# Treading the Borders

## Explicitness, Circuit Factoring, and Identity Testing

PhD Defense

Prateek Dwivedi

Prof Nitin Saxena

Department of Computer Science and Engineering, Indian Institute of Technology Kanpur, INDIA

# Treading the Borders

## Explicitness, Circuit Factoring, and Identity Testing

## in Algebraic Complexity Theory

# Polynomials

Algebraic Objects $f(\bar{x}) \in \mathbb{F}[x_1, \dots, x_n]$. $\deg f = d$.

Then, $\sum_j e_j \leq d$.

$$f = \sum_{\bar{e}=(e_1,\dots,e_n)} \alpha_{\bar{e}} \cdot \prod_{j \in [n]} x_j^{e_j}$$

**Question**

What is the efficient way to compute a family of polynomials?

$$f = 1 + x_1 + x_2 + x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_1x_2x_3$$

$$f = (x_1 + 1) \cdot (x_2 + 1) \cdot (x_3 + 1)$$

# Polynomials

Ubiquitous object in Computer Science.

- Graph Algorithms
- Coding Theory
- Cryptography
- Computational Algebra
- Circuit Complexity

$$f_1 = (x_1 + x_2)^2$$

$$f_2 = (1 + x_1)(1 + x_2) \cdots (1 + x_n)$$

$$f_3 = \sum_{\sigma \in S_n} sign(\sigma) \cdot x_{1\sigma(1)} \cdots x_{n\sigma(n)}$$

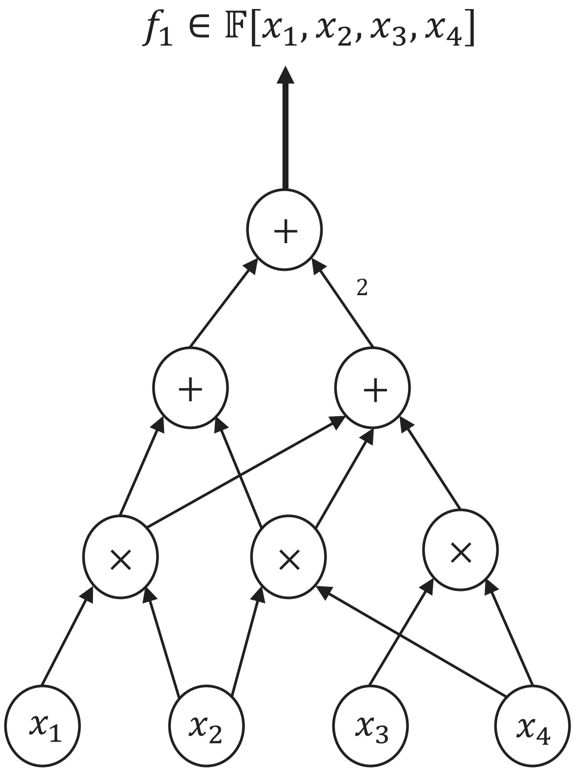
# Algebraic Circuits

**Definition (Algebraic Complexity)**

Size of the smallest circuit computing the polynomial. Denoted by size$(f)$.

Valiant (1977) formalized the notion of computation using Algebraic Circuits.

Circuit resources define Algebraic Complexity Classes.



# Algebraic Complexity Classes

Object of Interest: Polynomials of $n$ variate and degree $d$.

VP: Computable by circuits of size $\mathrm{poly}(n, d)$.

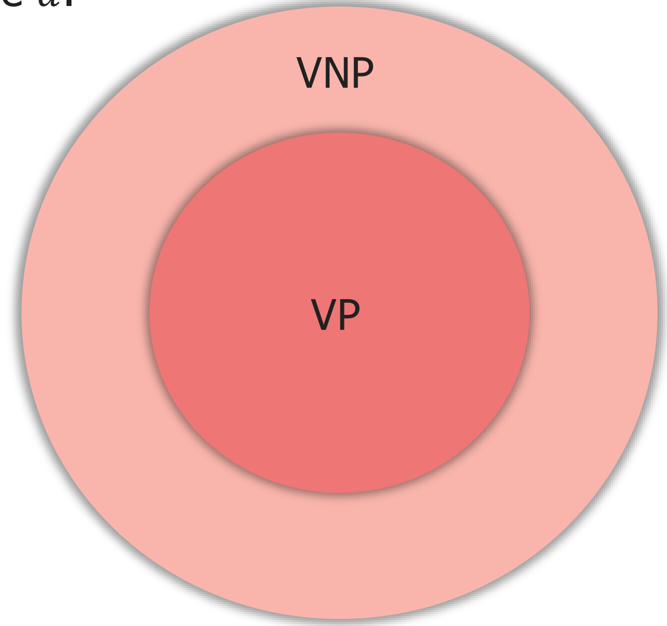
VNP: Explicit polynomials.

**Valiant's Conjecture**

There are explicit polynomials which cannot be computed efficiently.

**Bürgisser 1998**

VP = VNP implies* P/poly = NP/poly




In a more structural and relation-less world, VP $\neq$ VNP.

# Thesis Contribution

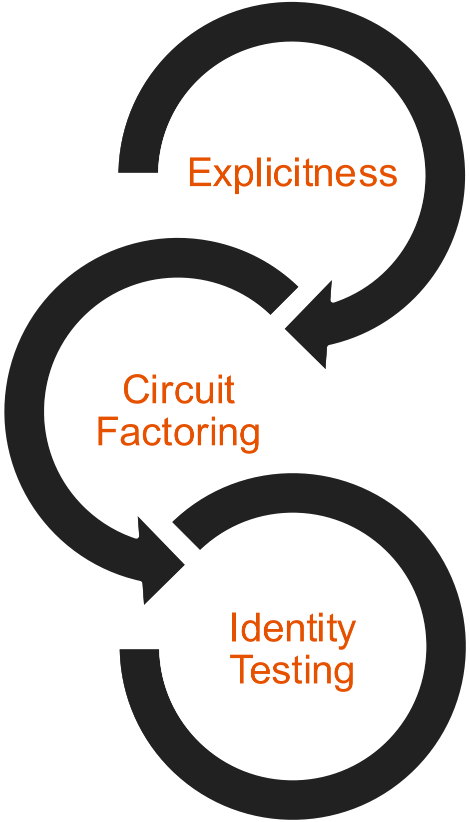
Yet another thesis which does not solve Valiant's Conjecture.

## Contributions

E: Prove that a class of polynomials is in VNP.

CF: A class of polynomials is closed under factoring.

IT: Efficiently test equivalence.



# Algebraic Approximation

Polynomial $g(\varepsilon, \boldsymbol{x})$ over $\mathbb{F}(\varepsilon)$ approximate $f(\boldsymbol{x})$

$$g(\varepsilon, \boldsymbol{x}) = f(\boldsymbol{x}) + \varepsilon \cdot Q(\varepsilon, \boldsymbol{x}).$$

where $Q(\varepsilon, \boldsymbol{x})$ over $\mathbb{F}[\varepsilon]$ is higher order error terms.

