Presentable Version of Border Complexity and Applications to Circuit Factoring

In Proceedings of the 56th Annual ACM Symposium on Theory of Computing (STOC 2024)

C.S. Bhargav

Prateek Dwivedi

Nitin Saxena

Algorithms Group, ITU and BARC, KU

Polynomials

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

Then, $\sum_j e_j \leq d$.

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

Question

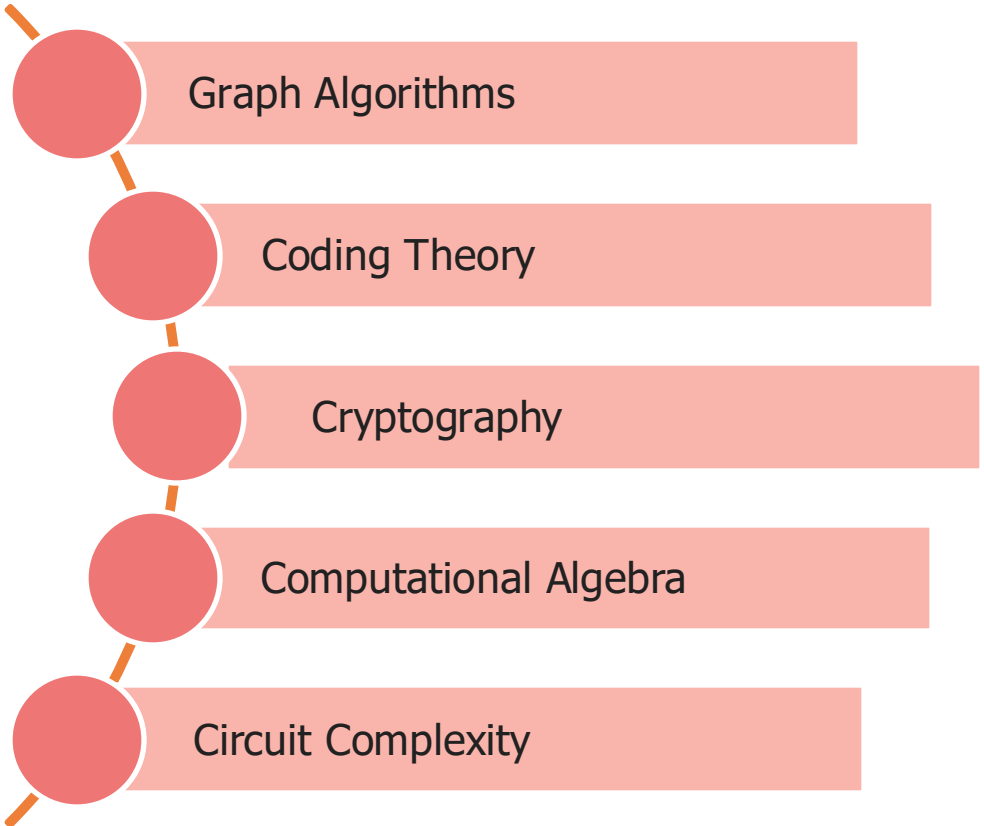
What is the efficient way to compute a family of polynomials?

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

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

Polynomials

Ubiquitous object in Computer Science.



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

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

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

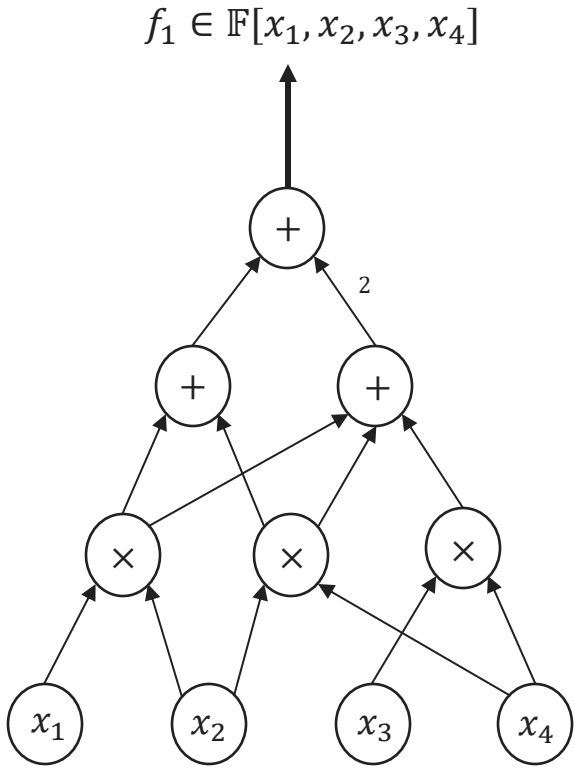
Algebraic Circuits

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.

