Treading the Border Complexity and Identity Testing Paradigms.

State of The Art Seminar

Prateek Dwivedi

Prelude

Polynomials

- Algebraic Objects $f(\bar{x}) \in \mathbb{F}[x_1, \ldots, x_n]$.
  - $\deg f = d$. Then, $\sum_j e_j \le d$.
- A class of functions which has many classical applications.

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

Question

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

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

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

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

- To use algebraic tools for our aid, we need a robust computational model for polynomials.

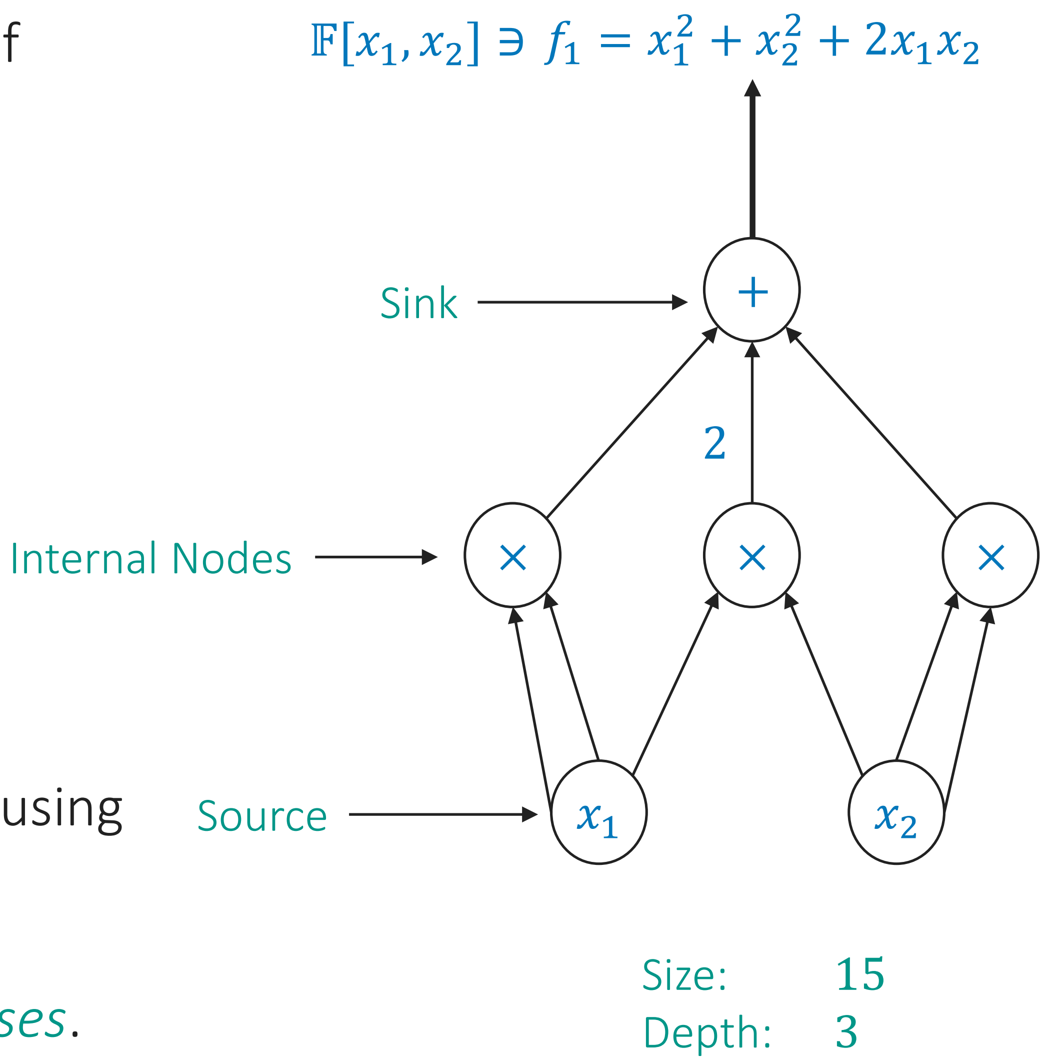
Algebraic Circuits

- Directed Acyclic Graph. Compact representation of polynomials.
- Resources: Size and Depth

Definition (Algebraic Complexity)

Size of the smallest circuit computing the polynomial. Denoted by $\mathbf{size}(f)$.

- Valiant (1977) formalized the notion computation using Algebraic Circuits.
- Circuit resources define *Algebraic Complexity Classes*.



Algebraic Circuits

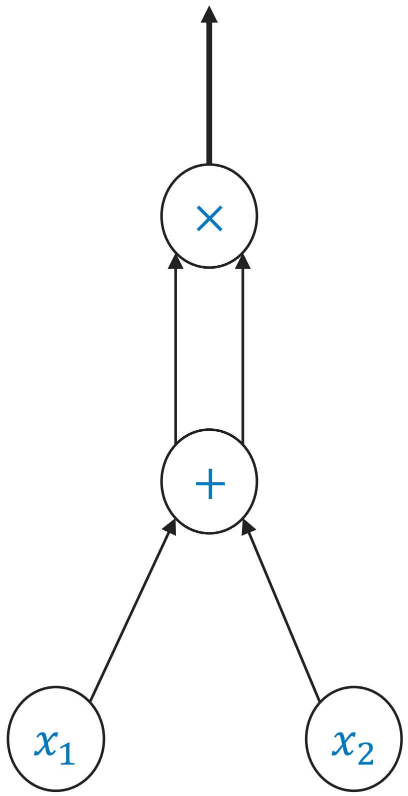
- Directed Acyclic Graph. Compact representation of polynomials.
- Resources: Size and Depth

Definition (Algebraic Complexity)

Size of the smallest circuit computing the polynomial. Denoted by $\mathbf{size}(f)$.

- Valiant [Val77] formalized the notion computation using Algebraic Circuits.
- Circuit resources define *Algebraic Complexity Classes*.

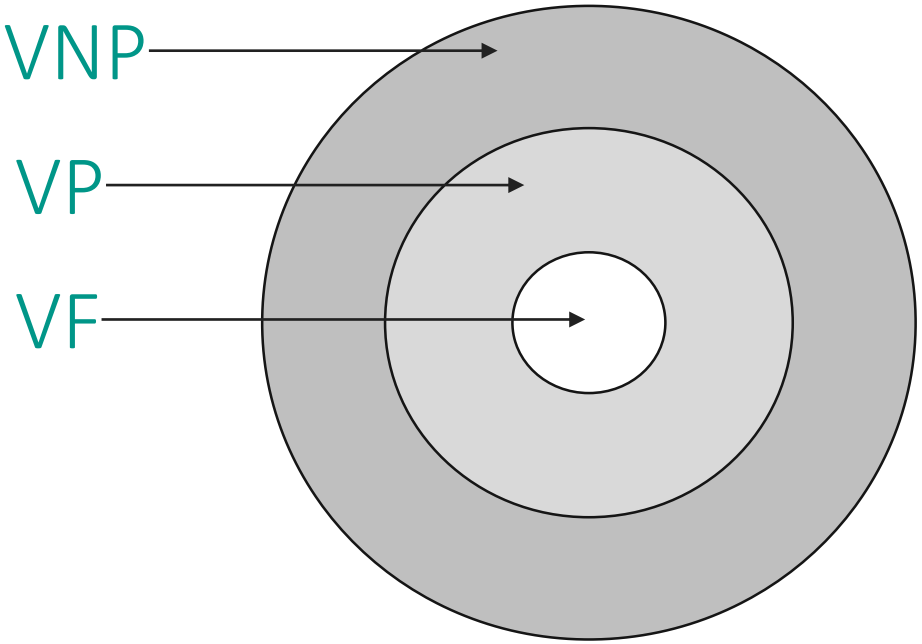
$$\mathbb{F}[x_1, x_2] \ni f_1 = x_1^2 + x_2^2 + 2x_1x_2 = (x_1 + x_2)^2$$



Size: 8
Depth: 3

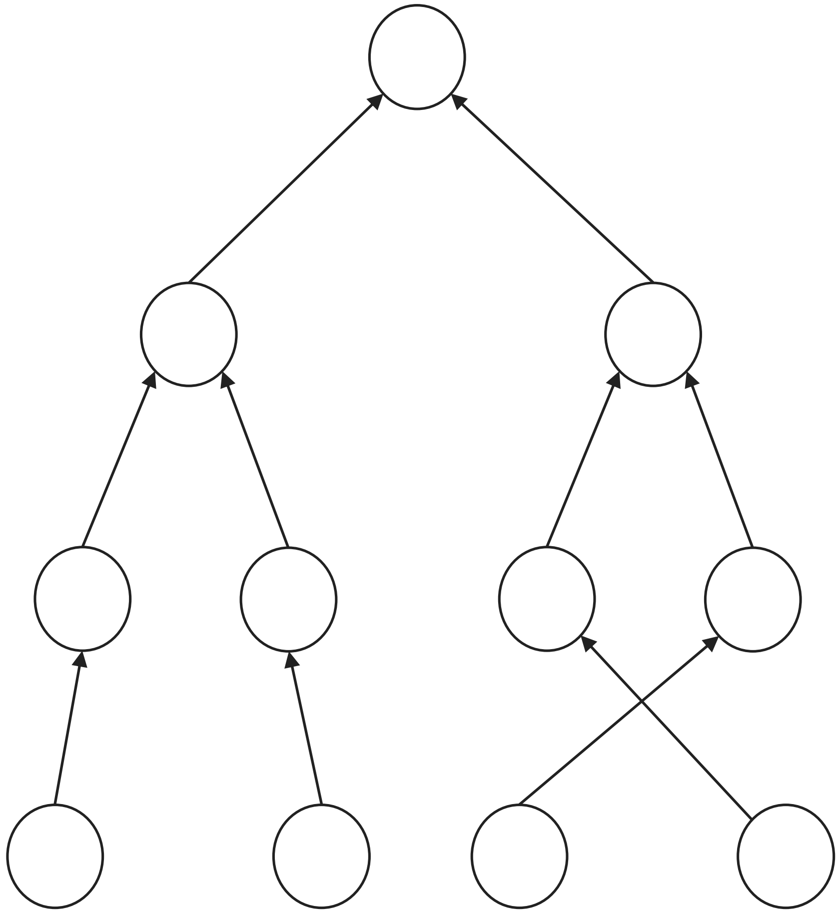
Algebraic Complexity Classes

- VP: Easy polynomials.
  - n-variate polynomials of poly(n) degree and poly(n) circuit complexity.
  - Example: Determinant.
- VNP: Hard polynomials
  - $\sum$ VP, exponential sum.
  - Example: Permanent.
- VF: Easy polynomials computable by *Formulas*.
  - Formulas are circuits without reuse of output of nodes.



