

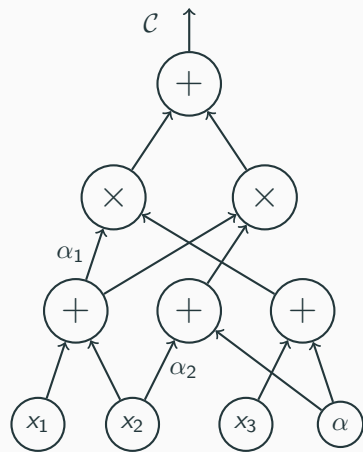
Monotone Classes Beyond VNP

Prerona Chatterjee [with Kshitij Gajjar (IIT Jodhpur) and Anamay Tengse (Reichman University)]

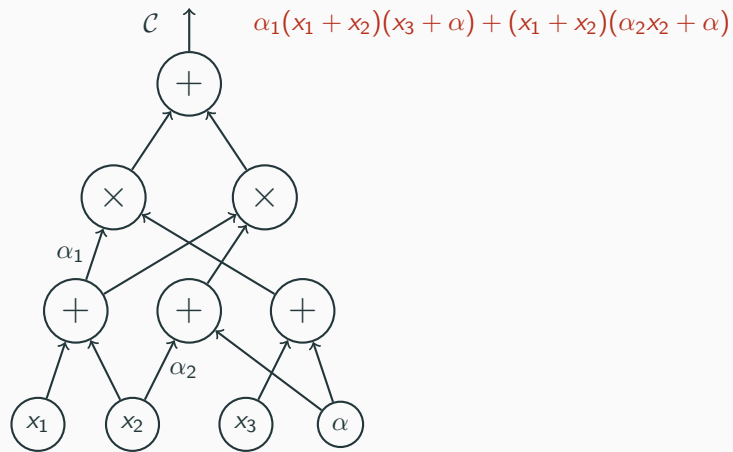
Tel Aviv University

December 18, 2023

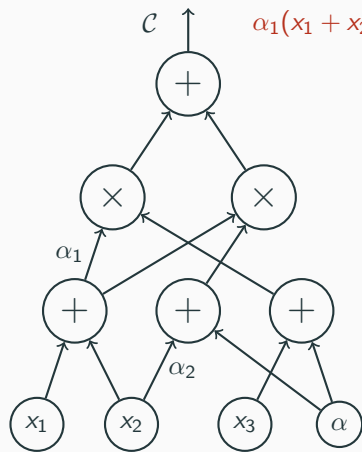
Algebraic Classes



Algebraic Classes



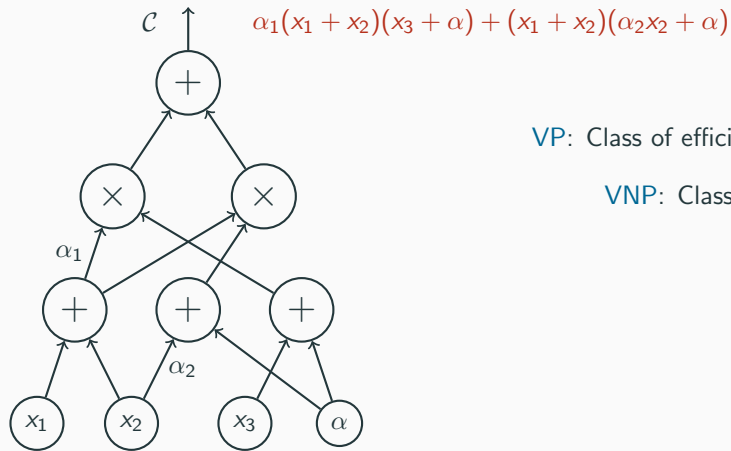
Algebraic Classes



$$\alpha_1(x_1 + x_2)(x_3 + \alpha) + (x_1 + x_2)(\alpha_2 x_2 + \alpha)$$

VP: Class of efficiently computable polynomials.

