is called the *Transcendence Basis*.

### Faithful homomorphism

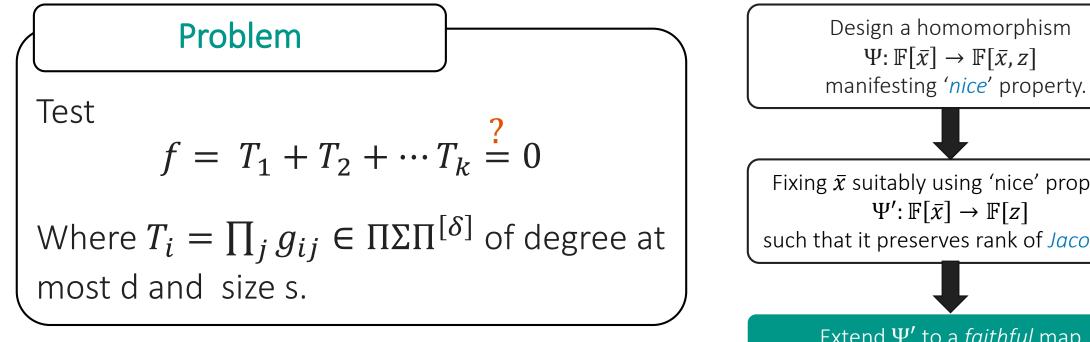
Definition [Faithful hom.]

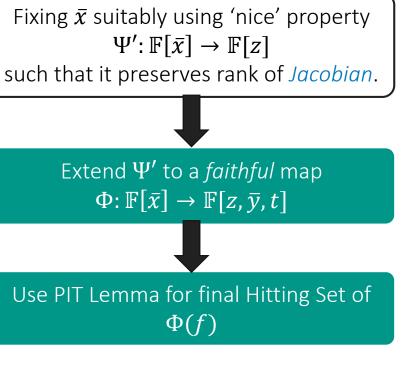
 $\Phi: \mathbb{F}[\bar{x}] \to \mathbb{F}[\bar{y}] \text{ such that}$  $\operatorname{trdeg}_{\mathbb{F}}(\bar{T}) = \operatorname{trdeg}_{\mathbb{F}}(\Phi(\bar{T})).$ 

Theorem [Faithful is useful]

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

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





### Jacobian Hits (Again)

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

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

• Linear rank captures the alg. rank.

Theorem [Beecken, Mittmann, Saxena, ICALP'11]

Jacobian Criterion: For large char F,

$$\operatorname{trdeg}_{\mathbb{F}}(\overline{T}) = \operatorname{rank}_{\mathbb{F}(\overline{x})} \mathcal{J}_{\overline{x}}(\overline{T})$$

#### Jacobian Hits (Again)

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

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

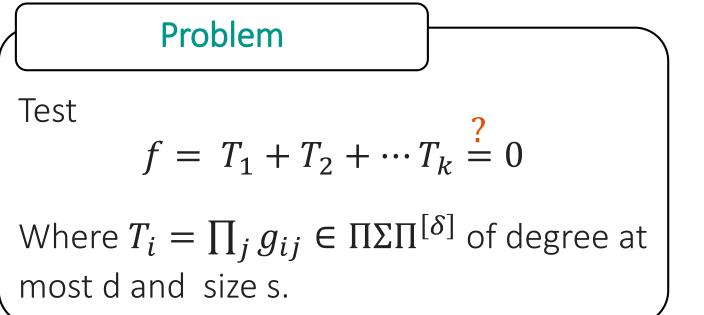
# Theorem [ASSS, STOC'12\*]

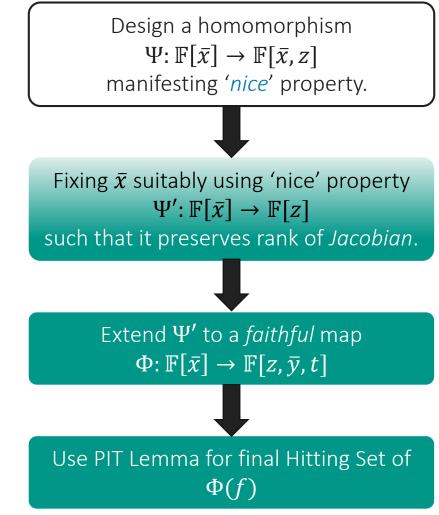
For large char  $\mathbb{F}$ , the map  $\Phi: \mathbb{F}[\bar{x}] \to \mathbb{F}[z, \bar{y}, t]$  defined as

$$x_i \to \left(\sum_{j \le k} y_j t^{ij}\right) + \Psi'(x_i)$$

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

\*Agarwal, Saha, Saptharishi and Saxena





### Homomorphism $\boldsymbol{\Psi}$

- Suppose  $T_1, \ldots, T_k$  is the tr-basis.
- Let  $J_{\bar{x}}(\bar{T}) = \operatorname{Det} \mathcal{J}_{\bar{x}}(\bar{T})$ ,

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

- To preserve rank, ensure determinant is non-zero.
- $L(T_i) := \{g_{ij} \mid j\}.$

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

#### Homomorphism $\boldsymbol{\Psi}$

• Consider an  $\bar{\alpha} = (a_1, \dots, a_n) \subseteq \mathbb{F}^n$  such that  $g(\bar{\alpha}) \neq 0$  for all

 $g \in \bigcup_i L(T_i)$ . Find it using PIT for sparse polynomials.