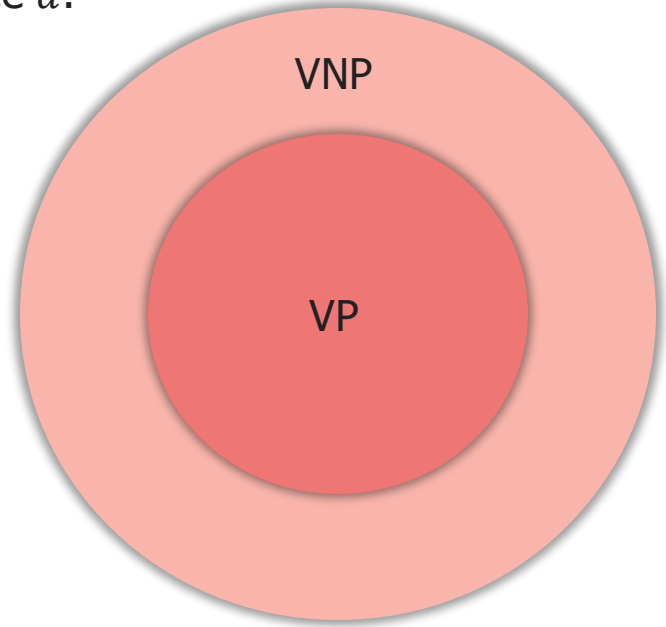


Algebraic Complexity Classes

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.

Explicit Class

Definition (VNP)

Polynomial $f \in \mathrm{VNP}$

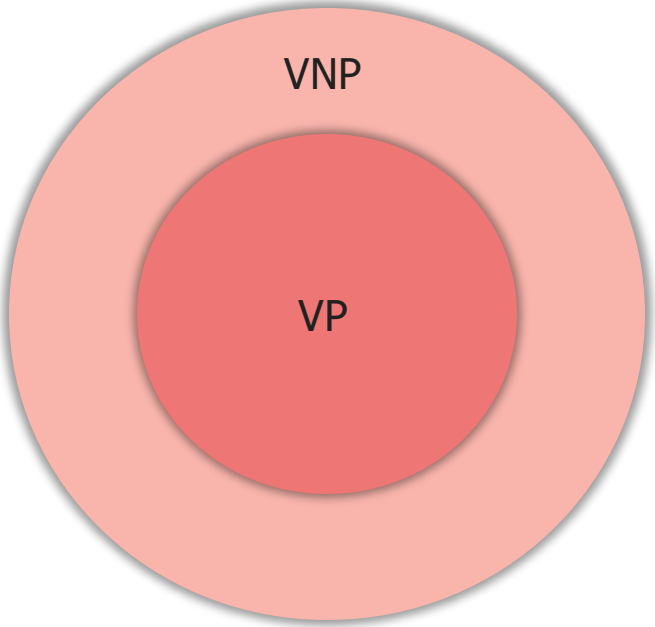
$$f(x_1, \ldots, x_n) = \sum_{a \in \{0,1\}^m} g(x, a)$$

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, $f \in \mathrm{VNP}$.



Evidences for Valiant Conjecture

Bürgisser 1998

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

In a more structural and relation-less world, VP ≠ VNP

- In the non-associative, commutative world.

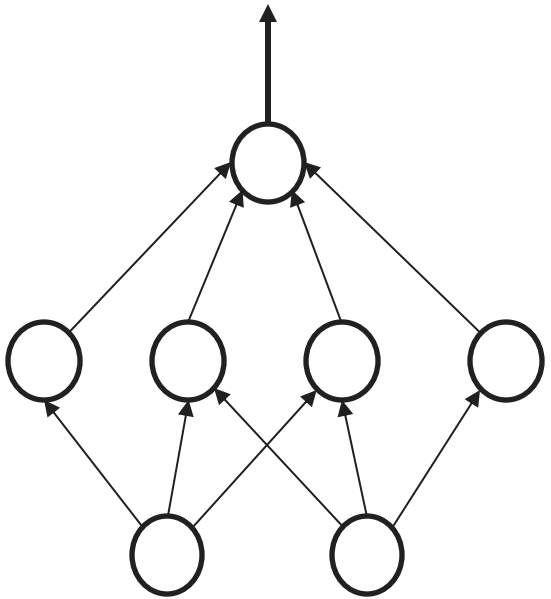
  Hrubeš, Wigderson, Yehudayoff 2010

- In the monotone world.