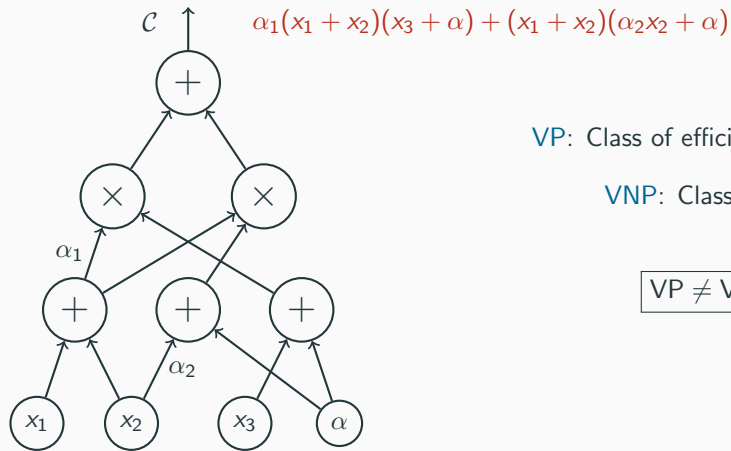
Algebraic Classes



VP: Class of efficiently computable polynomials.

VNP: Class of explicit polynomials.

Algebraic Classes

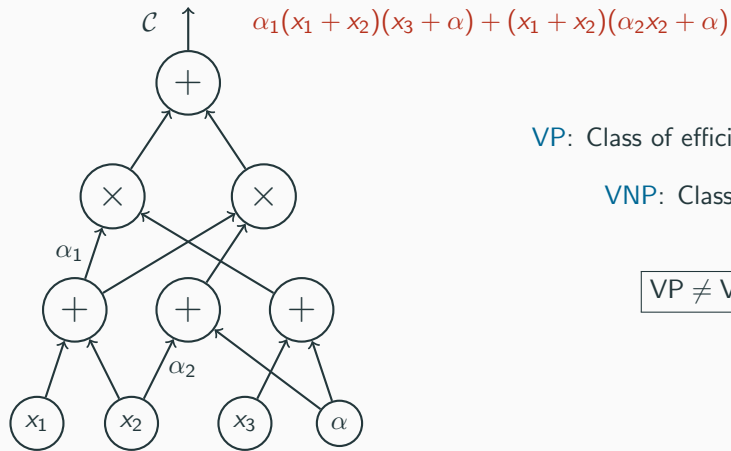


VP: Class of efficiently computable polynomials.

VNP: Class of explicit polynomials.

VP \neq VNP

Algebraic Classes

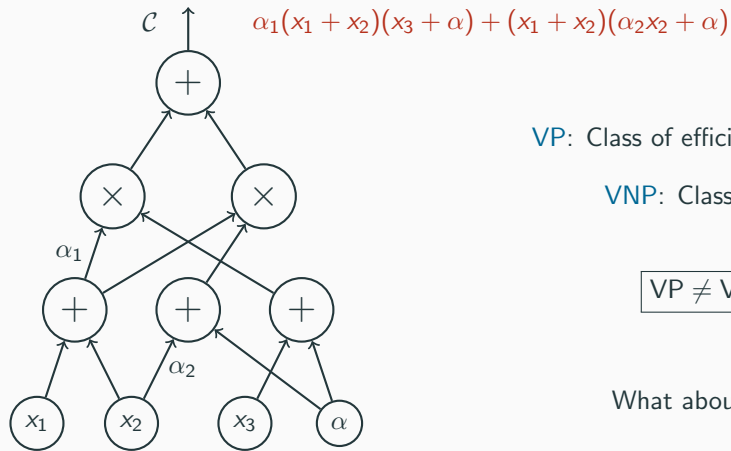


VP: Class of efficiently computable polynomials.

VNP: Class of explicit polynomials.

$$\boxed{VP \neq VNP} \iff \boxed{P \neq NP}$$

Algebraic Classes



VP: Class of efficiently computable polynomials.

VNP: Class of explicit polynomials.

$$\boxed{VP \neq VNP} \iff \boxed{P \neq NP}$$

What about classes beyond VNP?

The Class VPSPACE

[Koiran-Perifel]: $\{f_n\}_n$ is in VPSPACE^0 if the following language is in $\text{PSPACE}/\text{poly}$.

$\text{coeff}(n, \mathbf{e}, i) \equiv i\text{-th bit of the coefficient of } \mathbf{x}^{\mathbf{e}} \text{ in } f_n$

The Class VPSPACE

[Koiran-Perifel]: $\{f_n\}_n$ is in VPSPACE^0 if the following language is in $\text{PSPACE}/\text{poly}$.