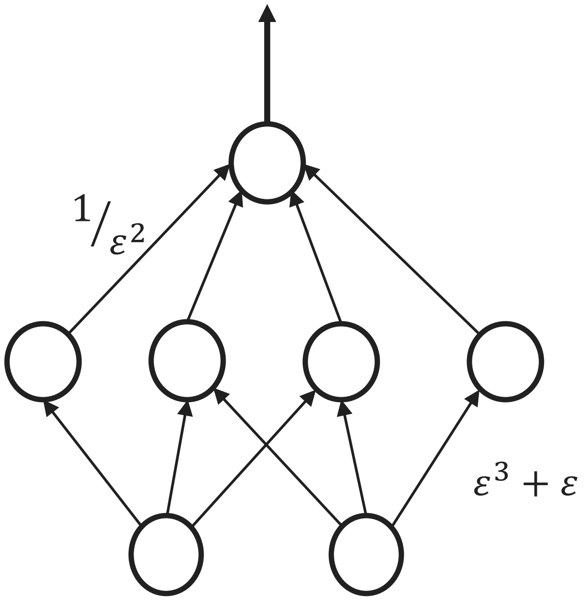
If $g$ is in circuit complexity class $\mathcal{C}$ over $\mathbb{F}(\varepsilon)$ :

- We say, $f \in \bar{\mathcal{C}}$
- $f$ may not be in $\mathcal{C}$

**Definition (Border Complexity)**

Size of the smallest circuit approximating the polynomial. Denoted by $\overline{\text{size}}(f)$.

$$g(\varepsilon, \boldsymbol{x}) = f(\boldsymbol{x}) + \varepsilon \cdot Q(\varepsilon, \boldsymbol{x})$$




$$\mathbb{F}(\varepsilon) = \left\{ {}^{p(\varepsilon)}/_{q(\varepsilon)} \,\middle|\, p, q \neq 0 \in \mathbb{F}[\varepsilon] \right\}$$

# Algebraic Approximation

**Question (Debordering)**

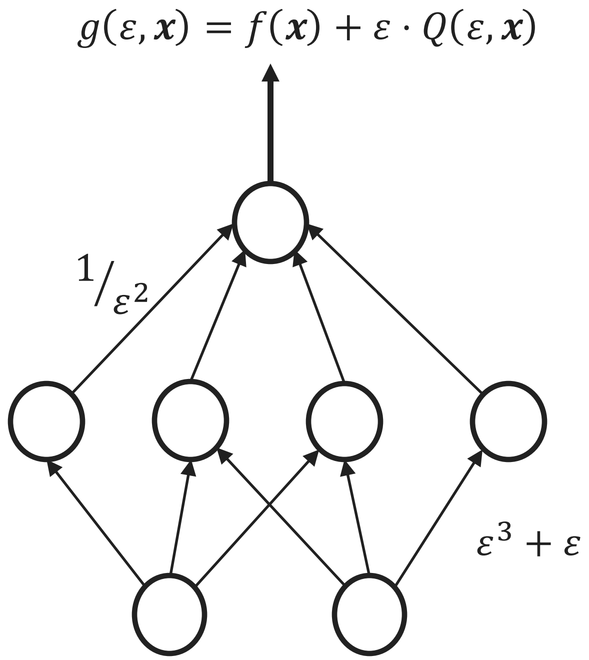
Given $\overline{\text{size}}(f) = \text{size}_{\mathbb{F}(\varepsilon)}(g)$, what is $\text{size}(f)$?

$\lim_{\varepsilon \to 0} g = f$. But circuits cannot compute limits.

Arbitrary polynomials in $\varepsilon$ are treated as free constants in circuit computing $g$.

**Bürgisser 2004**

$$\text{size}(f) \le \exp\left(\overline{\text{size}}(f)\right)$$




$\mathbb{F}(\varepsilon) = \left\{ p(\varepsilon)/q(\varepsilon) \,\middle|\, p, q \neq 0 \in \mathbb{F}[\varepsilon] \right\}$

# Border Classes

Consider a complexity class $\mathcal{C}_{\mathbb{F}}$ like VP or VNP.

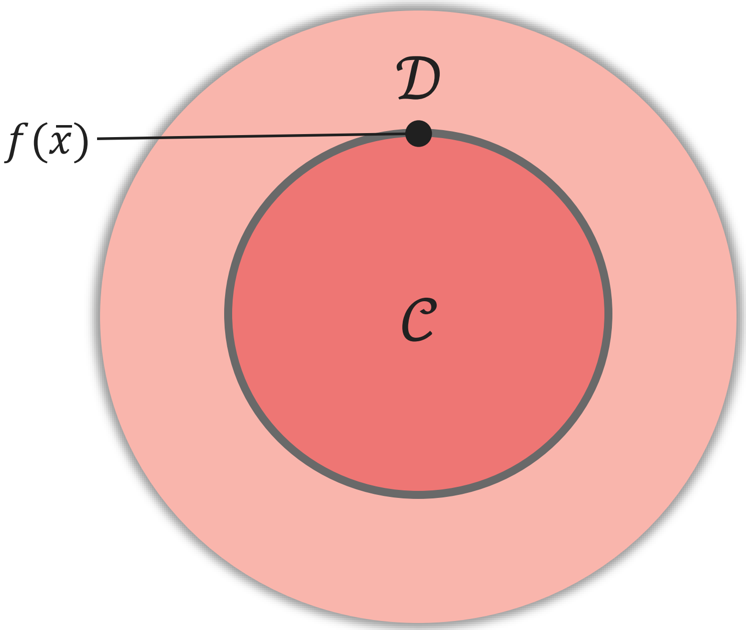
A polynomial $f \in \bar{\mathcal{C}}$,

$$g(\varepsilon, \bar{x}) = f(\bar{x}) + \varepsilon \cdot Q(\varepsilon, \bar{x}) \in \mathcal{C}_{\mathbb{F}(\varepsilon)}.$$

$f$ may not be in $\mathcal{C}_{\mathbb{F}}$.

**Border Closure**

$$\bar{\mathcal{C}} = \mathcal{C}$$




- $\mathcal{C} \subseteq \bar{\mathcal{C}}$, is trivial. The other direction is not.

# Strengthened Valiant's Conjecture

**Strengthened Conjecture**

$$\overline{\mathrm{VP}} \not\subseteq \mathrm{VNP}$$

Resolving this conjecture will prove VP ≠ VNP.

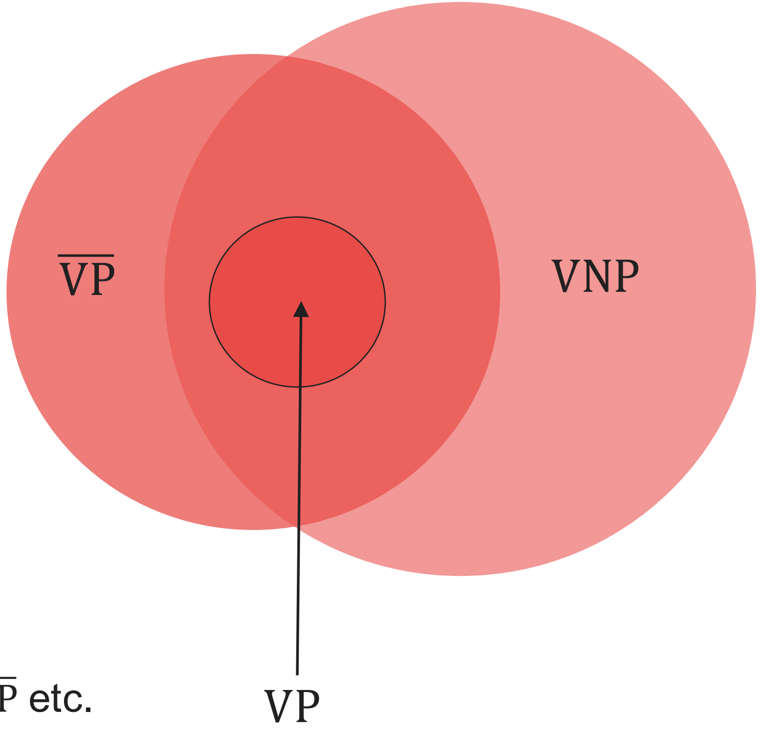
Because VP ⊆ VNP and VP ⊆ $\overline{\mathrm{VP}}$.

