Symmetric Algebraic Circuits and Homomorphism Polynomials

Anuj Dawar [1], **Benedikt Pago** [1], Tim Seppelt [2]

AlMoTh 2025, Bamberg

[1]University of Cambridge

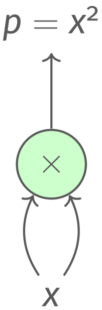
[2]RWTH Aachen University

RWTH AACHEN UNIVERSITY

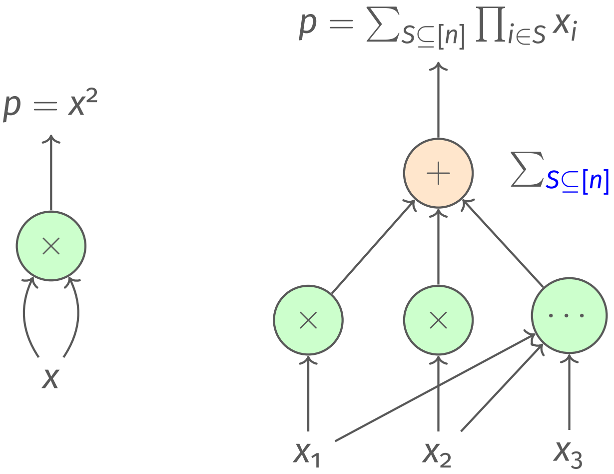
UNIVERSITY OF CAMBRIDGE
Department of Computer Science and Technology

Algebraic Circuits

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

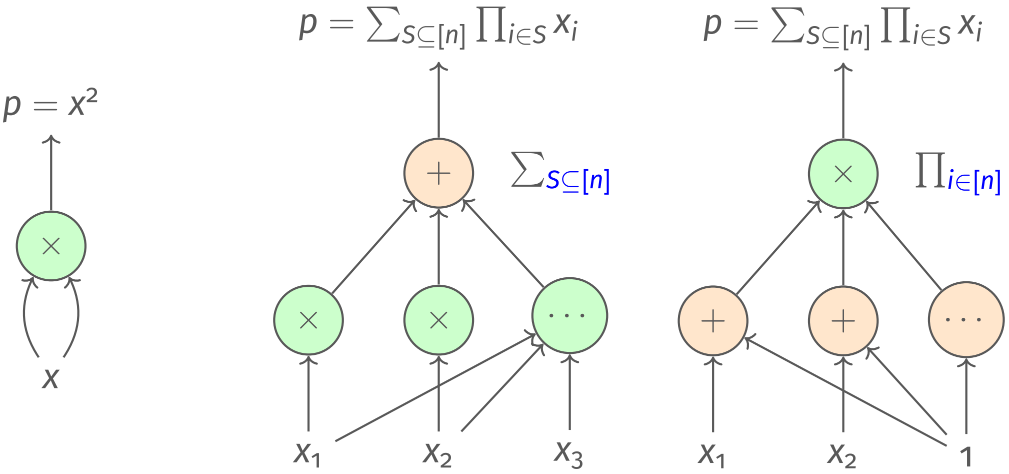


The **complexity of a polynomial** p is the *size* of the smallest *algebraic circuit* representing p.



Algebraic Circuits

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



Determinant

$$\mathrm{det}_n = \sum_{\pi \in \mathbf{Sym}_n} \mathrm{sgn}(\pi) \cdot x_{1\pi(1)} \cdots x_{n\pi(n)}$$

Circuit complexity: $\mathcal{O}(n^4)$.

Permanent

$$\mathrm{perm}_n = \sum_{\pi \in \mathbf{Sym}_n} x_{1\pi(1)} \cdots x_{n\pi(n)}$$

Circuit complexity: **???** (at most $\mathcal{O}(2^n \cdot n^2)$).

Determinant

$$\det_n = \sum_{\pi \in \mathbf{Sym}_n} \operatorname{sgn}(\pi) \cdot x_{1\pi(1)} \cdots x_{n\pi(n)}$$

Circuit complexity: $\mathcal{O}(n^4)$.

Permanent

$$\operatorname{perm}_n = \sum_{\pi \in \mathbf{Sym}_n} x_{1\pi(1)} \cdots x_{n\pi(n)}$$

Circuit complexity: **???** (at most $\mathcal{O}(2^n \cdot n^2)$).

“VP $=$ VNP?” is the question “Does $(\operatorname{perm}_n)_{n\in\mathbb{N}}$ admit polynomial-size algebraic circuits?”