$\text{coeff}(n, \mathbf{e}, i) \equiv i\text{-th bit of the coefficient of } \mathbf{x}^{\mathbf{e}} \text{ in } f_n$

Note: $\text{deg}(f_n)$ can be as large as $2^{\text{poly}(n)}$.

The Class VPSPACE

[Koiran-Perifel]: $\{f_n\}_n$ is in VPSPACE^0 if the following language is in $\text{PSPACE}/\text{poly}$.

$$\text{coeff}(n, \mathbf{e}, i) \equiv i\text{-th bit of the coefficient of } \mathbf{x}^{\mathbf{e}} \text{ in } f_n$$

Note: $\text{deg}(f_n)$ can be as large as $2^{\text{poly}(n)}$.

VPSPACE_b : Polynomials in VPSPACE that have degree bounded by $\text{poly}(n)$.

The Class VPSPACE

[Koiran-Perifel]: $\{f_n\}_n$ is in VPSPACE^0 if the following language is in $\text{PSPACE}/\text{poly}$.

$\text{coeff}(n, \mathbf{e}, i) \equiv i\text{-th bit of the coefficient of } \mathbf{x}^{\mathbf{e}} \text{ in } f_n$

Note: $\text{deg}(f_n)$ can be as large as $2^{\text{poly}(n)}$.

VPSPACE_b : Polynomials in VPSPACE that have degree bounded by $\text{poly}(n)$.

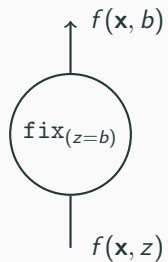
[Koiran-Perifel]: $\text{VP} \neq \text{VPSPACE}_b \implies \text{VP} \neq \text{VNP}$ or $\text{P}/\text{poly} \neq \text{PSPACE}/\text{poly}$.

Algebraic Circuits with Projection Gates

Is there a more algebraic definition?

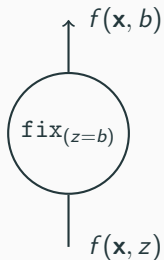
Algebraic Circuits with Projection Gates

Is there a more algebraic definition?



Algebraic Circuits with Projection Gates

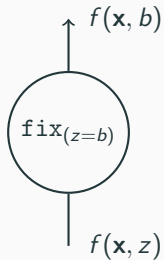
Is there a more algebraic definition?



$\text{VPROJ} \equiv$ polynomials efficiently computable by algebraic circuits with projection gates.

Algebraic Circuits with Projection Gates

Is there a more algebraic definition?



$\text{VPROJ} \equiv$ polynomials efficiently computable by algebraic circuits with projection gates.

[Poizat]: $\text{VPROJ} = \text{VPSPACE}$.

Quantified Algebraic Circuits

Ok, but PSPACE is the same as TQBF.

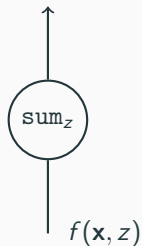
Quantified Algebraic Circuits

Ok, but PSPACE is the same as TQBF. Is something analogous true in the algebraic setting?

Quantified Algebraic Circuits

Ok, but PSPACE is the same as TQBF. Is something analogous true in the algebraic setting?

$$f(\mathbf{x}, 0) + f(\mathbf{x}, 1)$$



Quantified Algebraic Circuits

Ok, but PSPACE is the same as TQBF. Is something analogous true in the algebraic setting?

$$f(\mathbf{x}, 0) + f(\mathbf{x}, 1)$$



$$f(\mathbf{x}, z)$$

$$f(\mathbf{x}, 0) \times f(\mathbf{x}, 1)$$



$$f(\mathbf{x}, z)$$

Quantified Algebraic Circuits

Ok, but PSPACE is the same as TQBF. Is something analogous true in the algebraic setting?

$$f(\mathbf{x}, 0) + f(\mathbf{x}, 1)$$



$$f(\mathbf{x}, z)$$

$$f(\mathbf{x}, 0) \times f(\mathbf{x}, 1)$$



$$f(\mathbf{x}, z)$$

$$f = Q_{z_1} Q_{z_2} \cdots Q_{z_m} C[\mathbf{x}, \mathbf{z}].$$

Quantified Algebraic Circuits

Ok, but PSPACE is the same as TQBF. Is something analogous true in the algebraic setting?

$$f(\mathbf{x}, 0) + f(\mathbf{x}, 1)$$



$$f(\mathbf{x}, z)$$

$$f(\mathbf{x}, 0) \times f(\mathbf{x}, 1)$$



$$f(\mathbf{x}, z)$$

$$f = Q_{z_1} Q_{z_2} \cdots Q_{z_m} C[\mathbf{x}, \mathbf{z}].$$

TQAC \equiv polynomials efficiently computable by totally quantified algebraic circuits.