Natural to study the strength.

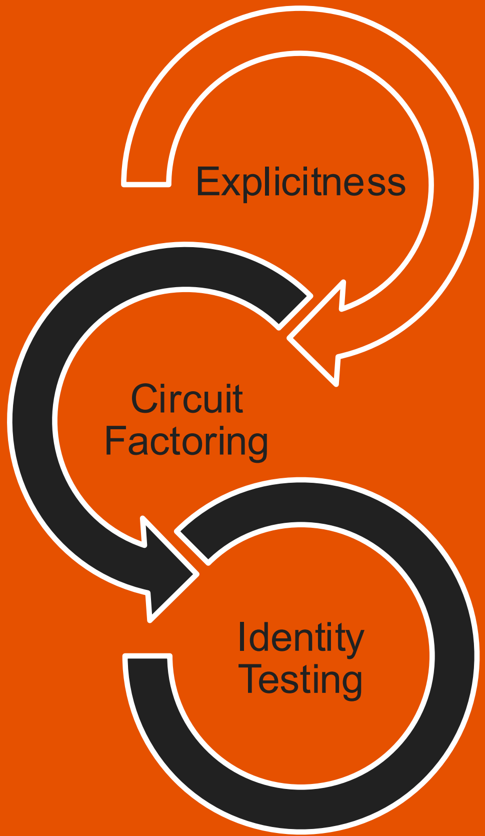
**Debordering**

$$\overline{\mathrm{VP}} \stackrel{?}{=} \mathrm{VP}$$

Question is open for most of the classes — $\overline{\mathrm{VF}}$, $\overline{\mathrm{VP}}$, $\overline{\mathrm{VNP}}$ etc.



# Explicitness



# Depth-4 circuits $\Sigma^{[k]}\Pi\Sigma\wedge$

Computes sum of product of sum of univariates.

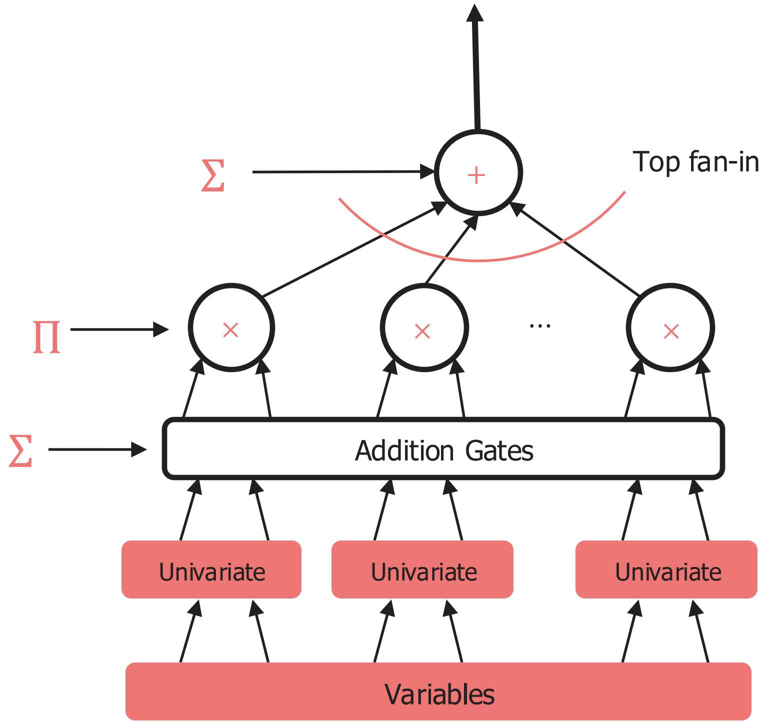
**Algebraic Branching Program (VBP)**

$$f(x_1,\ldots,x_n) = \mathrm{Det}\begin{pmatrix} & \vdots & \\ \ldots & a\cdot x_i + c & \ldots \\ & \vdots & \end{pmatrix}_{w\times w}$$

The $\mathrm{size}_{\mathrm{ABP}}(f) = \ min\ dim \ \leq \mathrm{poly}(n)$.

$$\Sigma^{[k]}\Pi\Sigma\wedge \subseteq \mathrm{VBP} \subseteq \mathrm{VNP}$$

$$\mathbb{F}[x_1,\ldots,x_n] \ni f = \sum_{i=1}^{k}\prod_{j=1}^{d}\left(g_{ij1}(x_1) + \cdots + g_{ijn}(x_n)\right)$$



# Depth-4 circuits $\Sigma^{[k]}\Pi\Sigma\wedge$

Let $f(\bar{x})$ be homogeneous of degree $d$ polynomial.

**Mrinal 2020**

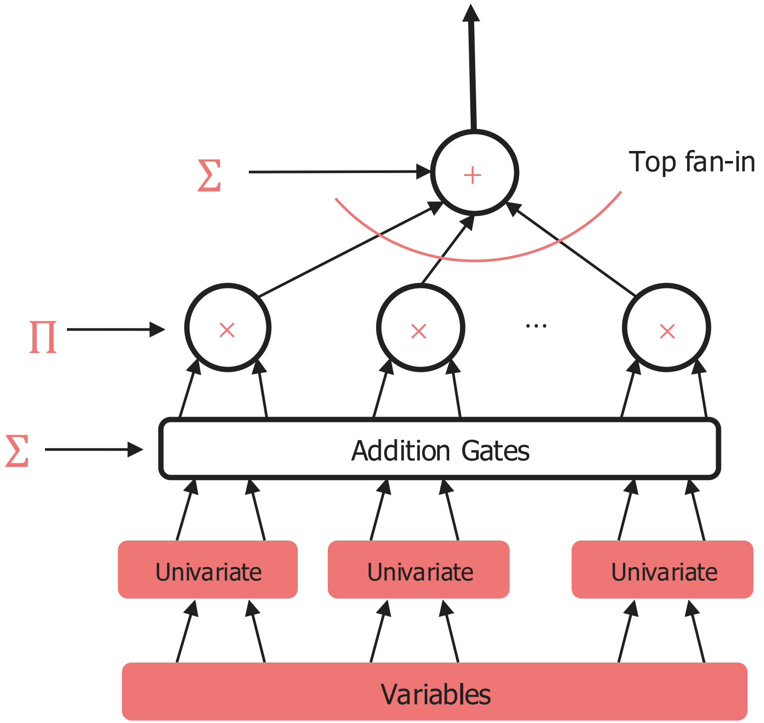
$$f(\bar{x}) \in \overline{\Sigma^{[2]}\Pi^{[D]}\Sigma}$$

Where, $D = \exp(n, d)$.