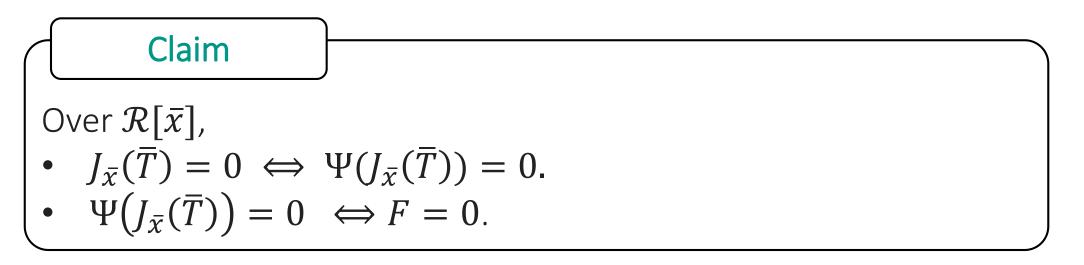
• Define  $\Psi: \mathbb{F}[\bar{x}] \to \mathbb{F}[\bar{x}, z]$  such that

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

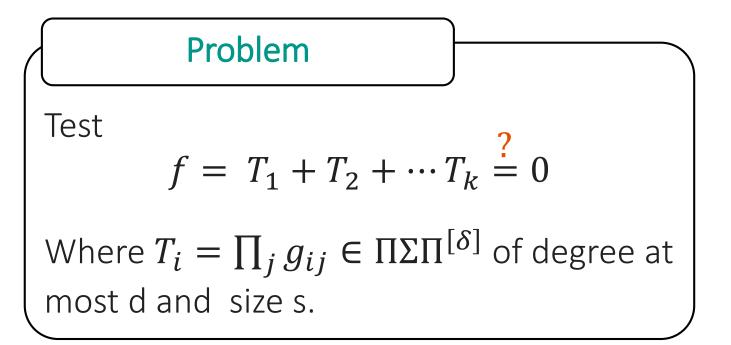
$$\Psi(J_{\bar{x}}(\bar{T})) = \Psi(T_1 \dots T_k) \boxed{\sum_{(\cdot)} \frac{\Psi(J_{\bar{x}}(g_1, \dots, g_k))}{\Psi(g_1 \cdots g_k)}}$$
F

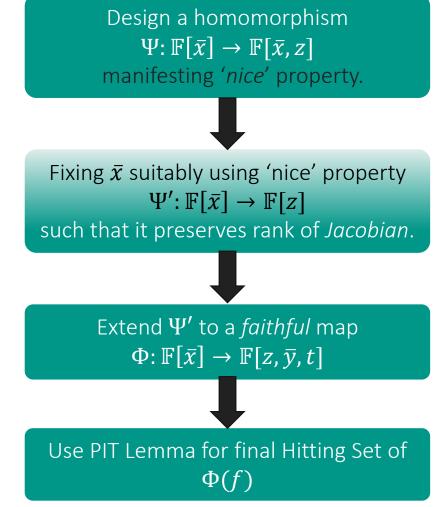
### Homomorphism $\boldsymbol{\Psi}$

For *inverses*--- Define  $\mathcal{R} := \mathbb{F}[z]/\langle z^D \rangle$ , where D := k(d-1) + 1.



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





#### Towards extending $\Psi$ to $\Psi'$

Claim [Nice Property]

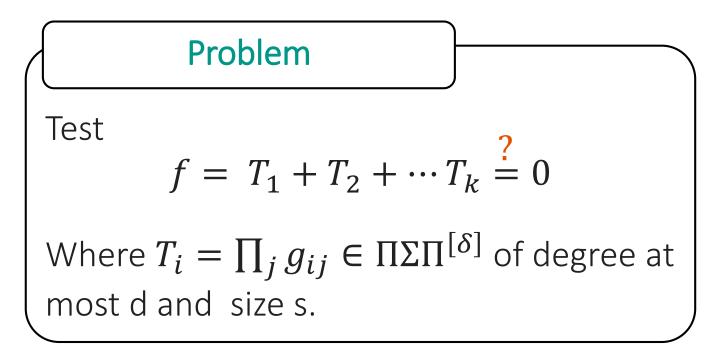
Over  $\mathcal{R}[\bar{x}]$ , F can be computed by  $\Sigma \wedge \Sigma \Pi^{[\delta]}$ -circuit of size  $(s \cdot 3^{\delta})^{O(k)}$ .

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

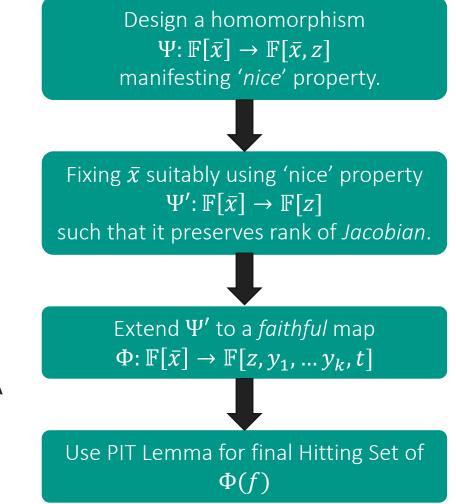
 $\Sigma \wedge \Sigma \Pi^{[\delta]}$  - sum of powers of (degree  $\delta$ ) sparse polynomials.

#### Towards extending $\Psi$ to $\Psi'$

- *Essentially,* H' will be the hitting-set for 'small' size  $\Sigma \wedge \Sigma \Pi^{[\delta]}$ .
- [Forbes, FOCS'15] gave the hitting set for the class.
- Use that to conclude that  $H' \subseteq \mathbb{F}^n$  such that  $P(H', z) \neq 0$ is of size  $s^{O(\delta^2 \cdot k \cdot \log s)}$ .
- H' fixes  $\bar{x}$  in  $\Psi$  and gives  $\Psi'$ .



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



### **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  $\Sigma^{[k]}\Pi\Sigma \Lambda^{[2]}$  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.