  Yehudayoff 2019, Srinivasan 2020

- In symmetric circuits.

  Dawar, Wilsenach 2020



Algebraic Approximation

Polynomial $g(\varepsilon, \bar{x}) \in \mathbb{F}[\varepsilon][\bar{x}]$ approximate $f(\bar{x})$

$$g(\varepsilon, \bar{x}) = \varepsilon^M \cdot f(\bar{x}) + \varepsilon^{M+1} \cdot Q(\varepsilon, \bar{x}).$$

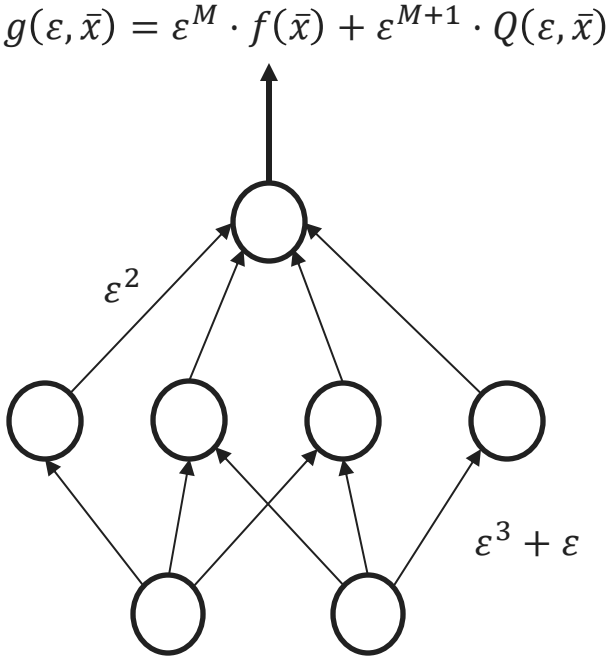
where $Q(\varepsilon, \bar{x})$ is higher order error terms, and M is called order of approximation.

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 $\overline{\text{size}}(f)$.



Motivating Example

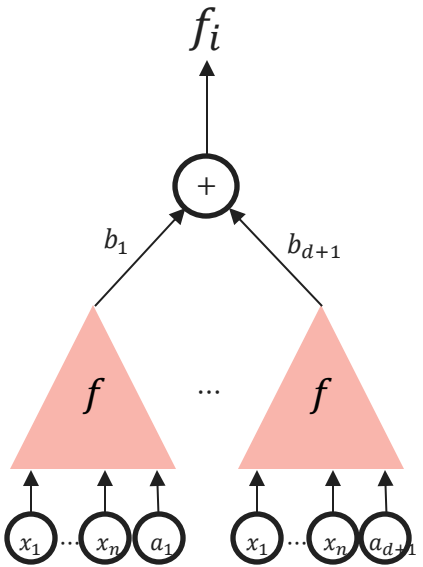
Consider a degree d polynomial $f(\bar{x}) \in \mathbb{F}[x_1, \ldots, x_n]$.

Let p be a positive integer.

$$f(\bar{x}) = \sum_{\bar{a}} c_{\bar{a}} \cdot x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$$

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

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



Interpolation

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

Motivating Example

We can do better if small error is tolerable.