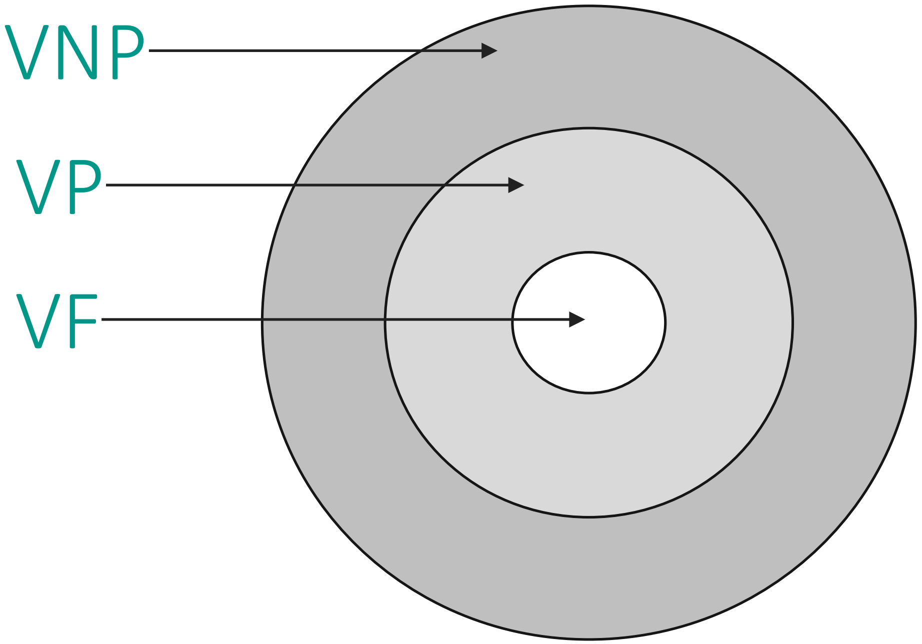
Algebraic Complexity Classes

- VP: Easy polynomials.
  - n-variate polynomials of poly(n) degree and poly(n) circuit complexity.
  - Example: Determinant.
- VNP: Hard polynomials
  - $\sum$ VP, exponential sum.
  - Example: Permanent.
- VF: Easy polynomials computable by *Formulas*.
  - Formulas are circuits without reuse of output of nodes.



Algebraic Complexity Classes

- VP: Easy polynomials.
  - n-variate polynomials of poly(n) degree and poly(n) circuit complexity.
  - Example: Determinant.
- VNP: Hard polynomials
  - $\sum$ VP, exponential sum.
  - Example: Permanent.
- VF: Easy polynomials computable by *Formulas*.
  - Formulas are circuits without reuse of output of nodes.



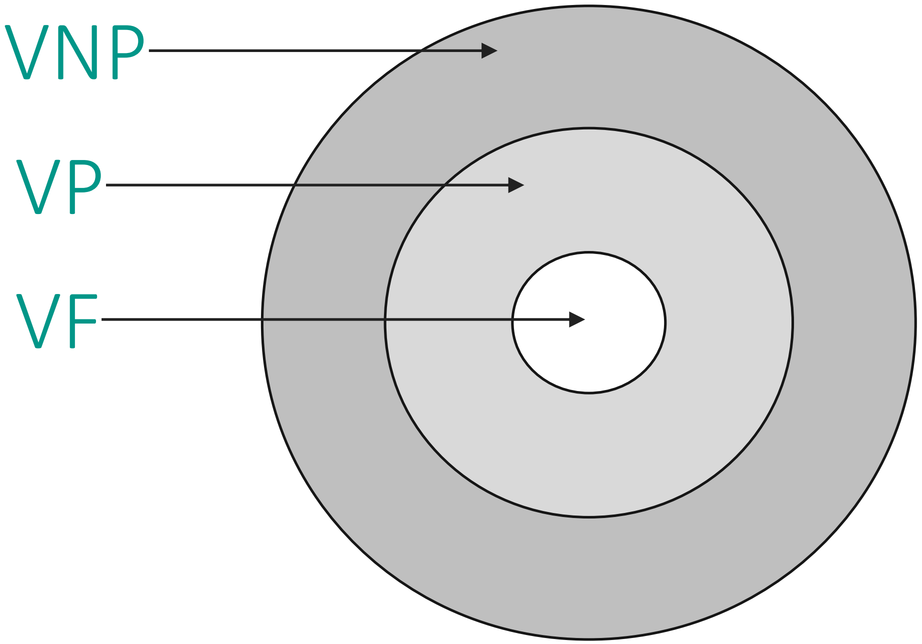
Valiant's Conjecture

Valiant's Conjecture

VP $\neq$ VNP

- To resolve it, show that Permanent is not an easy polynomial.

$$\mathrm{Perm}_n = \sum_{\sigma \in S_n} x_{1\sigma(1)} \cdot x_{2\sigma(2)} \cdots x_{n\sigma(n)}$$



- More structure means easier to prove separation.
  - Since algebra has more structure than Boolean, VP vs VNP should be 'easier' than P vs NP.

Evidences for Valiant Conjecture

Bürgisser 1998

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

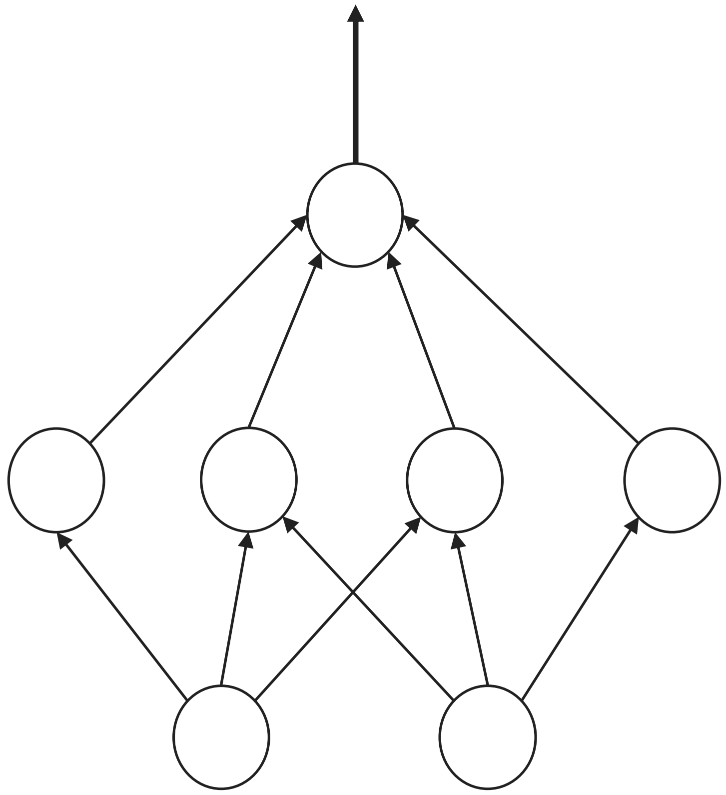
- VP ≠ VNP is consistent with our belief P/poly ≠ NP/poly.
- In a relationless world they are separated.

Hrubeš, Wigderson, Yehudayoff 2010

In non-associative, commutative world VP ≠ VNP

Dawar, Wilsenach 2020

In symmetric circuits, VP ≠ VNP



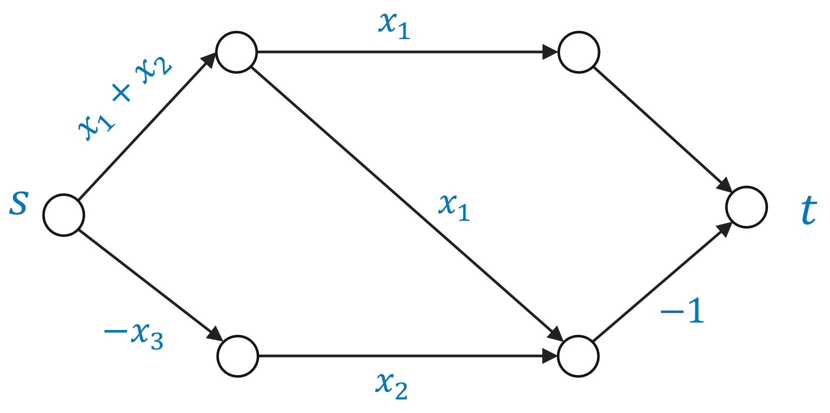
**Assuming Generalized Riemann Hypothesis*

Algebraic Branching Programs (ABP)

- Layered directed Acyclic Graph.
  - Edge Labels are linear polynomials in input variables.
- Another compact representation of polynomials.
- Resources: Size, Width, and Depth
- Complexity: Size of the smallest ABP computing the polynomial.
- **VBP**: Easy polynomials computable by small size ABP.

