Lower Bounds in Algebraic Complexity via Symmetry and Homomorphism Polynomials

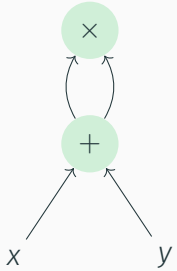
Benedikt Pago (University of Cambridge)

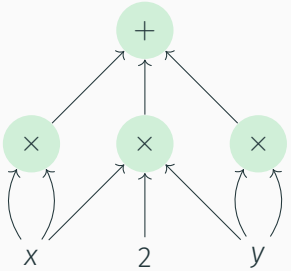
Proof Complexity Workshop, University of Bath, 17 June 2026

Joint work with Prateek Dwivedi and Tim Seppelt (IT-Universitetet i København)

Algebraic complexity

The *complexity* of a polynomial is the size of the smallest algebraic circuit representing it.





VP vs. VNP

Determinant

$$\det_n = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \prod_{i=1}^{n} X_{i,\pi(i)}$$

has poly-size algebraic circuits.

Permanent

$$\operatorname{perm}_n = \sum_{\pi \in S_n} \prod_{i=1}^{n} X_{i,\pi(i)}$$

VP vs. VNP (Valiant, 1979)

Does perm_n admit poly-size algebraic circuits?

Towards Valiant's conjecture

Approach: Prove lower bounds for **restricted** circuit models.

No sub-exponential size family of *monotone* circuits computes the permanent.

[Jerrum, Snir 1982]

No sub-exponential size family of *depth 3* circuits computes the permanent.

[Grigoriev, Karpinski 1998]

But: Both methods yield similar lower bounds for the determinant.

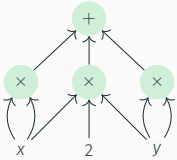
Theorem (Dawar, Wilsenach 2020)

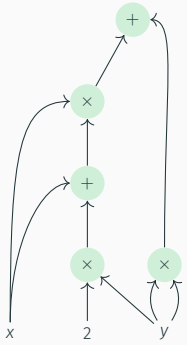
There are no subexponential-size ***symmetric circuits*** *for* perm_n.
There are polynomial-size ***symmetric circuits*** *for* $\det_n$.

Symmetry in polynomials and circuits

The polynomial $(x + y)^2$ is symmetric under exchanging x and y.

A *symmetric circuit* is one with an *automorphism* swapping x and y.





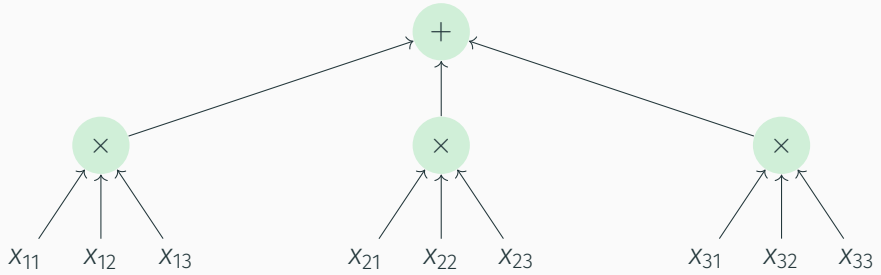
Matrix-symmetric polynomials and circuits

For a *matrix polynomial* p over $X_n = \{x_{ij} \mid 1 \leq i, j \leq n\}$, we consider $\mathbf{Sym}_n \times \mathbf{Sym}_n$-symmetry.

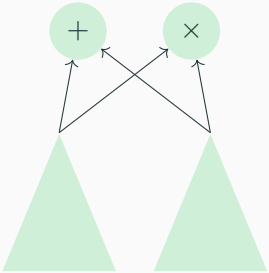
Each $(\pi, \sigma) \in \mathbf{Sym}_n \times \mathbf{Sym}_n$ maps x_{ij} to $x_{\pi(i)\sigma(j)}$.

Matrix-symmetric polynomials and circuits

A polynomial / circuit over X_n is *matrix-symmetric* if it is invariant under the action of $\mathbf{Sym}_n \times \mathbf{Sym}_n$.