Quantified Algebraic Circuits

Ok, but PSPACE is the same as TQBF. Is something analogous true in the algebraic setting?

$$f(\mathbf{x}, 0) + f(\mathbf{x}, 1)$$



$$f(\mathbf{x}, z)$$

$$f(\mathbf{x}, 0) \times f(\mathbf{x}, 1)$$



$$f(\mathbf{x}, z)$$

$$f = Q_{z_1} Q_{z_2} \cdots Q_{z_m} C[\mathbf{x}, \mathbf{z}].$$

TQAC \equiv polynomials efficiently computable by totally quantified algebraic circuits.

[Malod]: TQAC = VPSPACE.

- There are various definitions of $VPSPACE$, all of which happen to be equivalent.

In Summary

- There are various definitions of VPSPACE, all of which happen to be equivalent.
- There is no restriction on the degree, but we focus on VPSPACE_b .

In Summary

- There are various definitions of VPSPACE , all of which happen to be equivalent.
- There is no restriction on the degree, but we focus on VPSPACE_b .

[Koiran-Perifel]: $\text{VP} \neq \text{VPSPACE}_b \implies \text{VP} \neq \text{VNP}$ or $\text{P/poly} \neq \text{PSPACE/poly}$.

In Summary

- There are various definitions of VPSPACE, all of which happen to be equivalent.
- There is no restriction on the degree, but we focus on VPSPACE_b .

[Koiran-Perifel]: $\text{VP} \neq \text{VPSPACE}_b \implies \text{VP} \neq \text{VNP}$ or $\text{P/poly} \neq \text{PSPACE/poly}$.

It would be interesting to study classes beyond VNP in the algebraic world.

In Summary

- There are various definitions of VPSPACE, all of which happen to be equivalent.
- There is no restriction on the degree, but we focus on VPSPACE_b .

[Koiran-Perifel]: $\text{VP} \neq \text{VPSPACE}_b \implies \text{VP} \neq \text{VNP}$ or $\text{P/poly} \neq \text{PSPACE/poly}$.

It would be interesting to study classes beyond VNP in the algebraic world.

- Connections with the boolean world?

In Summary

- There are various definitions of VPSPACE, all of which happen to be equivalent.
- There is no restriction on the degree, but we focus on VPSPACE_b .

[Koiran-Perifel]: $\text{VP} \neq \text{VPSPACE}_b \implies \text{VP} \neq \text{VNP}$ or $\text{P/poly} \neq \text{PSPACE/poly}$.

It would be interesting to study classes beyond VNP in the algebraic world.

- Connections with the boolean world?
- Connections to algebraic pseudorandomness.

In Summary

- There are various definitions of VPSPACE, all of which happen to be equivalent.
- There is no restriction on the degree, but we focus on VPSPACE_b .

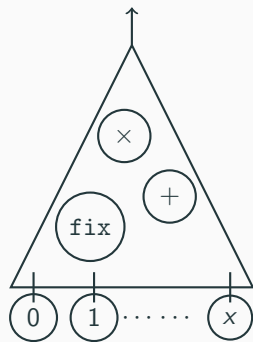
[Koiran-Perifel]: $\text{VP} \neq \text{VPSPACE}_b \implies \text{VP} \neq \text{VNP}$ or $\text{P/poly} \neq \text{PSPACE/poly}$.

It would be interesting to study classes beyond VNP in the algebraic world.