$$f = \sum_{path\ \gamma : s \to t} wt(\gamma)$$

Product of edge weights



$f = x_2 x_3$

Algebraic Branching Programs

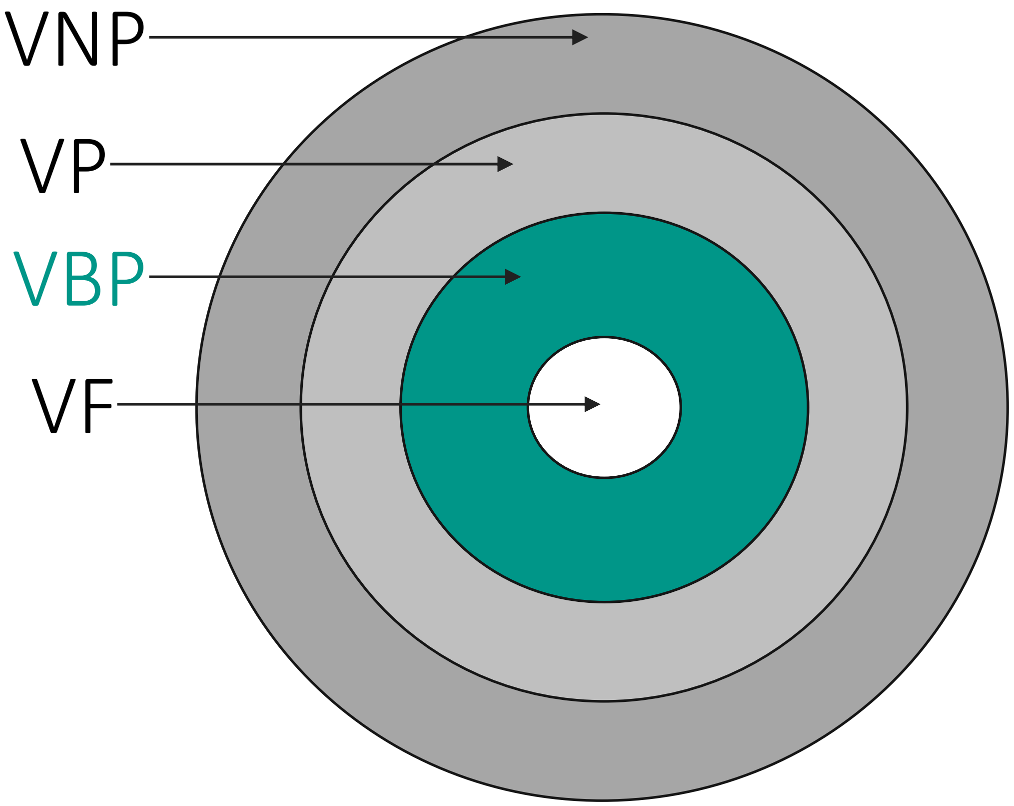
Nisan 1991

VF ⊆ VBP ⊆ VP

- ABP is a restriction on the circuit.
- More such interesting restriction?
- VBP_k: Bounded width ABPs.

Ben-Or and Cleve 1992

$\mathrm{VBP}_2 \neq \mathrm{VBP}_3 = \mathrm{VBP}_k =$ VF ⊆ VBP ⊆ VP



Algebraic Branching Programs

Nisan 1991

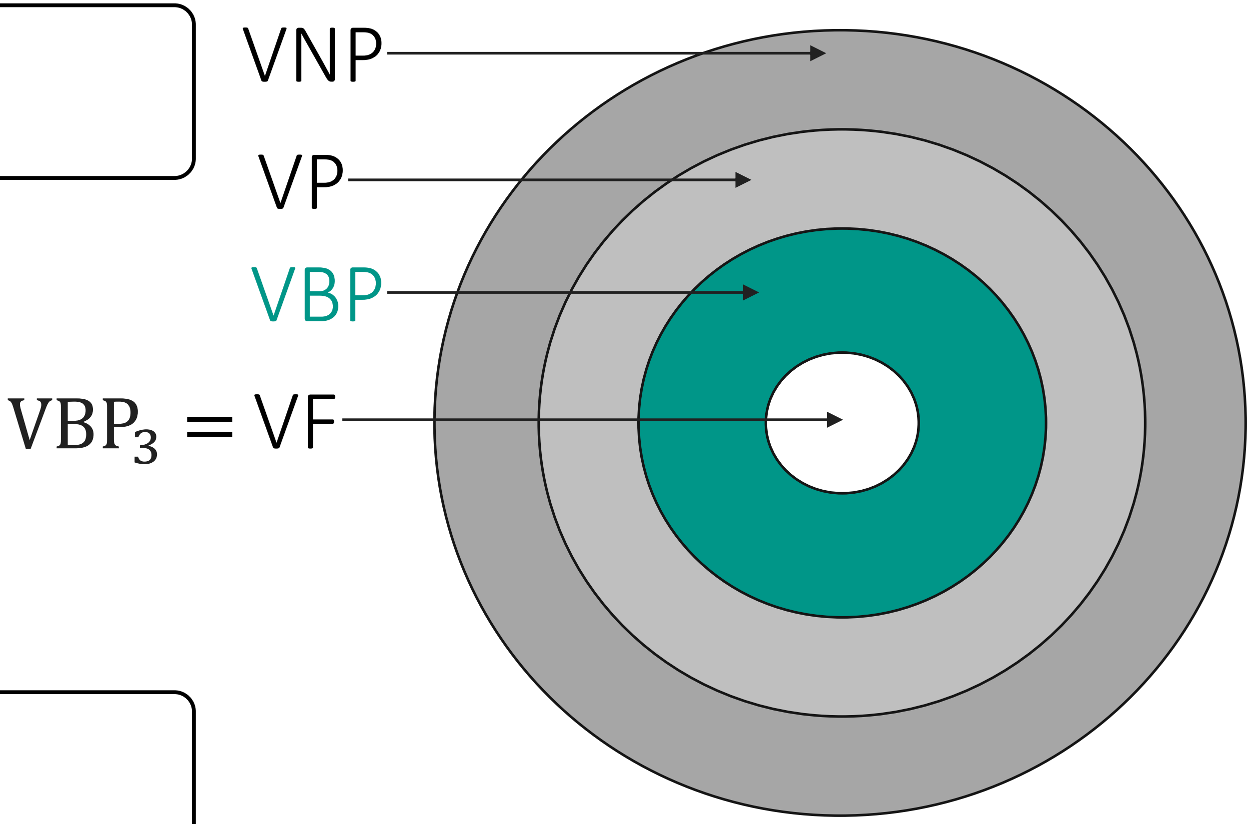
$\mathrm{VF} \subseteq \mathrm{VBP} \subseteq \mathrm{VP}$

- ABP is a restriction on the circuit.
- More such interesting restriction?
- VBP_k: Bounded width ABPs.

Ben-Or and Cleve 1992

$\mathrm{VBP}_2 \neq \mathrm{VBP}_3 = \mathrm{VBP}_k = \mathrm{VF} \subseteq \mathrm{VBP} \subseteq \mathrm{VP}$

- Strict containment is Open.



Motivating Example

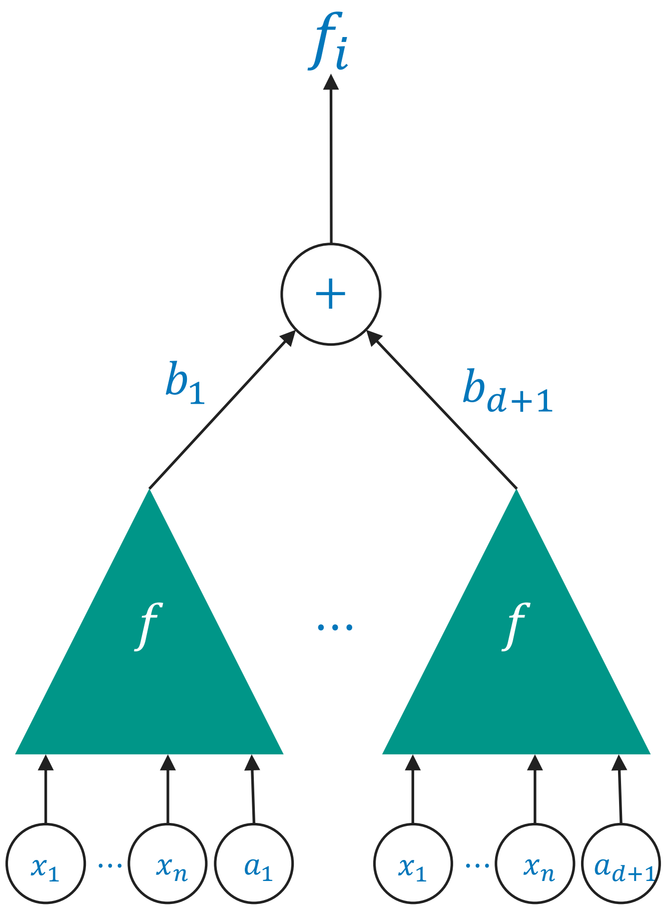
- Let C compute polynomial $f(\bar{x}, y) \in \mathbb{F}[x_1, \dots, x_n, y]$.
  - $\deg_y(f) = d$.

$$f(\bar{x}, y) = f_0(\bar{x}) + f_1(\bar{x}) \cdot y + \cdots + f_d(\bar{x}) \cdot y^d$$

Interpolation

For all $i \in [d]$, $\mathrm{size}(f_i) \leq \mathrm{size}(f) \cdot (d+1)$

- Each term is linear combination of $f(\bar{x}, a_i)$.
- All the coefficients can be extracted in size $\mathrm{O}(\mathrm{size}(f) \cdot d^2)$.
- If $f \in \mathrm{VP}$, then $f_i \in \mathrm{VP}$.