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

$$= \sum_{\bar{a}} c_{\bar{a}} \cdot \varepsilon^{\sum a_i} \cdot \bar{x}^{\bar{a}}$$

$$= \varepsilon^p \cdot h(\bar{x}) + O(\varepsilon^{p+1})$$

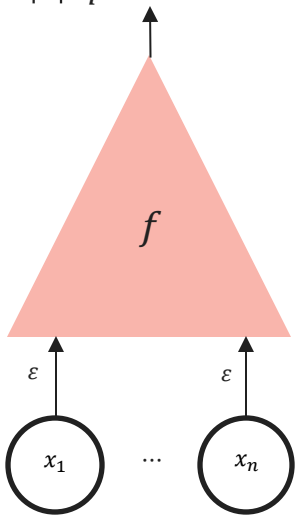
Approximation

$$\text{size}(g) = \overline{\text{size}}(h) \leq O(\text{size}(f))$$

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

$$f(\bar{x}) = \sum_{\bar{a}} c_{\bar{a}} \cdot x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$$

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



Algebraic Approximation

Question (Debordering)

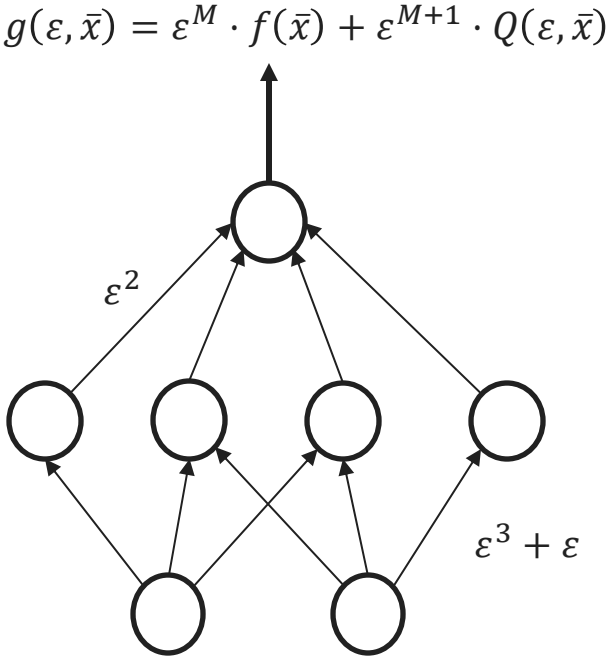
Given $\overline{\text{size}}(f) = \text{size}_{\mathbb{F}[\varepsilon]}(g)$, what is $\text{size}(f)$?

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

Arbitrary polynomials in ε are treated as free constants in circuit computing g.

Bürgisser 2004

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



Border Classes

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

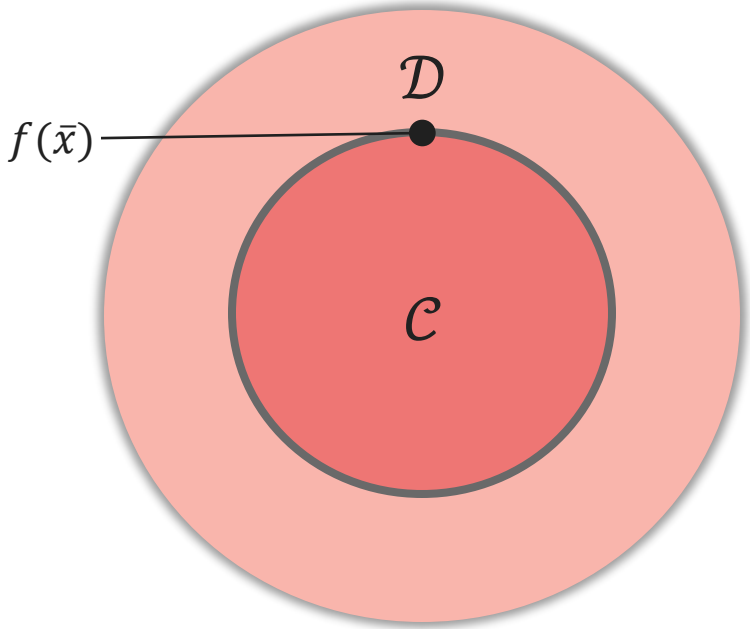
A polynomial $f \in \bar{\mathcal{C}}$,

$$g(\varepsilon, \bar{x}) = \varepsilon^M \cdot f(\bar{x}) + \varepsilon^{M+1} \cdot Q(\varepsilon, \bar{x}) \in \mathcal{C}_{\mathbb{F}[\varepsilon]}.$$