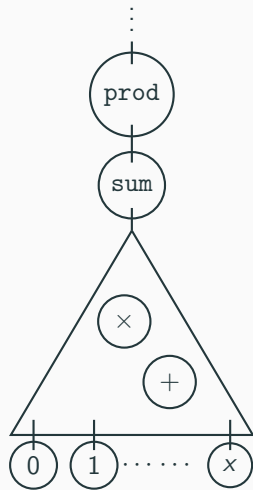
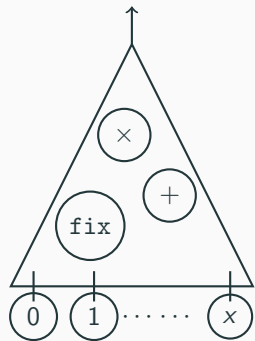
- Connections with the boolean world?
- Connections to algebraic pseudorandomness.

Can we prove lower bounds in the monotone setting?

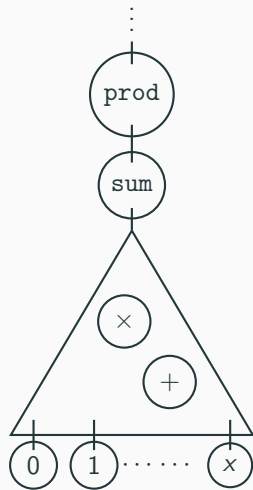
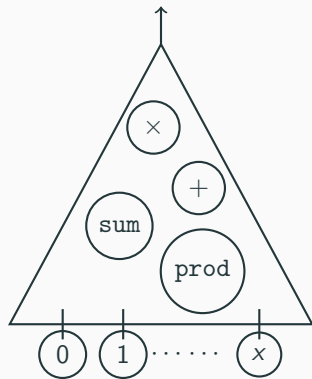
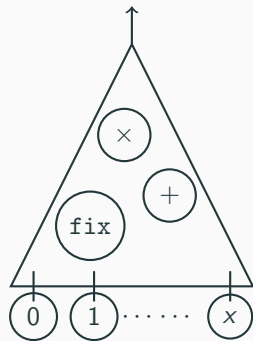
Monotone VPSPACE?



Monotone VPSPACE?

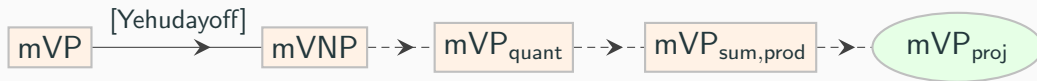


Monotone VPSPACE?



Our Results

Polynomials have bounded degree throughout



Our Results

Polynomials have bounded degree throughout



- $mVP_{quant} = mVNP$ if and only if all homogeneous components of polynomials in mVP_{quant} are contained in mVP_{quant} .

Our Results

Polynomials have bounded degree throughout



- $mVP_{\text{quant}} = mVNP$ if and only if all homogeneous components of polynomials in mVP_{quant} are contained in mVP_{quant} . In particular, $\text{hom}(mVP_{\text{quant}}) \subseteq mVNP$.

Our Results

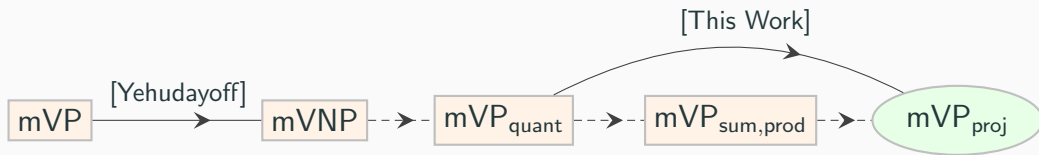
Polynomials have bounded degree throughout



- $mVP_{quant} = mVNP$ if and only if all homogeneous components of polynomials in mVP_{quant} are contained in mVP_{quant} . In particular, $\text{hom}(mVP_{quant}) \subseteq mVNP$.
- $mVP_{quant} = mVP_{sum,prod}$ if and only if mVP_{quant} is closed under compositions.

Our Results

Polynomials have bounded degree throughout



- $mVP_{\text{quant}} = mVNP$ if and only if all homogeneous components of polynomials in mVP_{quant} are contained in mVP_{quant} . In particular, $\text{hom}(mVP_{\text{quant}}) \subseteq mVNP$.
- $mVP_{\text{quant}} = mVP_{\text{sum,prod}}$ if and only if mVP_{quant} is closed under compositions.
- $mVP_{\text{quant}} \neq mVP_{\text{proj}}$.

Properties of mVP_{proj}

- The Permanent Family is contained in mVP_{proj} .