Motivating Example

- Consider a polynomial $f(\bar{x}) \in \mathbb{F}[x_1, \dots, x_n]$.
  - $\deg(f) = d$
- Let p be a positive integer.

$$p = \min_{\bar{a}} \left(\sum_{i \in [n]} a_i \right)$$

$$f(\bar{x}) = \sum_{\bar{a} \in \mathrm{supp}(f)} C_{\bar{a}} \cdot x_1^{a_1} x_2^{a_2} \dots x_n^{a_n}$$

$$h(\bar{x}) = \sum_{|\bar{b}|=p} C_{\bar{b}} \cdot x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n}$$

Interpolation

$$\mathrm{size}(h) \leq \mathrm{O}(\mathrm{size}(f) \cdot d^2)$$

Motivating Example

- We can do better if small error is tolerable.
- Consider a polynomial $g \in \mathbb{F}(\varepsilon)[\bar{x}]$:

$$g(\varepsilon, \bar{x}) = \varepsilon^{-p} \cdot f(\varepsilon \cdot x_1, \dots, \varepsilon \cdot x_n)$$

$$= \sum_{\bar{a}} C_{\bar{a}} \cdot \varepsilon^{\sum a_i - p} \cdot \bar{x}^{\bar{a}}$$

$$= h(\bar{x}) + O(\varepsilon)$$

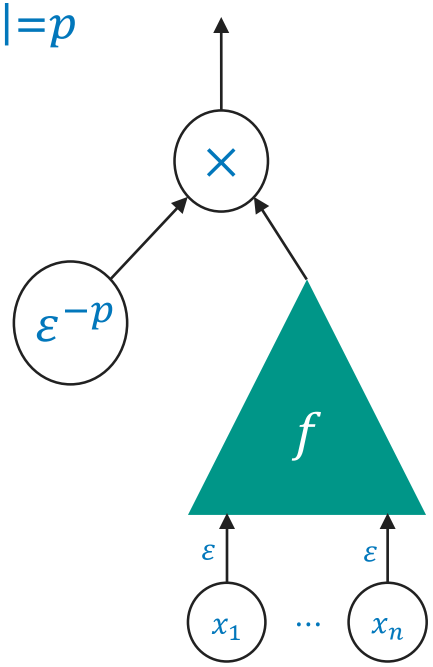
Approximation

$$\mathrm{size}(g) = \overline{\mathrm{size}}(h) \le O\big(\mathrm{size}(f)\big)$$

- Recall, $\mathrm{size}(h) \le O(\mathrm{size}(f) \cdot d^2)$.

$$f(\bar{x}) = \sum_{\bar{a} \in \mathrm{supp}(f)} C_{\bar{a}} \cdot x_1^{a_1} x_2^{a_2} \dots x_n^{a_n}$$

$$h(\bar{x}) = \sum_{|\bar{b}| = p} C_{\bar{b}} \cdot x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n} \quad + O(\varepsilon)$$



Border Complexity

Algebraic Approximation

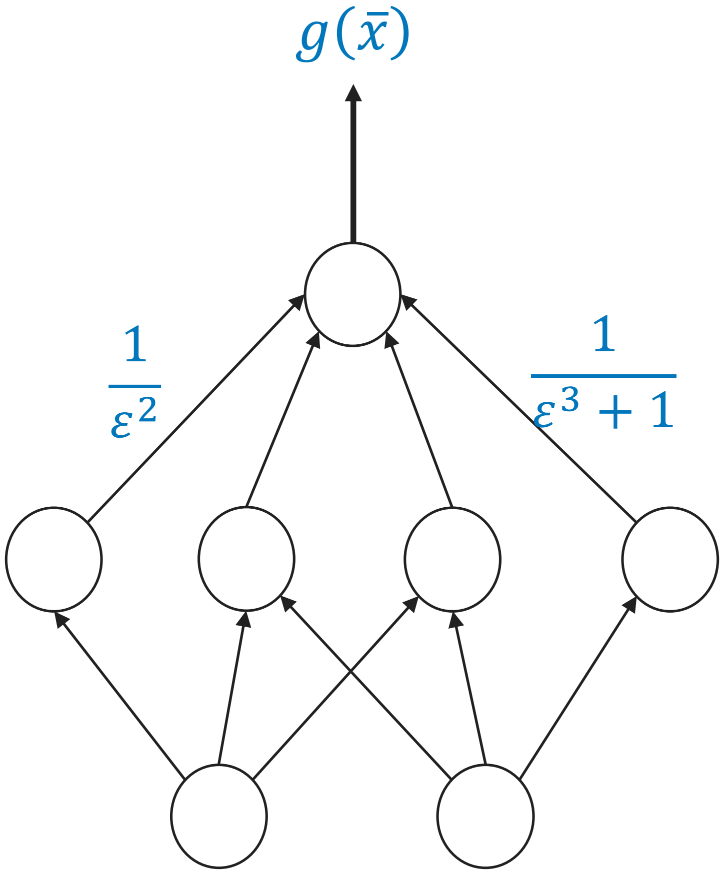
- A polynomial $g(\varepsilon,\bar{x}) \in \mathbb{F}(\varepsilon)[x_1,\dots,x_n]$ approximate $f(\bar{x}) \in \mathbb{F}[x_1,\dots,x_n]$

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

  - Where, $Q(\varepsilon,\bar{x}) \in \mathbb{F}[\varepsilon][\bar{x}]$.
- 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 $\overline{\text{size}}(f)$.



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

Algebraic Approximation

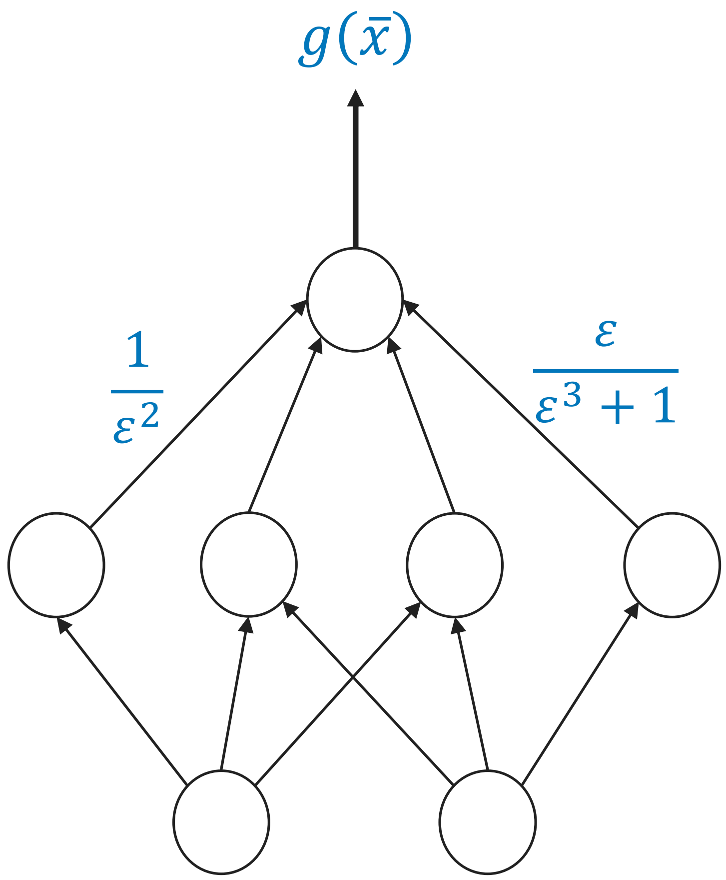
- Give a circuit which computes $g(\varepsilon, \bar{x})$ such that

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

Question

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

- Evaluate at $\varepsilon = 0$.
  - Not legal due to $1/\varepsilon$ terms in the circuit.
- $\lim_{\varepsilon \to 0} g = f$.
  - But circuits cannot compute limits.



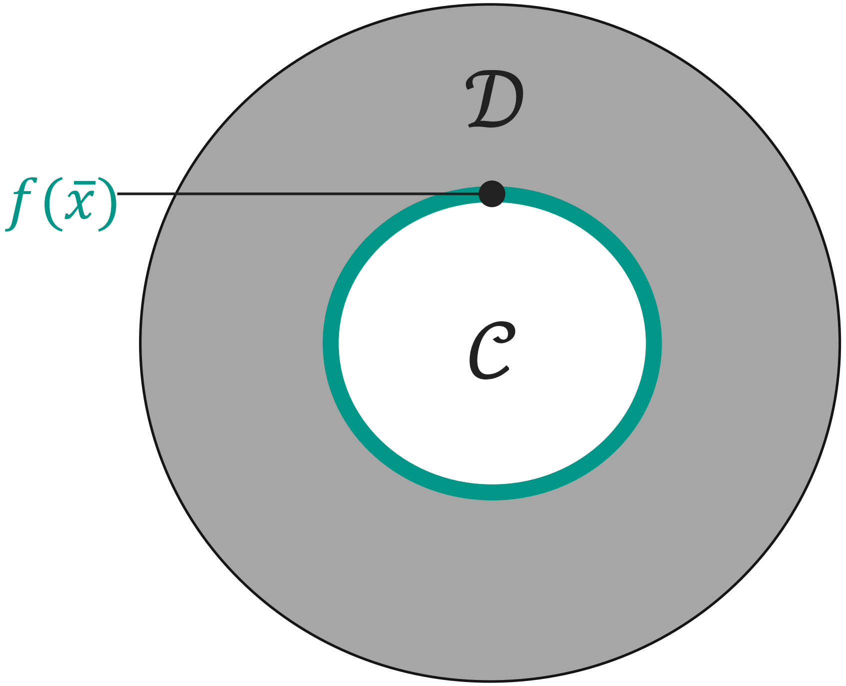
$$\mathbb{F}(\varepsilon) = \left\{ {p(\varepsilon)}/{q(\varepsilon)} \,\middle|\, p, q \neq 0 \in \mathbb{F}[\varepsilon] \right\}$$

Algebraic Closure

- Consider a complexity class $\mathcal{C}_{\mathbb{F}}$. E.g. VBP, VP, VNP etc.
- A polynomial $f(\bar{x}) \in \bar{\mathcal{C}}$, if there is a $g(\varepsilon, \bar{x}) \in \mathcal{C}_{\mathbb{F}(\varepsilon)}$ such that

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

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



Approximative Closure

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

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

Strengthened Valiant's Conjecture

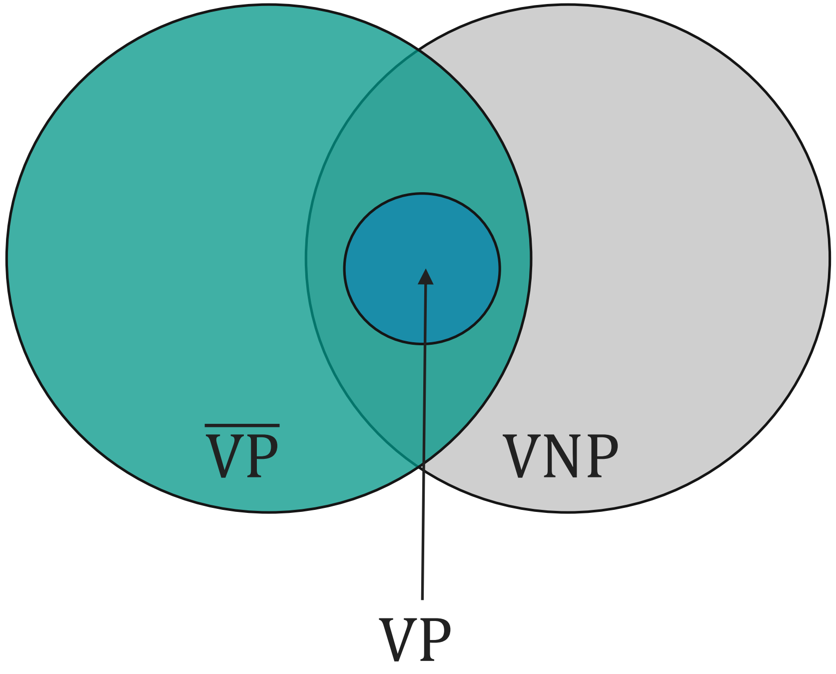
Strengthened Valiant's Conjecture

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

- Resolving this conjecture would imply 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. E.g. $\overline{\mathrm{VF}}$, $\overline{\mathrm{VP}}$, $\overline{\mathrm{VNP}}$ etc