Say D= poly$(n)$. What is the size$(f)$?

Are polynomials in $\overline{\Sigma^{[k]}\Pi^{[D]}\Sigma\wedge}$ explicit?

$$\mathbb{F}[x_1, \ldots, x_n] \ni f = \sum_{i=1}^{k} \prod_{j=1}^{d} g_{ij1}(x_1) + \cdots + g_{ijn}(x_n)$$



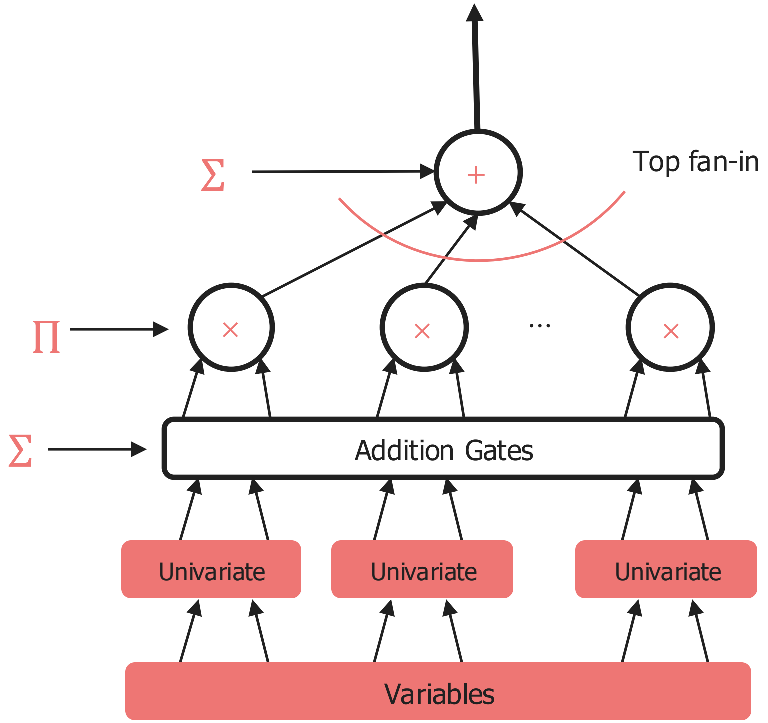
# Depth-4 circuits $\Sigma^{[k]}\Pi^{[d]}\Sigma\wedge$

$$\mathbb{F}[x_1, \dots, x_n] \ni f = \sum_{i=1}^{k} \prod_{j=1}^{d} g_{ij1}(x_1) + \dots + g_{ijn}(x_n)$$

**Dutta, D., Saxena 2021**

$$\overline{\Sigma^{[k]}\Pi^{[D]}\Sigma\wedge} \subseteq \mathrm{VBP} \subseteq \mathrm{VNP}$$

where, $D = \mathrm{poly}(n)$ and constant $k$.




The size of the depth-4 circuit is polynomial in the number of variables.

Explicitness is proved using DiDIL — Divide, Derive, Interpolate, with Limits.

# Explicit Class

## Definition (VNP)

Polynomial $f \in \mathrm{VNP}$

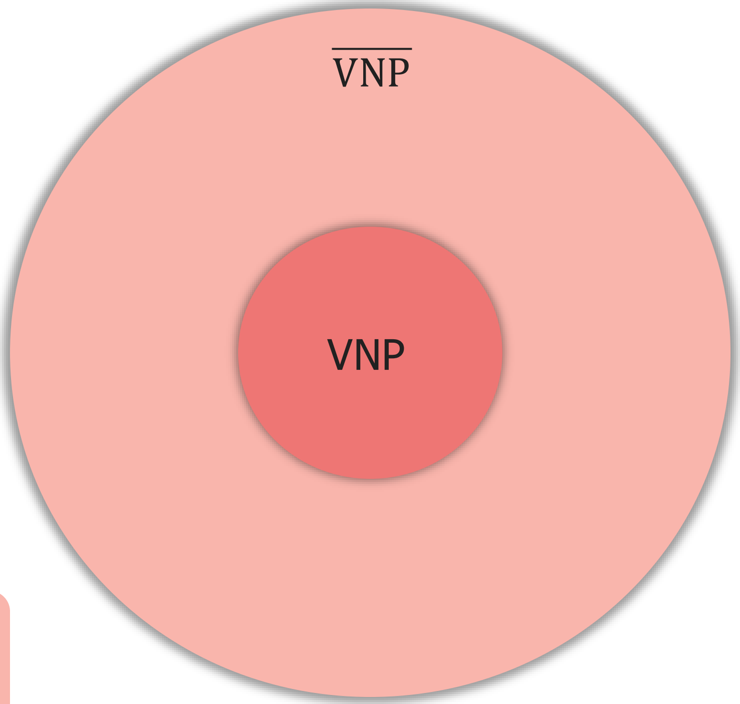
$$f(x_1, \ldots, x_n) = \sum_{\boldsymbol{a} \in \{0,1\}^m} g(x, a)$$

Where the verifier $g$ in VP and $m = \mathrm{poly}(n)$.

A class of polynomials whose coefficients can be computed efficiently, and perhaps more.

## Valiant's Criterion

If the coefficient function of a polynomial $f$ is in #P/poly. Then, $f \in \mathrm{VNP}$.



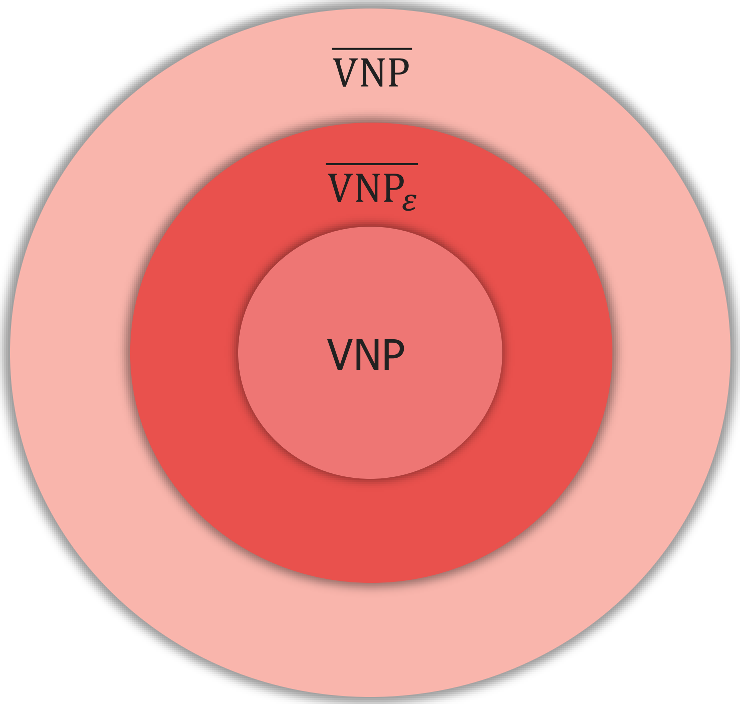
# Presentable Border

Approximating circuits use arbitrary polynomials in $\varepsilon$ of arbitrary complexity as free constant.