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

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

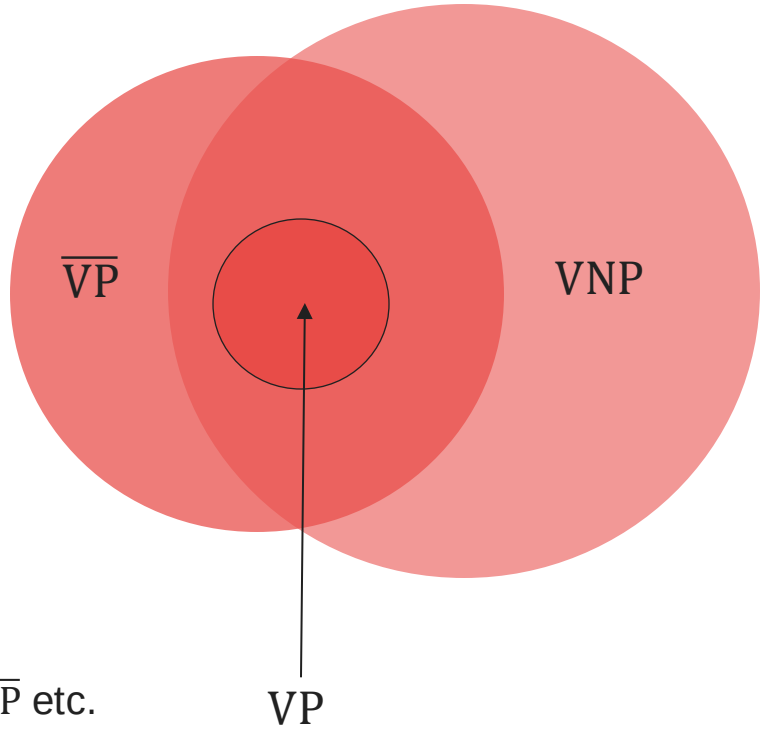
Resolving this conjecture will prove VP ≠ VNP.

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.

Main Results

Presentable Border

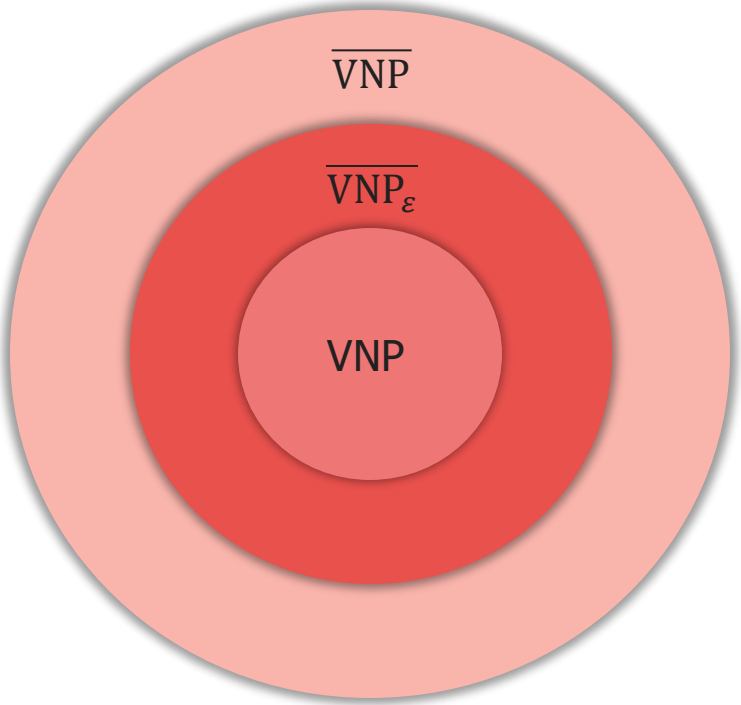
Approximating circuits use arbitrary polynomials in ε of arbitrary complexity as free constant. Their circuit complexity may not be bounded by $\text{size}_{\mathbb{F}[\varepsilon]}(g)$

Definition (Presentable $\overline{\text{VNP}}$)

Polynomial $f \in \overline{\text{VNP}}_{\varepsilon}$

$$g = \varepsilon^M \cdot f + \varepsilon^M \cdot Q$$

where g is in VNP over $\mathbb{F}[\varepsilon]$, but the ε polynomial are of size poly(n).



We don't know if $\overline{\text{VNP}}$ is explicit. What about $\overline{\text{VNP}_{\varepsilon}}$?