Debordering using Interpolation

- Consider a polynomial $f(\bar{x}) \in \mathbb{F}[x_1, \ldots, x_n]$ such that
  - $\overline{\text{size}}(f) = s.$

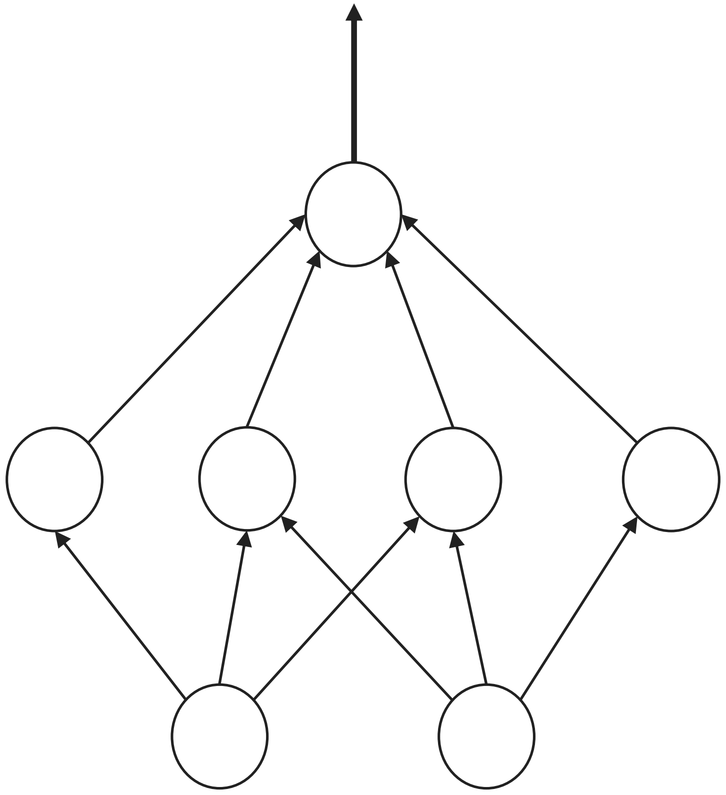
$$g(\varepsilon, \bar{x}) = g_0 + g_1 \cdot \varepsilon + g_2 \cdot \varepsilon^2 + \cdots + g_M \cdot \varepsilon^M$$

Bürgisser 2004, 2020

$$M = O\left(2^{s^2}\right)$$

- Interpolate to get $g_0 = f(\bar{x})$.
  - $\text{size}(f) = \exp(\overline{\text{size}}(f))$

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

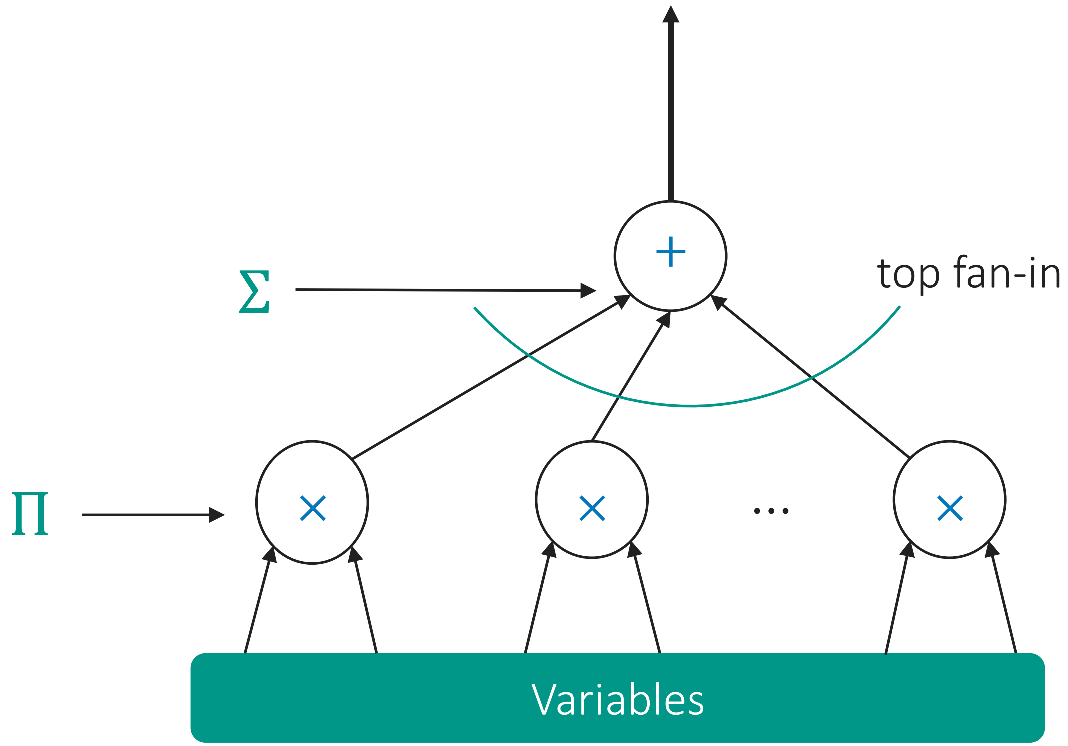


$\overline{\text{size}}(f) \leq \text{size}(f) \leq \exp(\overline{\text{size}}(f))$

Known Debordering Results

- $\overline{\Sigma^{[s]}\Pi} = \Sigma^{[s]}\Pi$

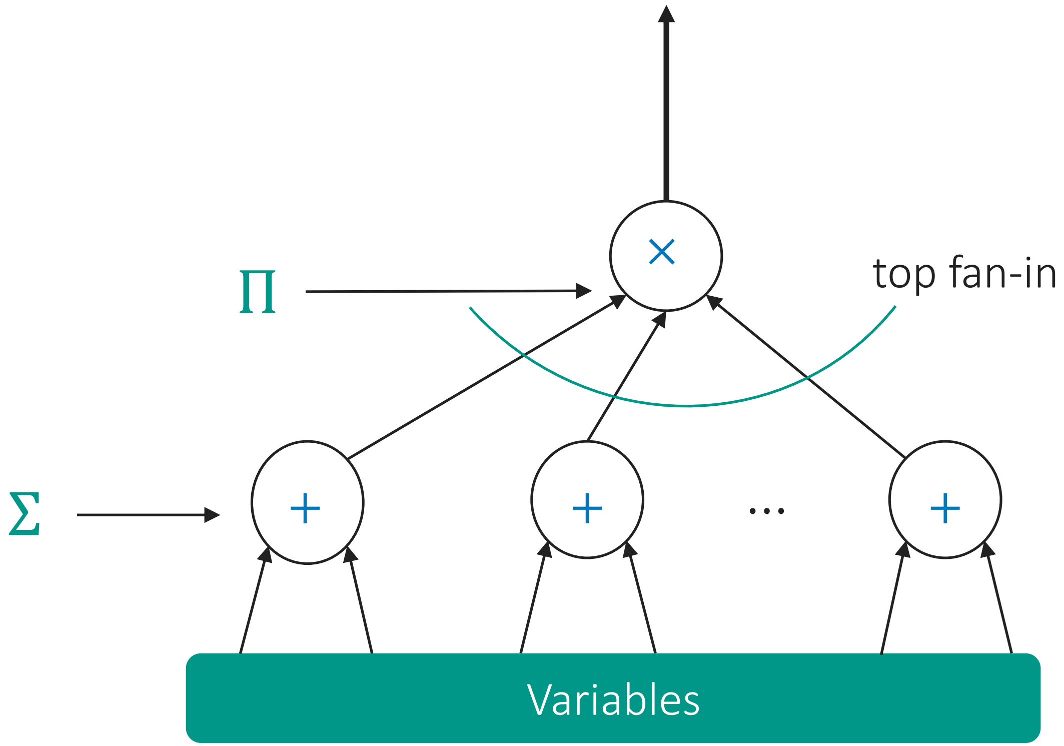
$$\mathbb{F}(\varepsilon)[x_1, \dots, x_n] \ni g = \sum_{i=1}^{s} (\text{monomial})_i$$



Known Debordering Results

- $\overline{\Sigma^{[s]}\Pi} = \Sigma^{[s]}\Pi$ and $\overline{\Pi\Sigma} = \Pi\Sigma$