Although $\mathrm{size}_{\mathbb{F}[\varepsilon]}(g)$ is bounded, $\mathrm{size}_{\mathbb{F}}(g)$ is perhaps unbounded.

**Definition (Presentable $\overline{\mathrm{VNP}}$)**

Essentially the same as $\overline{\mathrm{VNP}}$, but all the $\varepsilon$ polynomial are of small size.



# Presentable is Explicit

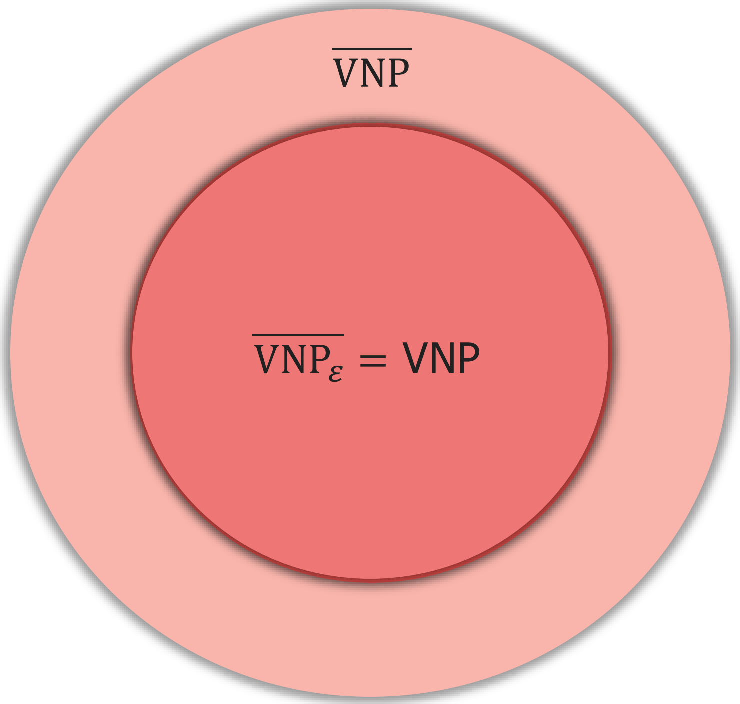
**Bhargav, Dwivedi, and Saxena 2024**

Over any finite fields, $\overline{\mathrm{VNP}_\varepsilon} = \mathrm{VNP}$.

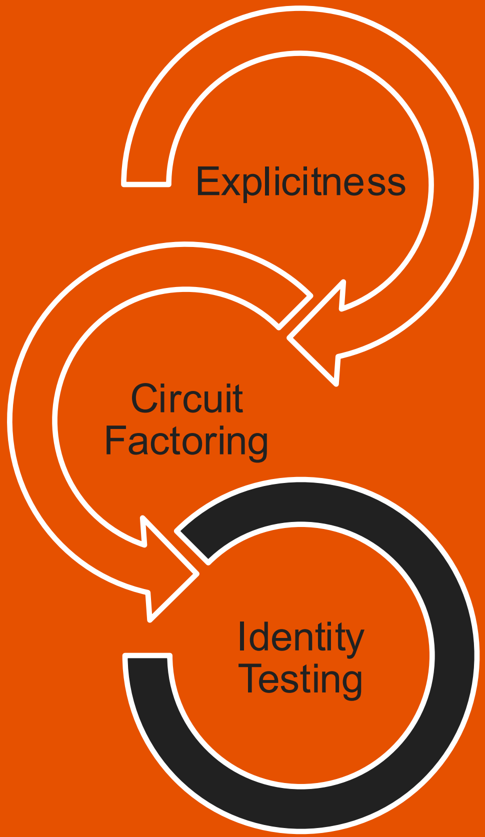
It gives a tower of containment: $\mathrm{VP} \subseteq \overline{\mathrm{VP}_\varepsilon} \subseteq \mathrm{VNP}$

**Conjecture (Presentable Separation)**

$\mathrm{VP} = \overline{\mathrm{VP}_\varepsilon} \neq \mathrm{VNP}$.



# Circuit Factoring



# VNP Factor Closure

Consider an arbitrary factor $u$ of a polynomial $f \in \mathcal{C}$.

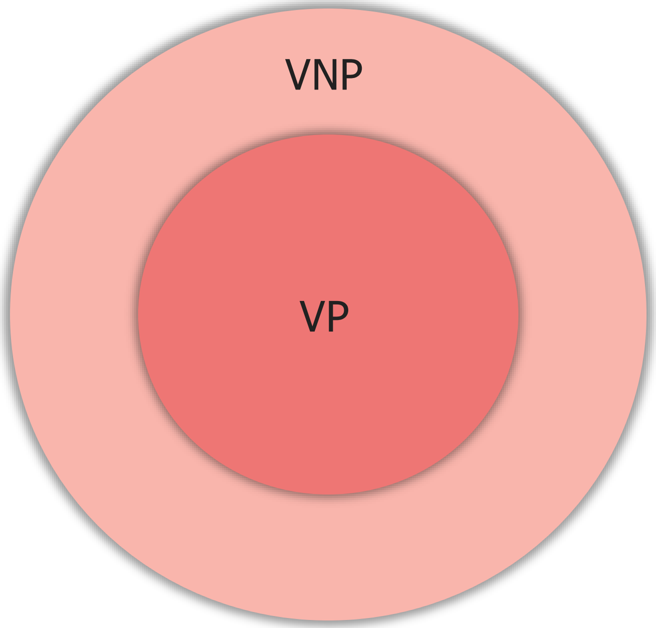
Then is $u \in \mathcal{C}$?

Bürgisser conjectured that VNP is closed under factorization.

Chou, Kumar and Solomon, 2018 proved it for characteristic zero fields.

**Bhargav, Dwivedi, and Saxena 2024**

Over any finite field, VNP is closed under factorization.




Factors of VP over finite fields are in VNP.

# Debordering Factors

Bürgisser used Border to understand the complexity of low-degree factors.

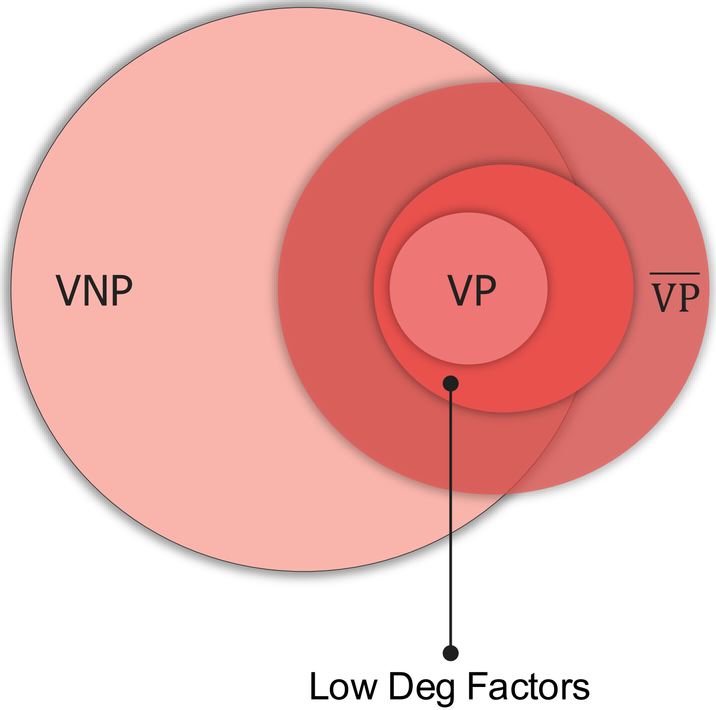
**Conjecture (Low degree factors)**

The poly($n$)-degree factors of poly($n$)-size circuits are in VP.