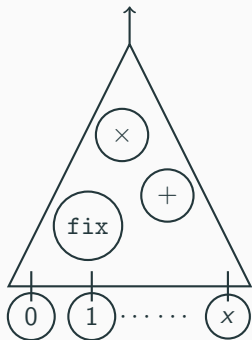
Properties of mVP_{proj}

- The Permanent Family is contained in mVP_{proj} .
- mVP_{proj} is closed under taking compositions.

Properties of mVP_{proj}

- The Permanent Family is contained in mVP_{proj} .
- mVP_{proj} is closed under taking compositions.
- Homogeneous components of polynomials in mVP_{proj} are also contained in mVP_{proj} .

Monotone VPSPACE

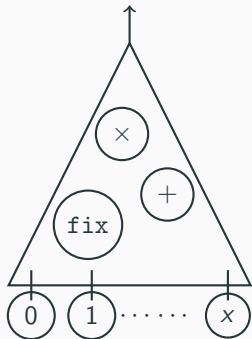


Properties of mVP_{proj}

- The Permanent Family is contained in mVP_{proj} .
- mVP_{proj} is closed under taking compositions.
- Homogeneous components of polynomials in mVP_{proj} are also contained in mVP_{proj} .

Defining $mVPSPACE$

A polynomial family $\{f_n\}_n$ is contained in $mVPSPACE$ if f_n is computable by an algebraic circuit with projection gates of size $\text{poly}(n)$.



Properties of mVP_{proj}

- The Permanent Family is contained in mVP_{proj} .
- mVP_{proj} is closed under taking compositions.
- Homogeneous components of polynomials in mVP_{proj} are also contained in mVP_{proj} .

Defining $mVPSPACE$

A polynomial family $\{f_n\}_n$ is contained in $mVPSPACE$ if f_n is computable by an algebraic circuit with projection gates of size $\text{poly}(n)$. The degree of f_n need not be bounded by $\text{poly}(n)$.

Upper Bound for Permanent

$$P(\mathbf{x}, \mathbf{y}) := \sum_{\sigma \in S_n} x_{1,\sigma(1)} \cdots x_{n,\sigma(n)}.$$

Upper Bound for Permanent

$$P_0(\mathbf{x}, \mathbf{y}) := \left(\sum_{j=1}^n y_{1,j} x_{1,j} \right) \left(\sum_{j=1}^n y_{2,j} x_{2,j} \right) \cdots \left(\sum_{j=1}^n y_{n,j} x_{n,j} \right).$$

$$P(\mathbf{x}, \mathbf{y}) := \sum_{\sigma \in S_n} x_{1,\sigma(1)} \cdots x_{n,\sigma(n)}.$$

Upper Bound for Permanent

$$P_0(\mathbf{x}, \mathbf{y}) := \left(\sum_{j=1}^n y_{1,j} x_{1,j} \right) \left(\sum_{j=1}^n y_{2,j} x_{2,j} \right) \cdots \left(\sum_{j=1}^n y_{n,j} x_{n,j} \right).$$

$$P_1(\mathbf{x}, \mathbf{y}) := \left(x_{1,1} + \sum_{j=2}^n y_{1,j} x_{1,j} \right) \cdots \left(\sum_{j=2}^n y_{n,j} x_{n,j} \right) + \cdots + \left(\sum_{j=2}^n y_{1,j} x_{1,j} \right) \cdots \left(x_{n,1} + \sum_{j=2}^n y_{n,j} x_{n,j} \right).$$

$$P(\mathbf{x}, \mathbf{y}) := \sum_{\sigma \in S_n} x_{1,\sigma(1)} \cdots x_{n,\sigma(n)}.$$

Upper Bound for Permanent

$$P_0(\mathbf{x}, \mathbf{y}) := \left(\sum_{j=1}^n y_{1,j} x_{1,j} \right) \left(\sum_{j=1}^n y_{2,j} x_{2,j} \right) \cdots \left(\sum_{j=1}^n y_{n,j} x_{n,j} \right).$$

$$P_1(\mathbf{x}, \mathbf{y}) := \left(x_{1,1} + \sum_{j=2}^n y_{1,j} x_{1,j} \right) \cdots \left(\sum_{j=2}^n y_{n,j} x_{n,j} \right) + \cdots + \left(\sum_{j=2}^n y_{1,j} x_{1,j} \right) \cdots \left(x_{n,1} + \sum_{j=2}^n y_{n,j} x_{n,j} \right).$$
$$\vdots$$

$$P(\mathbf{x}, \mathbf{y}) := \sum_{\sigma \in S_n} x_{1,\sigma(1)} \cdots x_{n,\sigma(n)}.$$