Presentable is Explicit

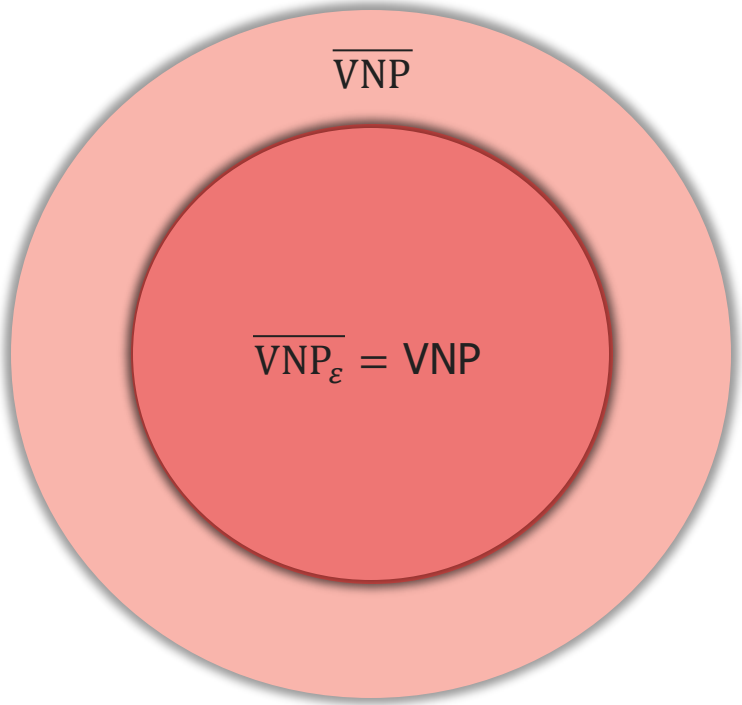
Bhargav, Dwivedi, and Saxena 2024

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

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

Conjecture (Presentable Separation)

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



Presentable is Explicit

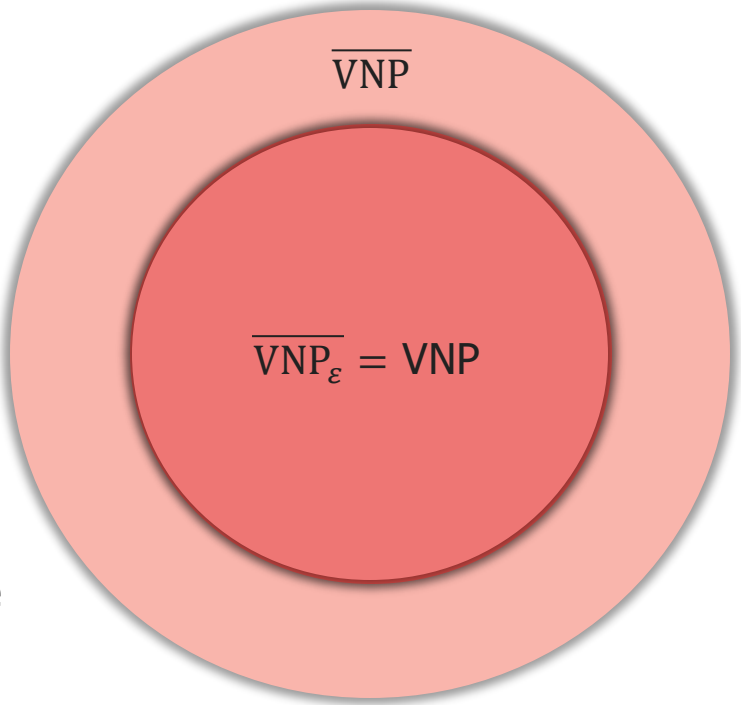
Instead of using the definition, we use the famous criterion.

VNP Criterion

If the coefficients of a polynomial f can be computed by a function in #P/poly, then $f \in$ VNP.

We use Exponential Interpolation to show that coefficients of $f \in \overline{\mathrm{VNP}_\varepsilon}$, can be computed by hypercube sum of exponential-degree small-sized circuits.

We transfer it to Boolean world to obtain #P/poly function.