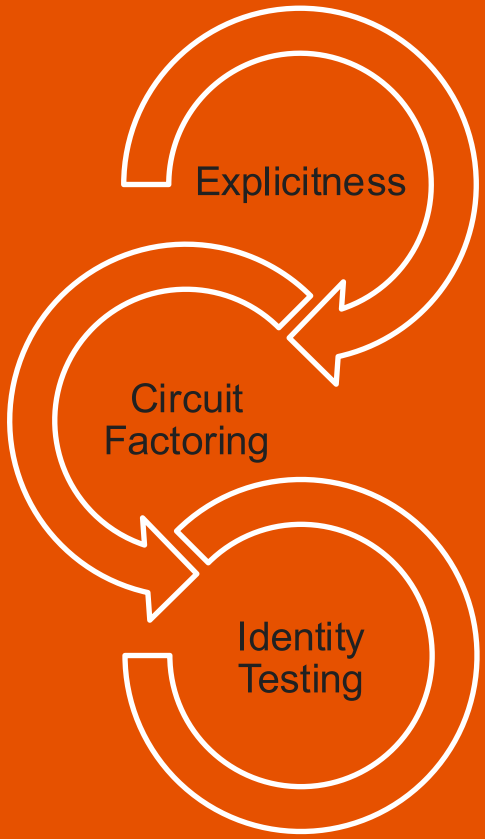
Bürgisser proved that such low-degree factors are in $\overline{\mathrm{VP}}$. We observe that they are, in fact, in $\overline{\mathrm{VP}_\varepsilon}$.

**Bhargav, Dwivedi, and Saxena 2024**

Over finite fields, low-degree factors of small-size circuits are in VNP.



# Identity Testing



# Identity Testing

Natural queries, given a polynomial $f$, include evaluation, addition, multiplication, factoring, etc.

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

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

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

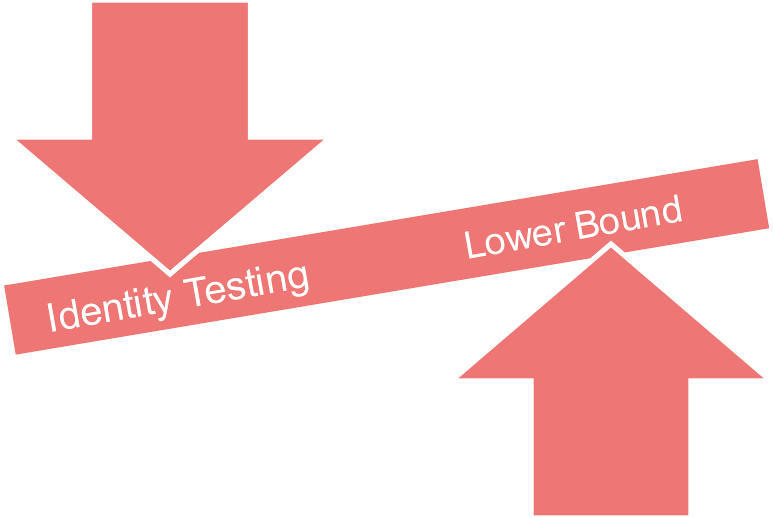
# Why do we care?

Primality Testing, Perfect Matching, Factoring,

and Reconstruction Algorithms.

Emerges naturally in complexity theory.

A simple to state, but difficult-to-solve problem.



# Efficient Randomized algorithm

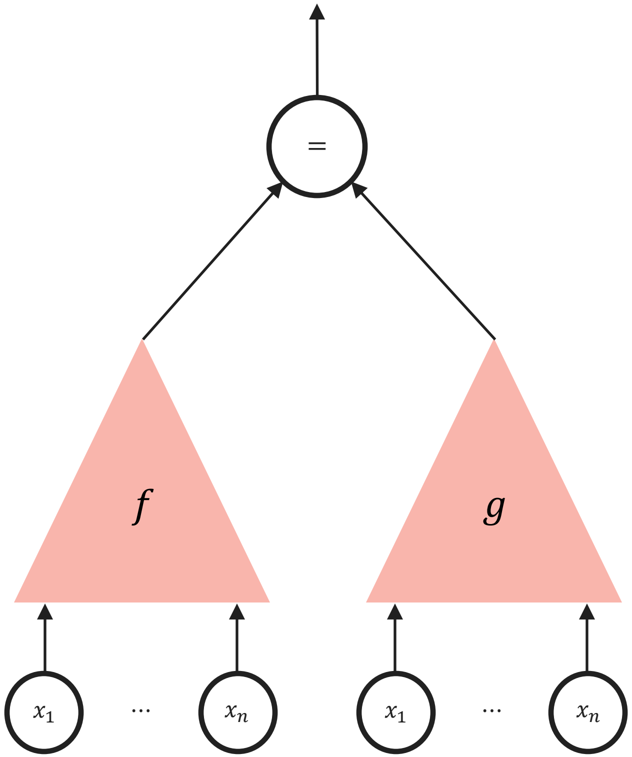
**PIT Lemma**

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 $\mathrm{poly}(d^n)$ time deterministic algorithm.



# Polynomial Identity Testing

**PIT**

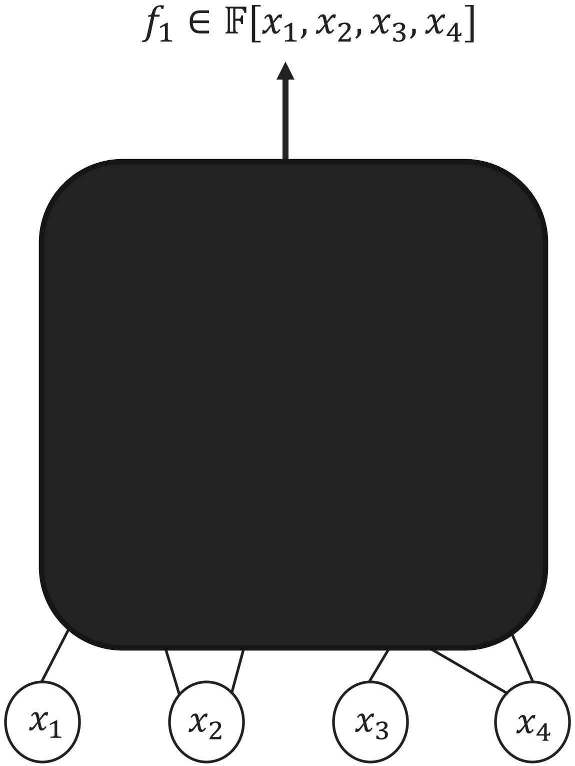
Given a circuit $C$ over a field $\mathbb{F}$, test if $C = 0$.