Upper Bound for Permanent

$$P_0(\mathbf{x}, \mathbf{y}) := \left(\sum_{j=1}^n y_{1,j} x_{1,j} \right) \left(\sum_{j=1}^n y_{2,j} x_{2,j} \right) \cdots \left(\sum_{j=1}^n y_{n,j} x_{n,j} \right).$$

$$P_1(\mathbf{x}, \mathbf{y}) := \left(x_{1,1} + \sum_{j=2}^n y_{1,j} x_{1,j} \right) \cdots \left(\sum_{j=2}^n y_{n,j} x_{n,j} \right) + \cdots + \left(\sum_{j=2}^n y_{1,j} x_{1,j} \right) \cdots \left(x_{n,1} + \sum_{j=2}^n y_{n,j} x_{n,j} \right).$$

⋮

$$P_n(\mathbf{x}, \mathbf{y}) := x_{1,n} \sum_{\sigma \in S_{n-1}} x_{2,\sigma(1)} \cdots x_{n-1,\sigma(n-1)} x_{n,\sigma(n-1)} + \cdots + x_{n,n} \sum_{\sigma \in S_{n-1}} x_{1,\sigma(1)} \cdots x_{n-1,\sigma(n-1)}.$$

$$P(\mathbf{x}, \mathbf{y}) := \sum_{\sigma \in S_n} x_{1,\sigma(1)} \cdots x_{n,\sigma(n)}.$$

Open Questions I

- If $f \in \text{mVP}_{\text{quant}}$, then

$$f(\mathbf{x}) = \sum_{\mathbf{b} \in \{0,1\}^{|\mathbf{w}|}} A_f(\mathbf{w} = \mathbf{b}) \cdot g_f(\mathbf{x}, \mathbf{w} = \mathbf{b})$$

where $g_f \in \text{mVP}$ but A_f can potentially have large size and degree.

Open Questions I

- If $f \in \text{mVP}_{\text{quant}}$, then

$$f(\mathbf{x}) = \sum_{\mathbf{b} \in \{0,1\}^{|\mathbf{w}|}} A_f(\mathbf{w} = \mathbf{b}) \cdot g_f(\mathbf{x}, \mathbf{w} = \mathbf{b})$$

where $g_f \in \text{mVP}$ but A_f can potentially have large size and degree.
Is there a polynomial $B(\mathbf{w})$ of small degree and small size such that

$$A_f(\mathbf{b}) = B(\mathbf{b}) \text{ for every } \mathbf{b} \in \{0,1\}^{|\mathbf{w}|}?$$

Open Questions I

- If $f \in \text{mVP}_{\text{quant}}$, then

$$f(\mathbf{x}) = \sum_{\mathbf{b} \in \{0,1\}^{|\mathbf{w}|}} A_f(\mathbf{w} = \mathbf{b}) \cdot g_f(\mathbf{x}, \mathbf{w} = \mathbf{b})$$

where $g_f \in \text{mVP}$ but A_f can potentially have large size and degree.
Is there a polynomial $B(\mathbf{w})$ of small degree and small size such that

$$A_f(\mathbf{b}) = B(\mathbf{b}) \text{ for every } \mathbf{b} \in \{0,1\}^{|\mathbf{w}|}?$$

- $\text{VPH} = \text{Q}_1\text{Q}_2 \cdots \text{Q}_m \text{ C}(\mathbf{x}, \mathbf{z})$ for constantly many alternations?

Can we show that $\text{VP} = \text{VNP}$ implies that $\text{VPH} = \text{VP}$?

Open Questions II

τ -conjecture for Newton polytopes [Koiran-Portier-Tavenas-Thomassé]

Suppose $f(x, y)$ is a bivariate polynomial that can be written as $\sum_{i \in [s]} \prod_{j \in [r]} T_{i,j}(x, y)$, where each $T_{i,j}$ has sparsity at most p . Then the Newton polygon of f has $\text{poly}(s, r, p)$ vertices.