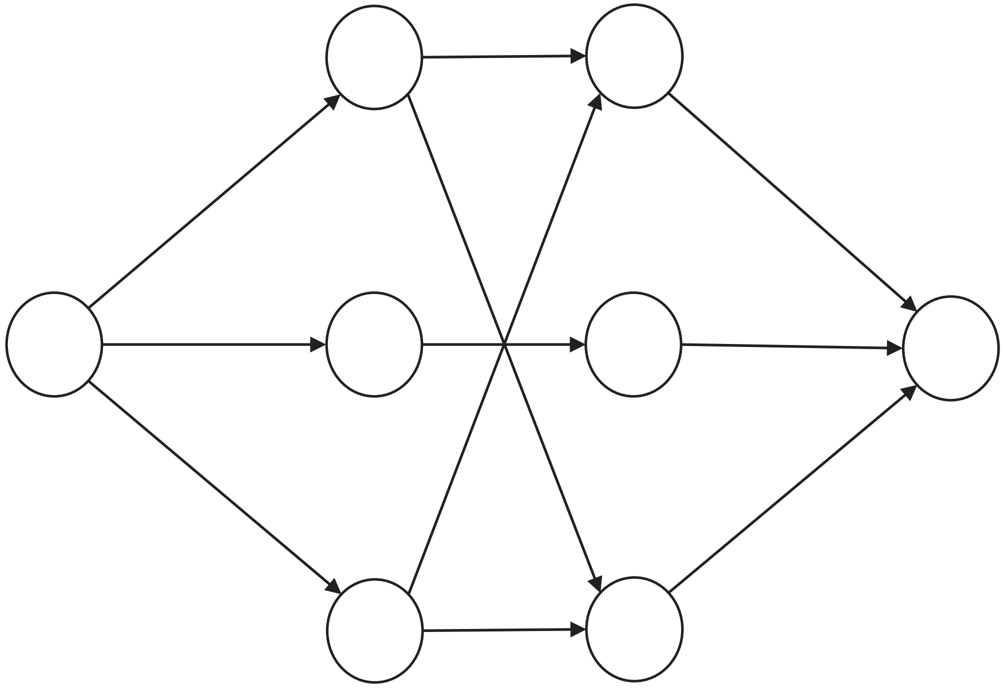
$$\mathbb{F}(\varepsilon)[x_1, \dots, x_n] \ni g = \prod_{i=1}^{s} (\text{lr.poly})_i$$



$(\text{lr.poly}) = a_1x_1 + \cdots + a_nx_n$

Known Debordering Results

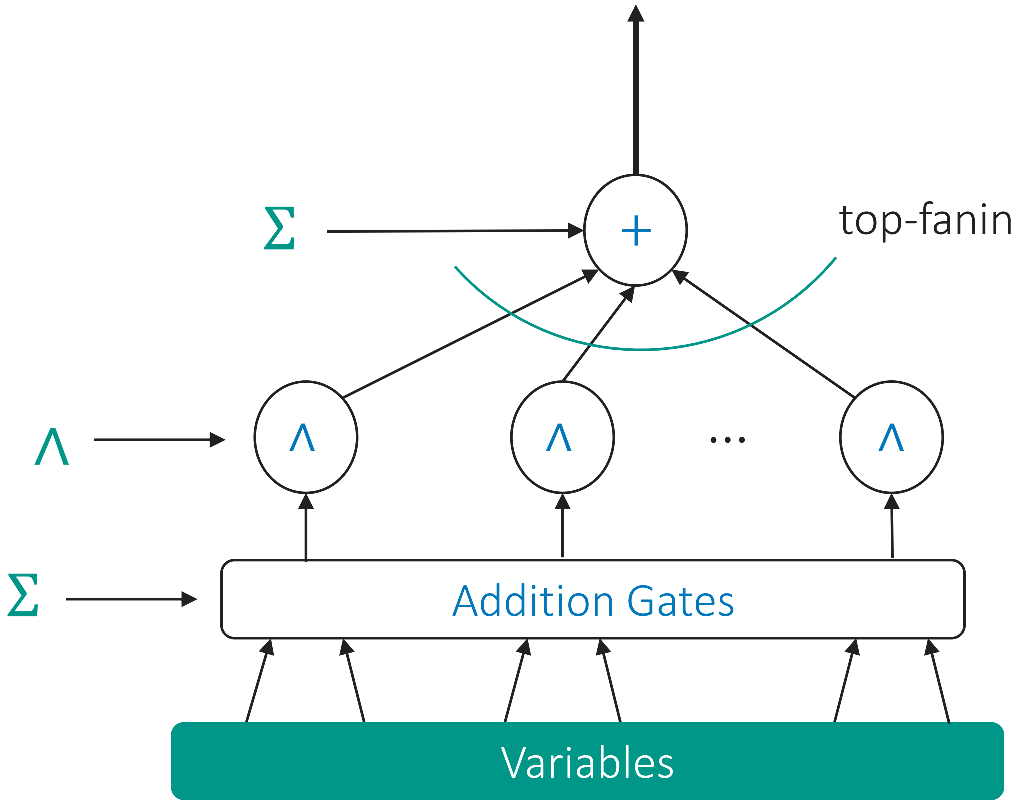
- $\overline{\Sigma^{[s]}\Pi} = \Sigma^{[s]}\Pi$ and $\overline{\Pi\Sigma} = \Pi\Sigma$
- In non-commutative realm $\overline{\mathrm{VBP}} = \mathrm{VBP}$.
  - Nisan 1991, Forbes 2016



Known Debordering Results

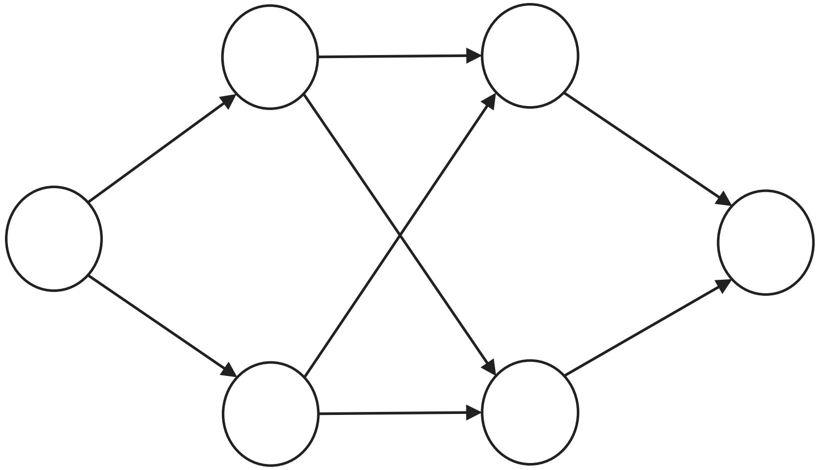
- $\overline{\Sigma^{[s]}\Pi} = \Sigma^{[s]}\Pi$ and $\overline{\Pi\Sigma} = \Pi\Sigma$
- In non-commutative realm $\overline{\mathrm{VBP}} = \mathrm{VBP}$.
  - Nisan 1991
- $\overline{\Sigma \wedge \Sigma} \subseteq \mathrm{VBP}$

$$\mathbb{F}(\varepsilon)[x_1, \dots, x_n] \ni g = \sum_{i}^{k} (\ell_{ij})^{e_i}$$



Known Debordering Results

- $\overline{\Sigma^{[s]}\Pi} = \Sigma^{[s]}\Pi$ and $\overline{\Pi\Sigma} = \Pi\Sigma$
- In non-commutative realm $\overline{\mathrm{VBP}} = \mathrm{VBP}$.
  - *Nisan 1991*
- $\overline{\Sigma \wedge \Sigma} \subseteq \mathrm{VBP}$
- $\mathrm{VBP}_2 \neq \overline{\mathrm{VBP}_2} = \overline{\mathrm{VF}}$.
  - *Bringmann, Ikenmeyer, Zuiddam 2018*
- In monotone setting $\overline{\mathrm{VBP}} = \mathrm{VBP}$.
  - *Bläser, Ikenmeyer, Mahajan, Pandey, Saurabh 2020*



Debordering Depth-3 Circuits

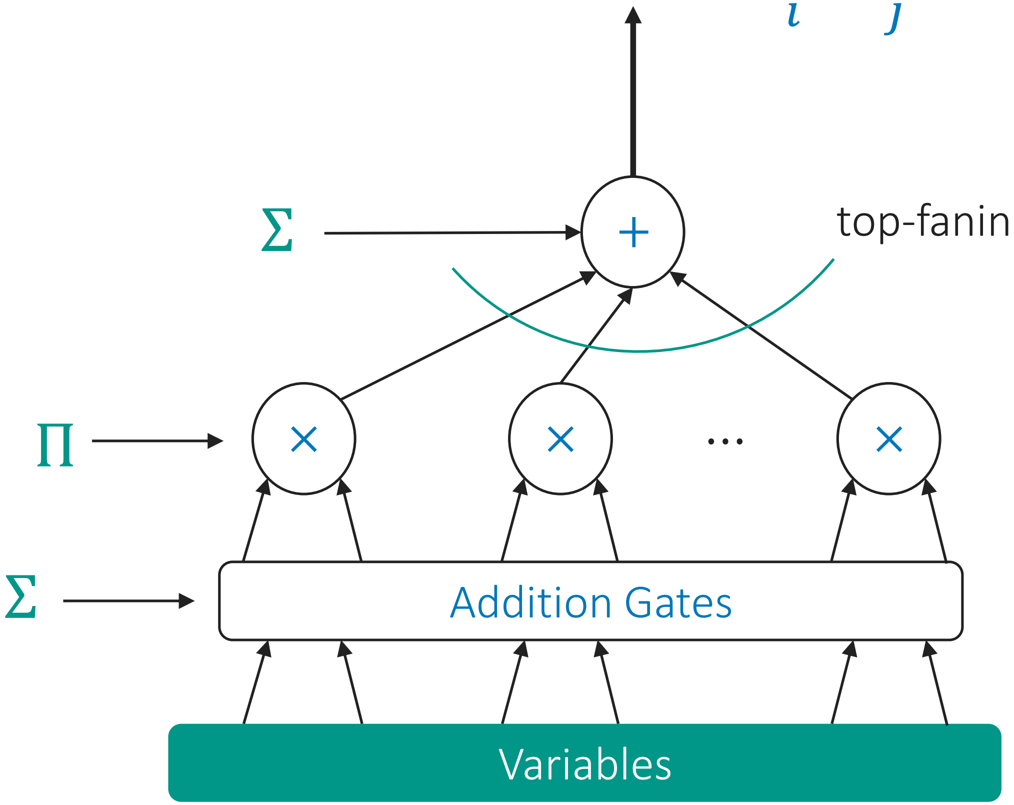
Depth-3 circuits $\Sigma^{[k]}\Pi^{[d]}\Sigma$

- Sum of product of *linear terms*.
- They cannot compute everything easily.

$$h_2(\bar{x},\bar{y}) = x_1 \cdot y_1 + x_2 \cdot y_2$$

- h_2 cannot be computed by $\Sigma^{[1]}\Pi^{[d]}\Sigma$.
  - Regardless of d.
- Moreover, $h_2 \in \mathrm{VBP}$.
  - $\Sigma^{[k]}\Pi\Sigma \subset \mathrm{VBP}$.