Blackbox: Test using evaluations only.

Whitebox: Look inside the circuit

Nothing better than exponential is known for general algebraic circuits. Constant depth circuits has SUBEXP algorithm. [LST21]

Efficient algorithms are known for only very restricted circuits.



# Depth-4 circuits

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

The restriction is special!

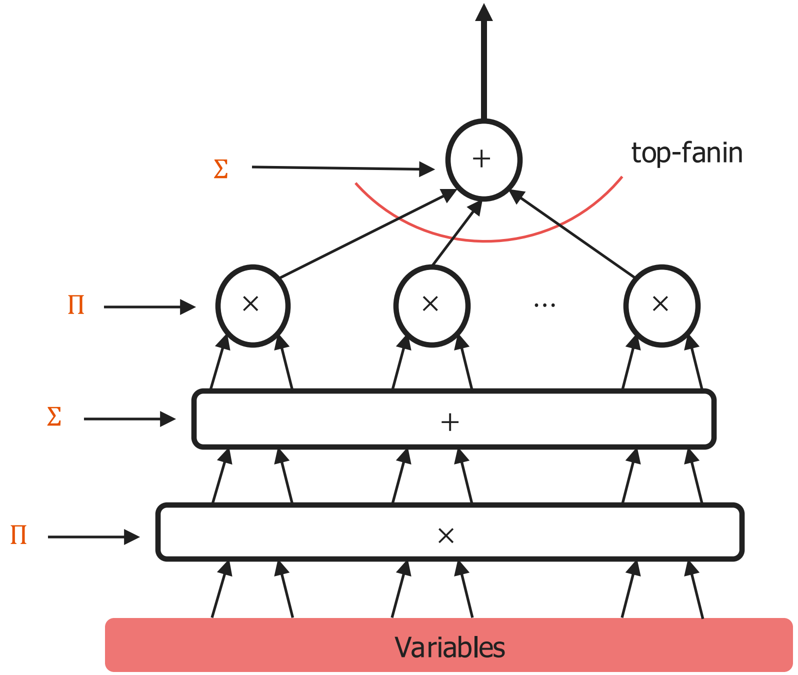
**Agrawal-Vinay**

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

**Dutta, D., Saxena 2021**

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

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

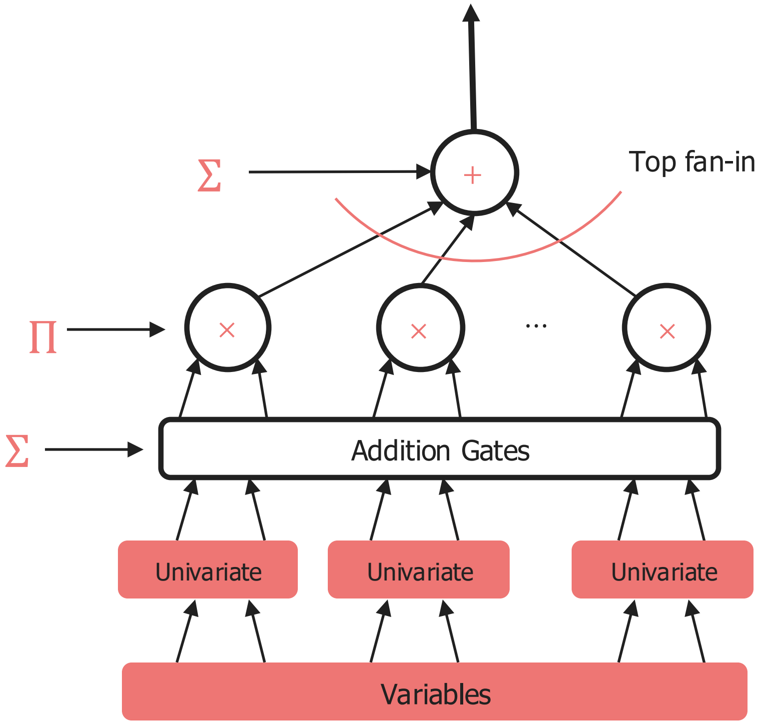


# Whitebox PIT on $\Sigma^{[k]}\Pi^{[d]}\Sigma\wedge$

**Dutta, D., Saxena 2021**

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

$$\mathbb{F}[x_1,\dots,x_n] \ni f = \sum_{i=1}^{k}\prod_{j=1}^{d} g_{ij1}(x_1)+\dots+g_{ijn}(x_n)$$




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 white box PIT.

# Border PIT

**Definition (Robust Hitting Set)**

$\mathcal{H}$ is robust hitting set for $\bar{\mathcal{C}}$ if there is a point $\bar{a} \in \mathcal{H}$ such that

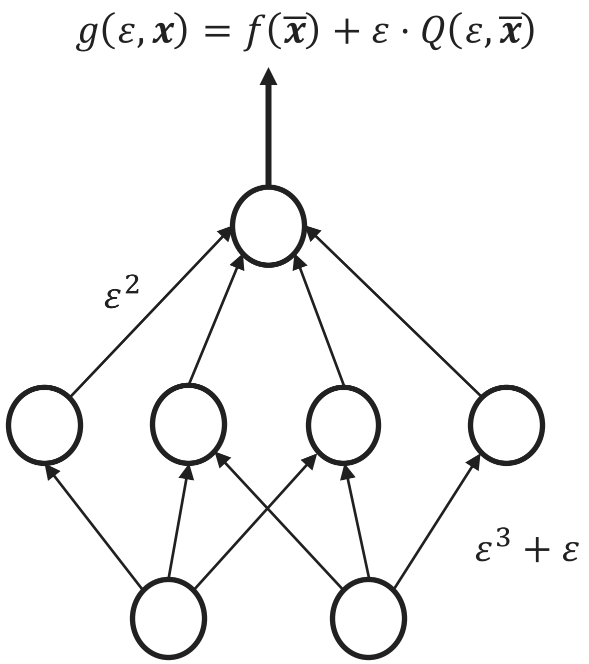
$$g(\varepsilon, \bar{a}) \neq \varepsilon \cdot h$$

where $h \in \mathbb{F}[\varepsilon]$.

The point $\bar{a}$ is a non-zeroness certificate — $f(\bar{a}) \neq 0$.

$g(\varepsilon, \bar{a}) \neq 0$ does not suffice; hence we need robustness.

DiDIL de-borders $\overline{\Sigma^{[k]}\Pi\Sigma\wedge}$, and DiDI de-randomize PIT on $\Sigma^{[k]}\Pi\Sigma\wedge$.