Open Questions II

τ -conjecture for Newton polytopes [Koiran-Portier-Tavenas-Thomassé]

Suppose $f(x, y)$ is a bivariate polynomial that can be written as $\sum_{i \in [s]} \prod_{j \in [r]} T_{i,j}(x, y)$, where each $T_{i,j}$ has sparsity at most p . Then the Newton polygon of f has $\text{poly}(s, r, p)$ vertices.

Transparent Polynomials [Hrubeš - Yehudayoff]

Polynomials that can be projected to bivariates in such a way that all of their monomials become vertices of the resulting Newton polygon.

Open Questions II

τ -conjecture for Newton polytopes [Koiran-Portier-Tavenas-Thomassé]

Suppose $f(x, y)$ is a bivariate polynomial that can be written as $\sum_{i \in [s]} \prod_{j \in [r]} T_{i,j}(x, y)$, where each $T_{i,j}$ has sparsity at most p . Then the Newton polygon of f has $\text{poly}(s, r, p)$ vertices.

Transparent Polynomials [Hrubeš - Yehudayoff]

Polynomials that can be projected to bivariates in such a way that all of their monomials become vertices of the resulting Newton polygon.

They give examples of transparent polynomials with exponential support.

Open Questions II

τ -conjecture for Newton polytopes [Koiran-Portier-Tavenas-Thomassé]

Suppose $f(x, y)$ is a bivariate polynomial that can be written as $\sum_{i \in [s]} \prod_{j \in [r]} T_{i,j}(x, y)$, where each $T_{i,j}$ has sparsity at most p . Then the Newton polygon of f has $\text{poly}(s, r, p)$ vertices.

Transparent Polynomials [Hrubeš - Yehudayoff]

Polynomials that can be projected to bivariates in such a way that all of their monomials become vertices of the resulting Newton polygon.

They give examples of transparent polynomials with exponential support. Can any such polynomial be in VP?

Open Questions II

τ -conjecture for Newton polytopes [Koiran-Portier-Tavenas-Thomassé]

Suppose $f(x, y)$ is a bivariate polynomial that can be written as $\sum_{i \in [s]} \prod_{j \in [r]} T_{i,j}(x, y)$, where each $T_{i,j}$ has sparsity at most p . Then the Newton polygon of f has $\text{poly}(s, r, p)$ vertices.

Transparent Polynomials [Hrubeš - Yehudayoff]

Polynomials that can be projected to bivariates in such a way that all of their monomials become vertices of the resulting Newton polygon.

They give examples of transparent polynomials with exponential support. Can any such polynomial be in VP?

[HY]: There is no transparent polynomial with super-poly support in mVP.

Open Questions II

τ -conjecture for Newton polytopes [Koiran-Portier-Tavenas-Thomassé]

Suppose $f(x, y)$ is a bivariate polynomial that can be written as $\sum_{i \in [s]} \prod_{j \in [r]} T_{i,j}(x, y)$, where each $T_{i,j}$ has sparsity at most p . Then the Newton polygon of f has $\text{poly}(s, r, p)$ vertices.

Transparent Polynomials [Hrubeš - Yehudayoff]

Polynomials that can be projected to bivariates in such a way that all of their monomials become vertices of the resulting Newton polygon.

They give examples of transparent polynomials with exponential support. Can any such polynomial be in VP?

[HY]: There is no transparent polynomial with super-poly support in mVP.

[This work]: There is no transparent polynomial with super-poly support in $\text{mVP}_{\text{sum,prod}}$.

Open Questions II

τ -conjecture for Newton polytopes [Koiran-Portier-Tavenas-Thomassé]

Suppose $f(x, y)$ is a bivariate polynomial that can be written as $\sum_{i \in [s]} \prod_{j \in [r]} T_{i,j}(x, y)$, where each $T_{i,j}$ has sparsity at most p . Then the Newton polygon of f has $\text{poly}(s, r, p)$ vertices.

Transparent Polynomials [Hrubeš - Yehudayoff]

Polynomials that can be projected to bivariates in such a way that all of their monomials become vertices of the resulting Newton polygon.

They give examples of transparent polynomials with exponential support. Can any such polynomial be in VP?

[HY]: There is no transparent polynomial with super-poly support in mVP.

[This work]: There is no transparent polynomial with super-poly support in $\text{mVP}_{\text{sum,prod}}$.

Can we extend this to mVP_{proj} ?

Thank you!