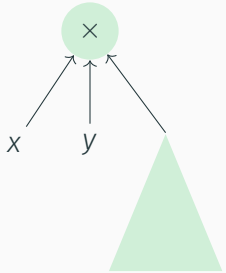


symVP
symmetric circuits of polynomial orbit-size



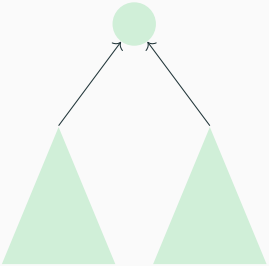
VP
poly-size circuits

symVS
symmetric skew circuits of polynomial orbit-size



VS
poly-size skew circuits

symVF
symmetric formulas of polynomial orbit-size



VF
poly-size formulas

Main result

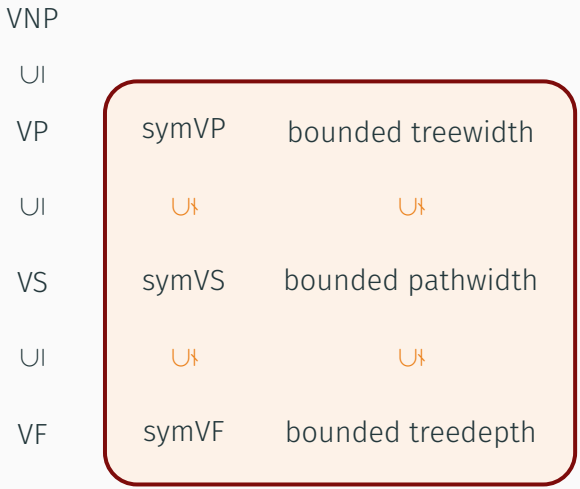
Open problem:

Do the algebraic complexity classes VF, VS, VP form a strict hierarchy?

Theorem

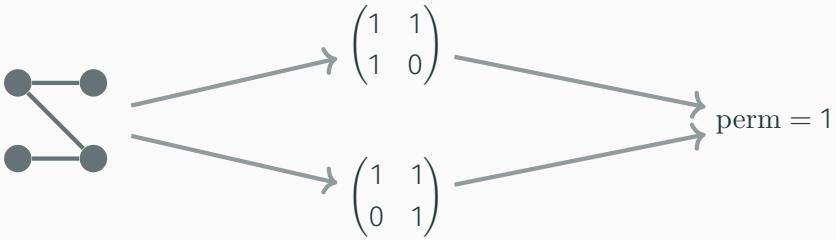
$$\mathrm{symVF} \subsetneq \mathrm{symVS} \subsetneq \mathrm{symVP}.$$

A Symmetric Algebraic Complexity Theory



Graph-theoretic semantics of symmetric polynomials

Symmetric polynomials are functions of (n, n)-vertex bipartite graphs.
E.g., the permanent $\mathrm{perm}_n(G)$ is the number of perfect matchings in G.



For a bipartite multigraph F and $n \in \mathbb{N}$,

$$\hom_{F,n} \coloneqq \sum_{h\colon V(F)\to[n]\uplus[n]} \prod_{uv\in E(F)} X_{h(u),h(v)}$$