$$\mathbb{F}[x_1,\dots,x_n] \ni f = \sum_i^k \prod_j^d \ell_{ij}$$



$$(\mathrm{lr.poly}) = a_1x_1 + \cdots + a_nx_n$$

Universality of $\overline{\Sigma^{[k]}\Pi^{[d]}\Sigma}$

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

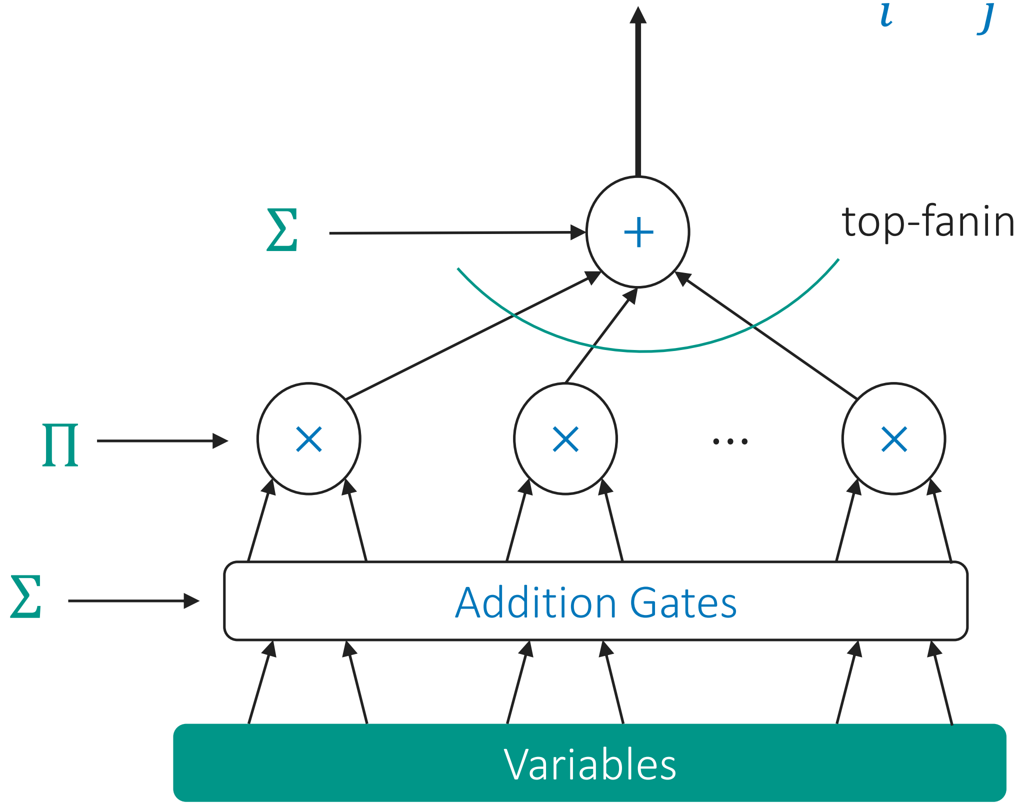
Kumar 2020

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

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

- Say D= $\mathrm{poly}(n)$.
  - What is the $\mathrm{size}(f)$?
  - $\overline{\Sigma^{[k]}\Pi^{[D]}\Sigma} \subseteq \mathrm{VNP}$?

$$\mathbb{F}(\varepsilon)[x_1, \dots, x_n] \ni g = \sum_i^k \prod_j^d \ell_{ij}$$



Debordering $\overline{\Sigma^{[k]}\Pi^{[d]}\Sigma}$

Dutta, Dwivedi, Saxena 2021

$$\overline{\Sigma^{[2]}\Pi^{[D]}\Sigma} \subseteq \mathrm{VBP}$$

Where, $D = \mathrm{poly}(n)$.

- Result holds for arbitrary constant k.

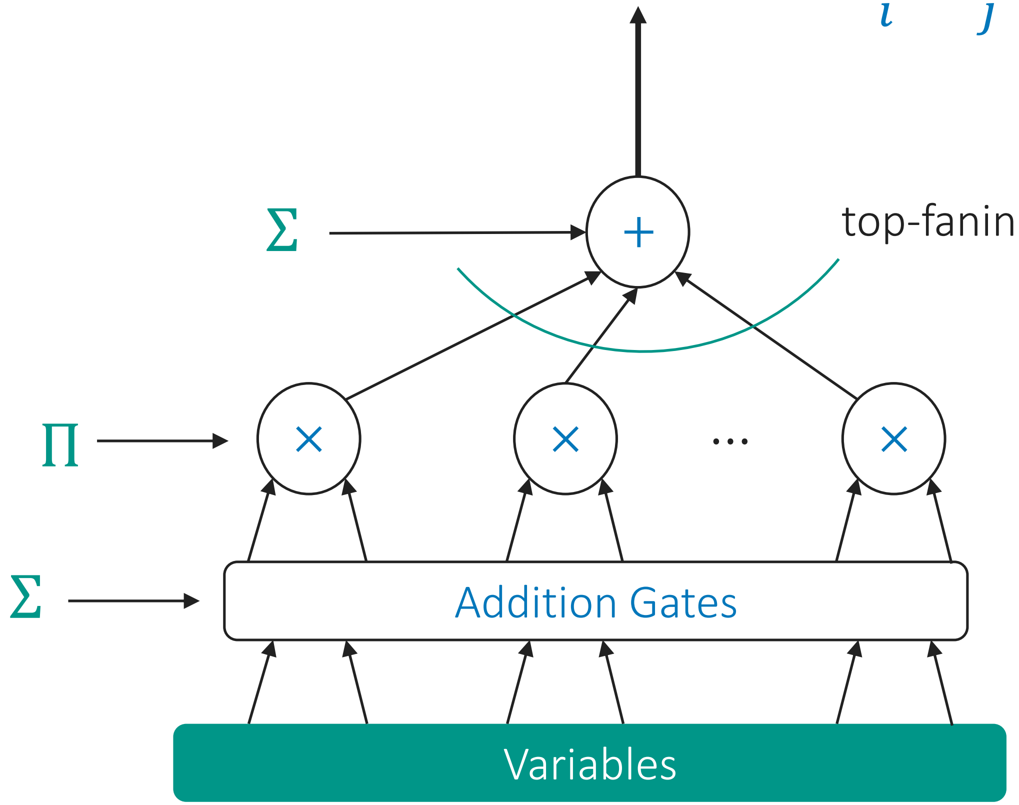
Dutta, Saxena 2021

$$\overline{\Sigma^{[k]}\Pi^{[D]}\Sigma} \neq \mathrm{VBP}$$

Where, $D = \mathrm{poly}(n)$.

- Exponential separation between $\overline{\Sigma^{[k+1]}\Pi^{[d]}\Sigma}$ and $\overline{\Sigma^{[k]}\Pi^{[d]}\Sigma}$

$$\mathbb{F}(\varepsilon)[x_1, \ldots, x_n] \ni g = \sum_i^k \prod_j^d \ell_{ij}$$



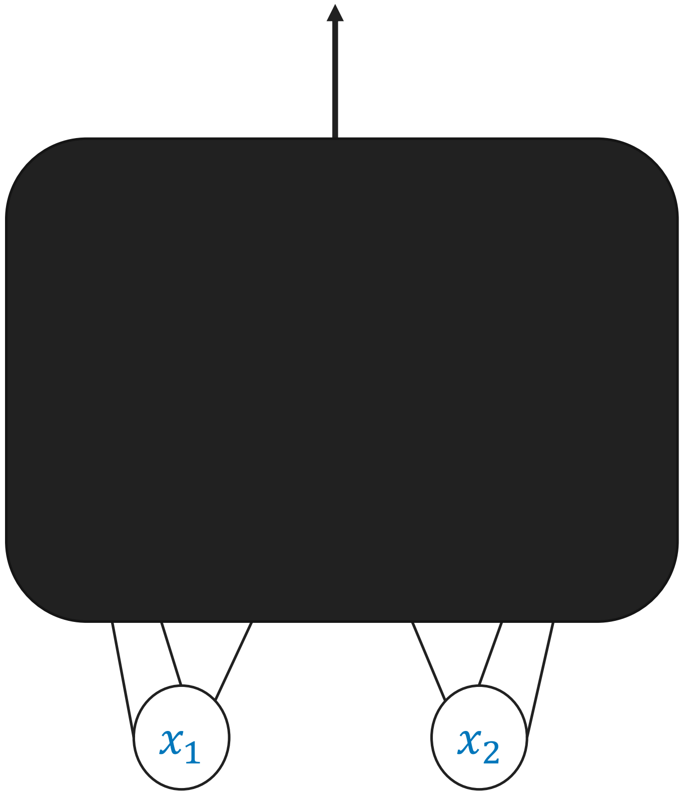
Polynomial Identity Testing

Polynomial Identity Testing

PIT

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

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



- Whitebox.
- Blackbox $\longleftrightarrow$ Hitting Set.

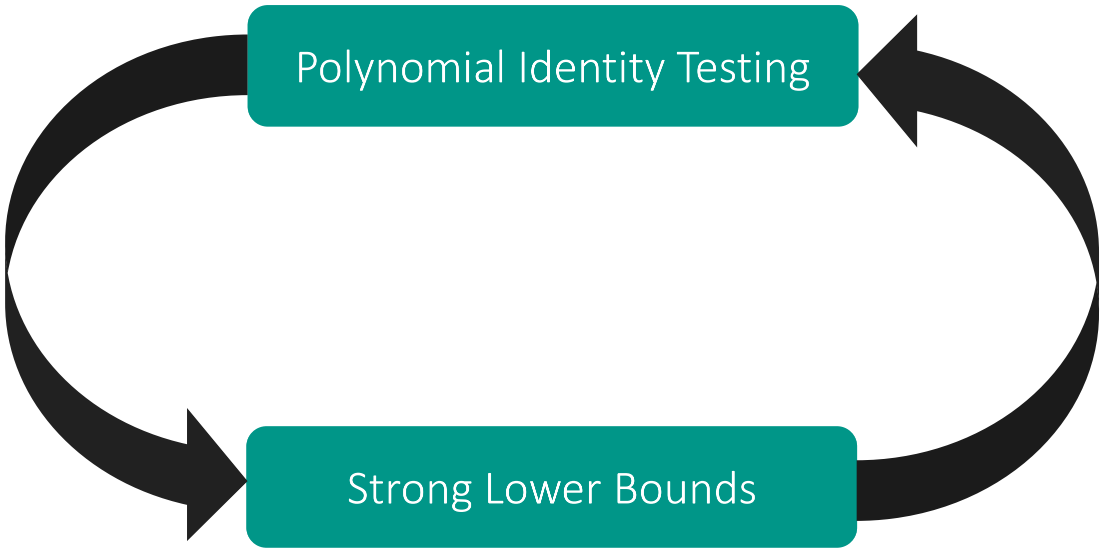
Hitting Set

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

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

Why do we care?