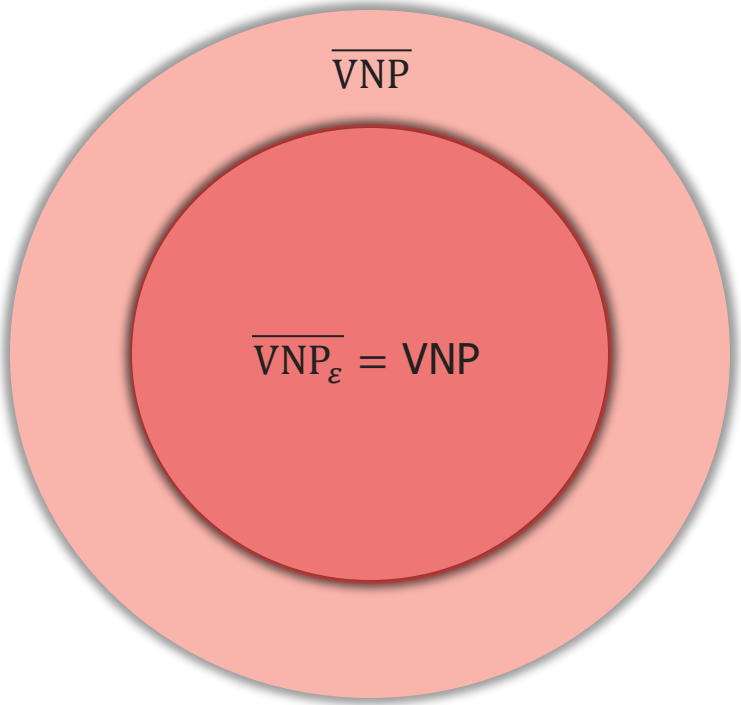


Presentable is Explicit

Instead of using the definition, we use the famous criterion.

VNP Criterion

If the coefficients of a polynomial f can be computed by a function in #P/poly, then $f \in$ VNP.



Tricky issues:

- Complexity of coefficient polynomial is tractable because of presentability.
- Careful choice of interpolation points.

Complexity of Multivariate Factoring

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

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

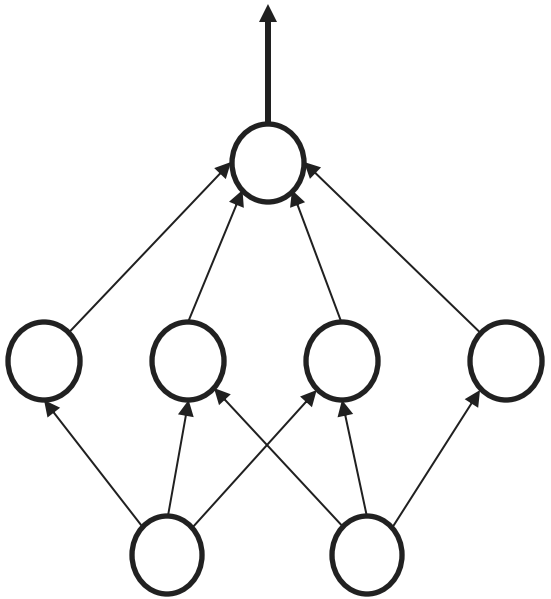
$$f(\bar{x}) = \prod_{i \in [m]} f_i(\bar{x})^{e_i}$$

- Circuit complexity bound on all irreducible factors.
- Efficient Algorithm to compute all irreducible factors.

Kaltofen (and others)

If $g \mid f$, then $\text{size}(g) \leq \text{poly}(\text{size}(f), \deg(g))$.

VP is *uniformly* closed under factoring.



VNP Factor Closure

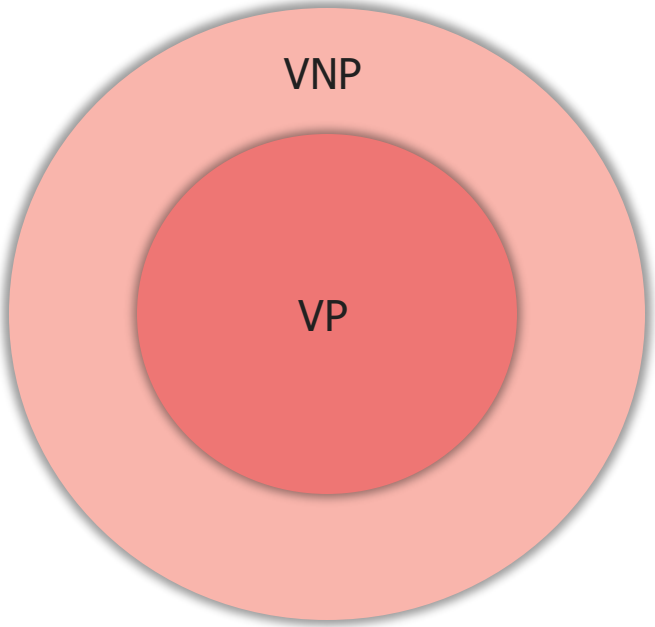
Bürgisser conjectured that VNP is closed under factorization.