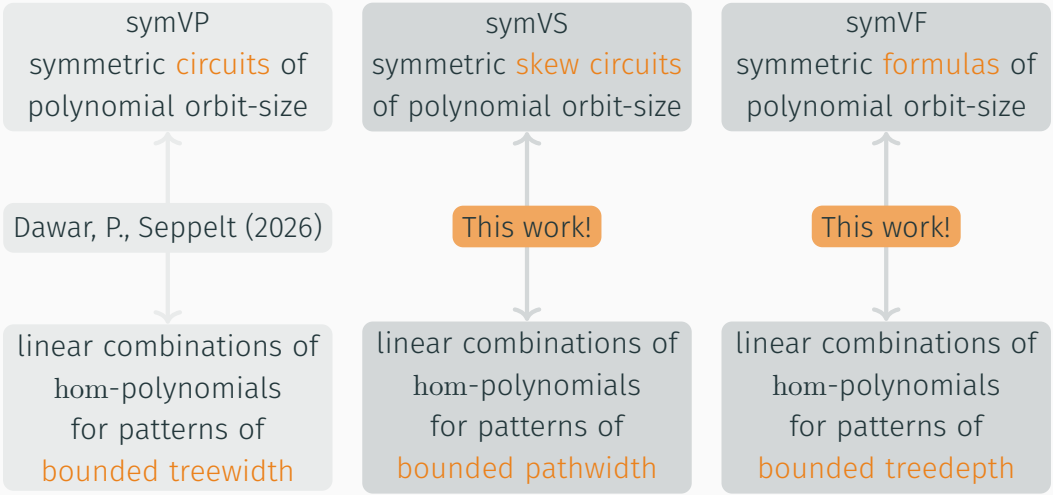
Fact

A polynomial is symmetric $\iff$ it is a linear combination of $\hom$-polynomials.

Corollary

Every graph parameter can be written as

$$p_n(\star) = \sum \alpha_{F,n} \hom(F,\star).$$


symVP
symmetric circuits of
polynomial orbit-size
Dawar, P., Seppelt (2026)
linear combinations of
hom-polynomials
for patterns of
bounded treewidth
symVS
symmetric skew circuits
of polynomial orbit-size
This work!
linear combinations of
hom-polynomials
for patterns of
bounded pathwidth
symVF
symmetric formulas of
polynomial orbit-size
This work!
linear combinations of
hom-polynomials
for patterns of
bounded treedepth

Proof of the separation result

Theorem

$$\text{symVF} \subsetneq \text{symVS} \subsetneq \text{symVP}.$$

Proof.

E.g. for symVS $\subsetneq$ symVP, show that there exist graphs (F_n) of bounded treewidth such that $\hom_{F,n}$ is not a linear combination of $\hom$-polynomials of bounded pathwidth.

$\Rightarrow$ via theory of ***homomorphism indistinguishability***. $\square$

Strength of the lower bounds

The power of the symmetric circuit models

Theorem

1. symVP *contains* ***VP-complete polynomials****, namely* $(\mathrm{hom}_{F_n,n})$ *for* $\mathrm{tw}(F_n) \in O(1), \mathrm{pw}(F_n) \geq \Omega(\log n)$ *(for example binary trees).*
2. symVS *contains* ***VS-complete polynomials****, namely* $(\mathrm{hom}_{F_n,n})$ *for* $\mathrm{pw}(F_n) \in O(1), \mathrm{td}(F_n) \geq \Omega(\log n)$ *(for example paths).*

Does symmetric VP capture all of VP?

Theorem

If (p_n) is a linear combination of hom*-polynomials of pattern graphs of size at most $n^{1-\varepsilon}$, then $(p_n) \in \mathsf{VP} \iff (p_n) \in \mathsf{symVP}$ (assuming VFPT $\neq$ VW[1]).*

Proof.

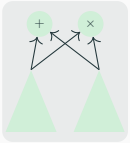
- Assuming VFPT $\neq$ VW[1], hom-polynomials of unbounded treewidth do not admit poly-size circuits.
- $\Rightarrow$ If (p_n) is a linear combination of hom-polynomials of unbounded treewidth, it is not in VP. Else, it is even contained in symVP.

□

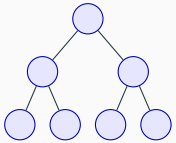
Outlook: Applications in proof complexity?

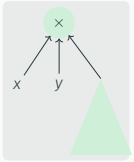
- In the **Ideal Proof System** (IPS), proofs are algebraic circuits.
- Can we use the homomorphism-framework to show lower bounds for symmetric IPS proofs?
- So far, we only have upper bounds [Dawar, Grädel, Kullmann, P. 2025].
- **Challenge:** Design hard symmetric instances in variables (x_{ij}).

Wrap-up

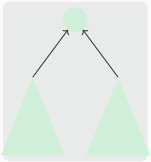


symVP ≈ treewidth





symVS ≈ pathwidth



symVF ≈ treedepth