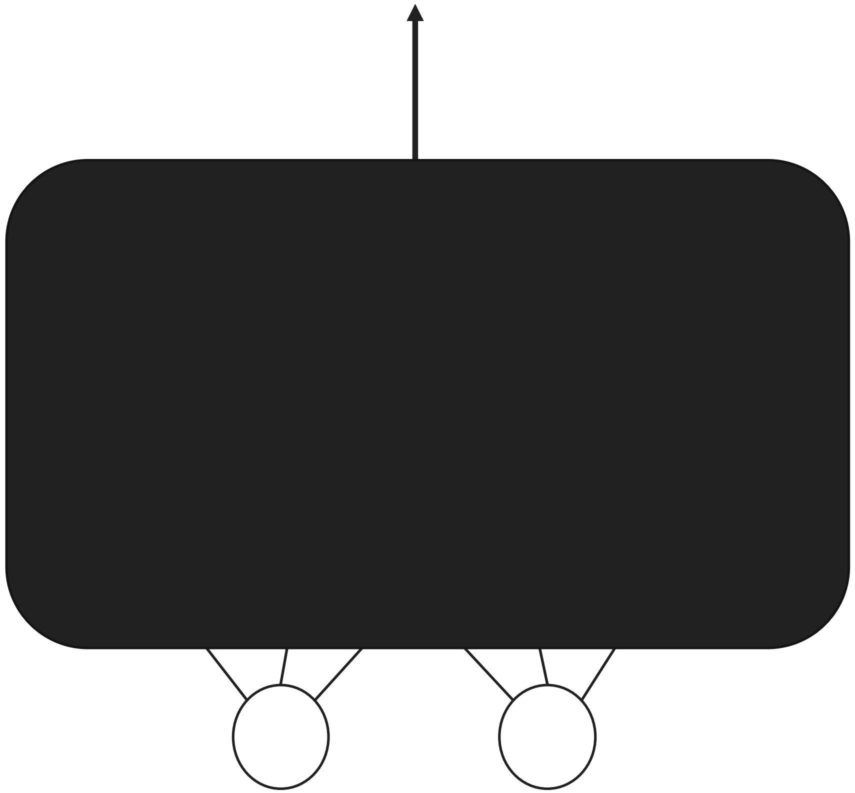
- Algorithms
- Complexity Theory
- Lower Bounds
  - PIT is intrinsically connected to proving circuit lower bounds.



Border Identity Testing

- Consider a border complexity class $\bar{\mathcal{C}}$. For every $f(\bar{x}) \in \bar{\mathcal{C}}$, there is $g(\varepsilon, \bar{x}) \in \mathcal{C}$ over $\mathbb{F}(\varepsilon)$.

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



Border Hitting Set

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

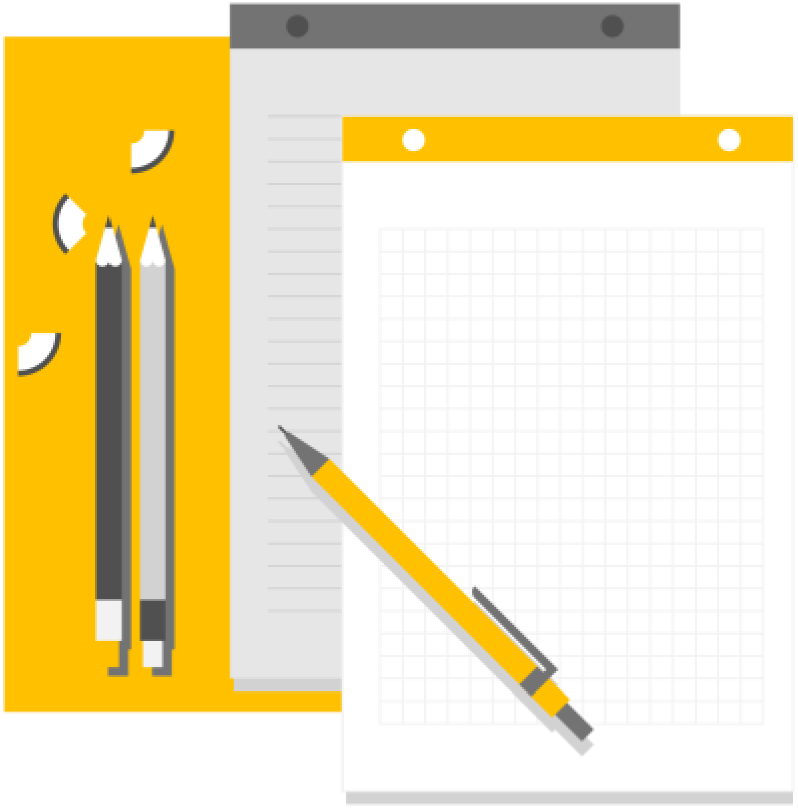
$$g(\varepsilon, \bar{a}) \neq \varepsilon \cdot h$$

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

- That means, $f(\bar{a}) \neq 0$
- $g(\varepsilon, \bar{a}) \neq 0$ does not suffice.
  - Therefore, $\mathcal{H}$ of $\mathcal{C}$ does not work.

Known Border PIT

- Polynomial time hitting set for $\overline{\Sigma\Pi} = \Sigma\Pi$.
  - Klivans and Spielman 2001
- Quasipolynomial time hitting set for $\overline{\Sigma \wedge \Sigma}$.
  - Forbes and Shpilka 2013
- PSPACE time hitting set for $\overline{\mathrm{VP}}$.
  - Forbes and Shpilka 2018
  - Guo, Saxena, Sinhababu 2019
- Polynomial time hitting set for sum of restricted logvariate ABP.
  - Bisht and Saxena 2021



Border PIT of Depth-3 Circuits

Dutta, Dwivedi, Saxena 2021

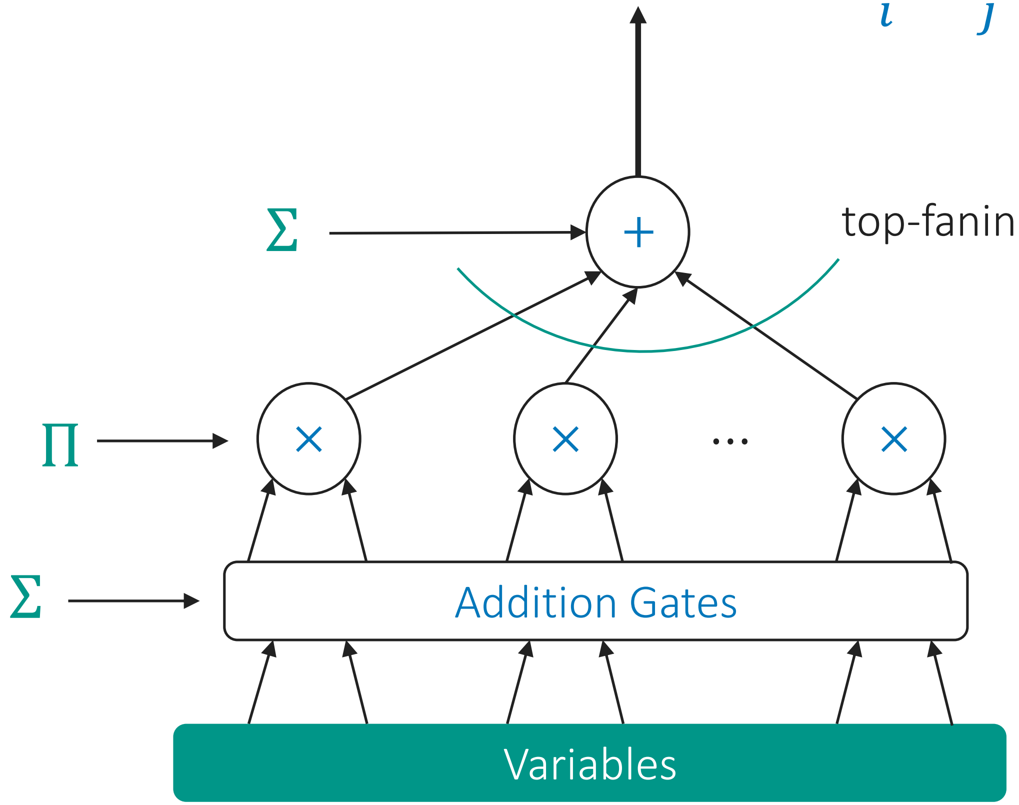
Quasipolynomial time hitting set of $\overline{\Sigma^{[k]}\Pi\Sigma}$, for any constant k.

- For circuit of size s and constant k,
  $s^{O(\log\log s)}$ time hitting set.

Dutta, Dwivedi, Saxena 2021

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

$$\mathbb{F}(\varepsilon)[x_1, \dots, x_n] \ni g = \sum_i^k \prod_j^d \ell_{ij}$$



Conclusion and Future Direction

Future Directions

- Debordering
  - Show $\overline{\Sigma^{[k]}\Pi\Sigma} = \Sigma^{[k]}\Pi\Sigma$ or $\overline{\Sigma^{[k]} \wedge \Sigma} = \Sigma^{[k]} \wedge \Sigma$.
  - Deborder width-2 ABP, and there by deborder VF.
  - Investigate other restricted models. E.g Sum of Read Once ABP.
- Identity Testing
  - Give polynomial time hitting set for $\overline{\Sigma^{[k]}\Pi\Sigma}$.
  - Debordering vs Derandomization.
- Other applications of debordering.