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.

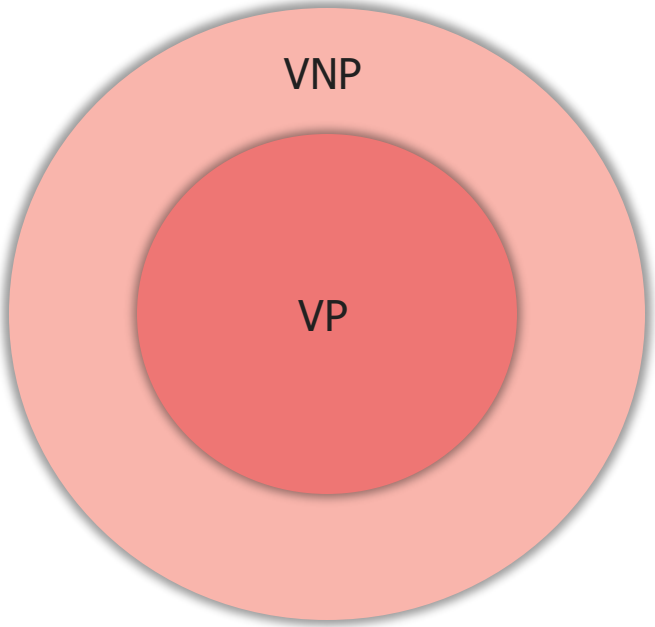


VNP Factor Closure

The proof reduces to two cases:

1. $f = u^e$ or in particular $f = u^{p^k}$ (*separable*).
2. $f = u \cdot v$ (*product of co-prime polynomials*).

Case (2) is more or less proved using known techniques. For Case (1) we use a different approach.



Converse of VNP Criterion

Over finite fields, if $f \in$ VNP, then coefficients of f can be computed by a function in #P/poly.

Debordering Factors

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

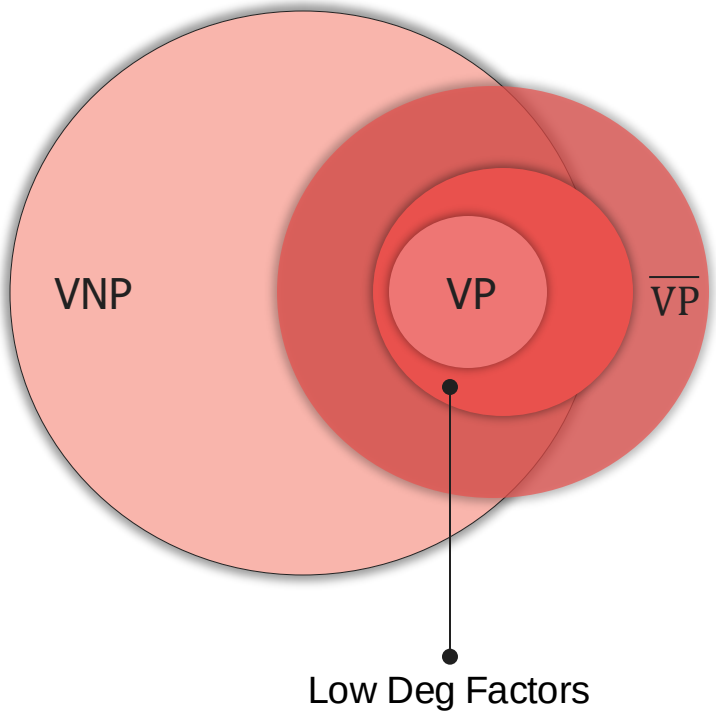
Conjecture (Low degree factors)

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

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

Bhargav, Dwivedi, and Saxena 2024

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



Conclusion

Open Problems

- Debordering Presentability beyond finite fields.
- Resolve factor conjecture by complete debordering of $\overline{\mathrm{VP}_\varepsilon}$.
- Transfer Presentability to restricted models of polynomial computation.