# PIT on $\overline{\Sigma^{[k]}\Pi^{[d]}\Sigma\wedge}$

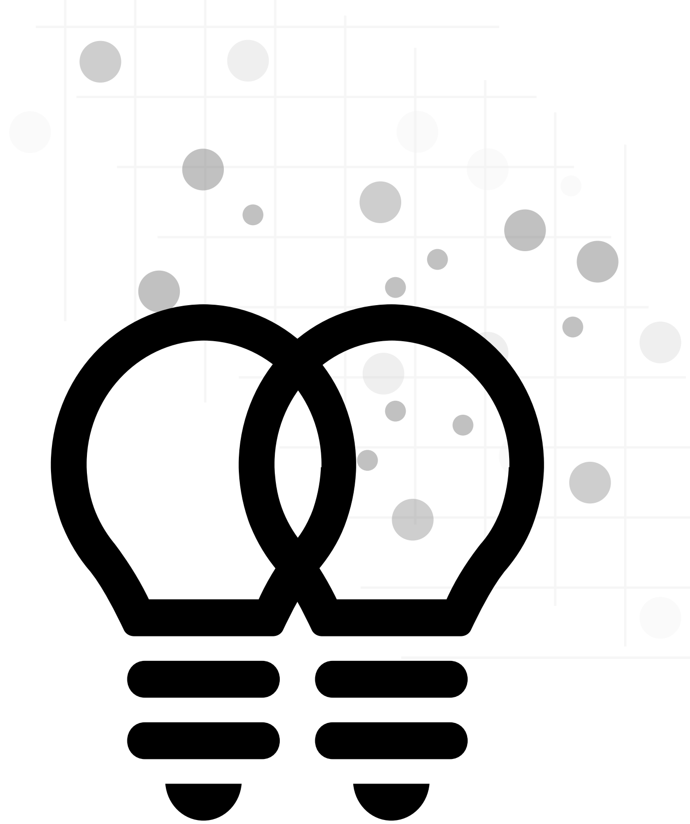
**Dutta, D., Saxena 2021**

Quasipolynomial time hitting set of $\overline{\Sigma^{[k]}\Pi\Sigma\wedge}$, for any constant $k$.

Although we could not de-border $\overline{\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}}$, but could de-randomize.

**Dutta, D., Saxena 2021**

Quasipolynomial time hitting set of $\overline{\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}}$, for any constant $k$ and $\delta$.



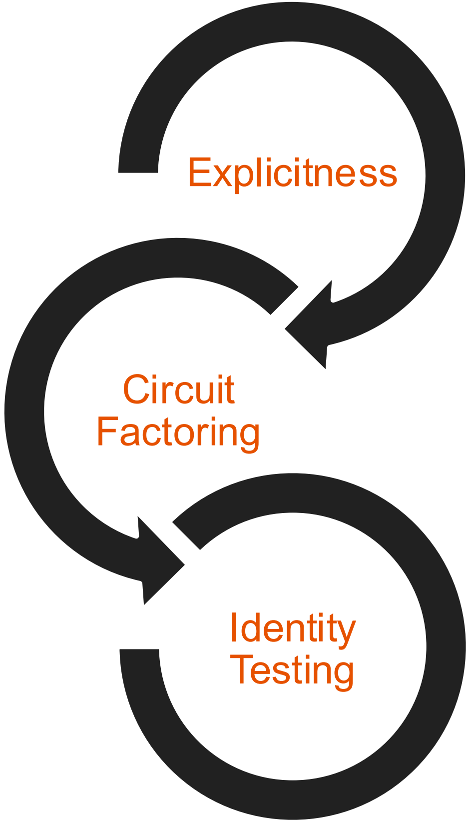
# Conclusion

# Conclusion

De-bordered $\overline{\Sigma^{[k]}\Pi^{[d]}\Sigma\wedge}$ using DiDIL. And presentable border class $\overline{\mathrm{VNP}_{\varepsilon}}$ is explicit over finite fields.

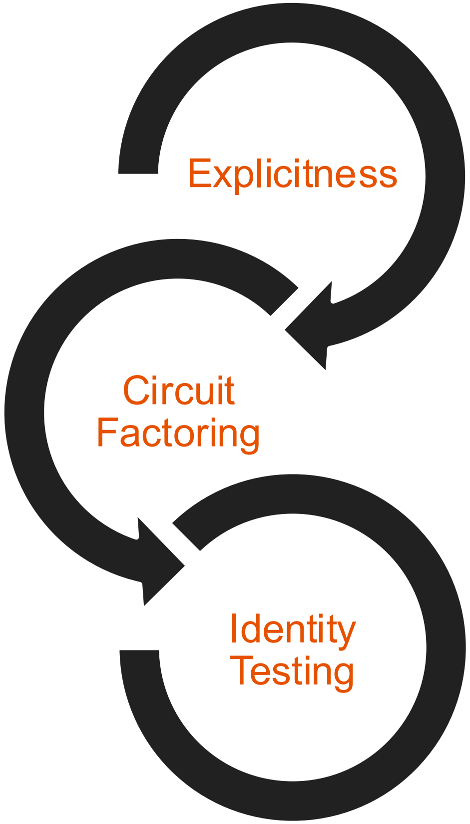
Factor closure of VNP over finite fields. And de-bordering low-degree factors of small size circuits.

White-box identity testing of $\Sigma^{[k]}\Pi^{[d]}\Sigma\wedge$ and border PIT of $\overline{\Sigma^{[k]}\Pi\Sigma\wedge}$ and $\overline{\Sigma^{[k]}\Pi\Sigma\Pi^{[\delta]}}$.



## Conclusion

# Treading the Borders

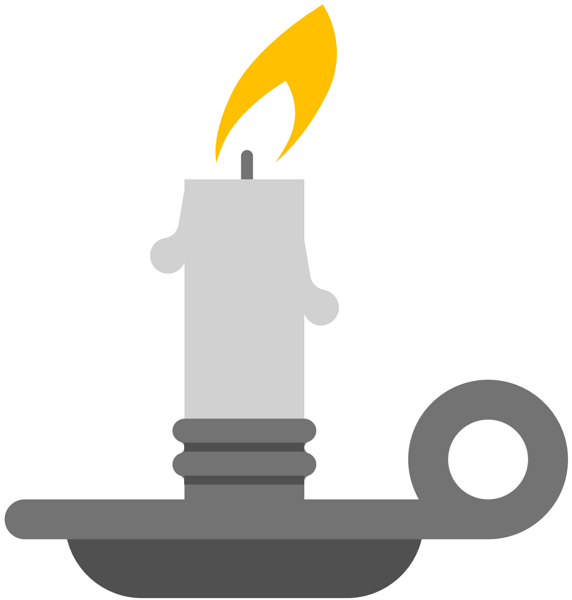


# Open Problems

Improve De-bordering upper bounds. Investigate the extent of de-bordering that is possible with presentability.

De-bordering helped in circuit factoring and identity testing. There could be hidden direct connections between the problems.

Solve Valiant's conjecture and PIT completely. It's high time now!



# Thanks to …

## Examiners and Committee Members

- Prof Nitin Saxena (Advisor)
- Prof Ramprasad Saptharishi
- Prof Dootika Vats
- Prof Sayak Ray Chowdhury
- Prof Satyadev Nandakumar

## Collaborators

- Dr. Pranjal Dutta (NUS)
- C.S. Bhargav (CSE, IIT K)
- Prof Radu Curticapean (UR, Germany)
- Prof Nutan Limaye (ITU)

## Endless list of incredible people in

## ACT fraternity.

## KD 213

- My Seniors and fellow lab mates

## Friends

- Avideep and Soumya
- Mahesh, Bhargav, and Muzafar
- My seniors

## Family

- Parents and my brothers
- My adorable nephews and nieces

## Shweta

- And her unwavering support