Theorem (Dawar, Wilsenach; 2020)

1. *There are polynomial-size symmetric circuits for* $(\mathrm{det}_n)_{n\in\mathbb{N}}$.
2. *There are no symmetric circuits for* $(\mathrm{perm}_n)_{n\in\mathbb{N}}$ *of subexponential size.*

Theorem (Dawar, Wilsenach; 2020)

1. *There are polynomial-size symmetric circuits for* $(\text{det}_n)_{n\in\mathbb{N}}$.
2. *There are no symmetric circuits for* $(\text{perm}_n)_{n\in\mathbb{N}}$ *of subexponential size.*

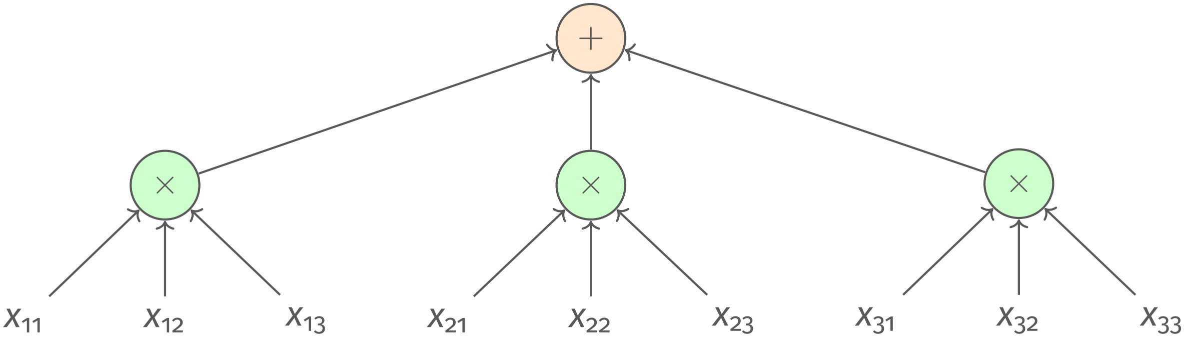
In this work: Complete characterisation of polynomials with polynomial-size symmetric circuits.

Symmetric algebraic circuits

- Let $\mathcal{X}_{n,m} := \{x_{ij} \mid i \in [n], j \in [m]\}$.
- $\textbf{Sym}_n \times \textbf{Sym}_m$ acts on $\mathcal{X}_{n,m}$: For $(\pi, \sigma) \in \textbf{Sym}_n \times \textbf{Sym}_m$, it is $(\pi, \sigma)(x_{ij}) = x_{\pi(i)\sigma(j)}$.
- An algebraic circuit C over $\mathcal{X}_{n,m}$ is $\textbf{Sym}_n \times \textbf{Sym}_m$-symmetric if the action on $\mathcal{X}_{n,m}$ extends to automorphisms of C.

Symmetric algebraic circuits

- Let $\mathcal{X}_{n,m} := \{x_{ij} \mid i \in [n], j \in [m]\}$.
- $\textbf{Sym}_n \times \textbf{Sym}_m$ acts on $\mathcal{X}_{n,m}$: For $(\pi, \sigma) \in \textbf{Sym}_n \times \textbf{Sym}_m$, it is $(\pi, \sigma)(x_{ij}) = x_{\pi(i)\sigma(j)}$.
- An algebraic circuit C over $\mathcal{X}_{n,m}$ is $\textbf{Sym}_n \times \textbf{Sym}_m$-symmetric if the action on $\mathcal{X}_{n,m}$ extends to automorphisms of C.



- Every $\mathbf{Sym}_n \times \mathbf{Sym}_m$-symmetric polynomial $p \in \mathbb{Q}[\mathcal{X}_{n,m}]$ defines a $\mathbb{Q}$-valued function on *bipartite (n, m)-vertex graphs*.
- **Example:** $\mathrm{perm}_n(G)$ is the number of perfect matchings in a bipartite (n, n)-vertex graph G.

Fact

Every $\mathbf{Sym}_n \times \mathbf{Sym}_m$*-symmetric polynomial can be written as a linear combination of* ***homomorphism*** *or* ***subgraph polynomials****.*

Fact

Every $\textbf{Sym}_n \times \textbf{Sym}_m$*-symmetric polynomial can be written as a linear combination of* ***homomorphism*** *or* ***subgraph polynomials****.*

Let F be a bipartite graph. For each $n, m \in \mathbb{N}$, the following polynomial evaluated in an (n, m)-vertex graph G counts the number of homomorphisms from F to G.

$$\mathrm{hom}_{F,n,m} := \sum_{h \colon V(F) \to [n] \uplus [m]} \prod_{ab \in E(F)} x_{h(a)h(b)}.$$

Main result

Let $\mathfrak{T}^k_{n,m}$ be the set of $\mathbb{Q}$-linear combinations of polynomials $\hom_{F_i,n,m}$ where all F_i have *treewidth at most k*.

Theorem

For every family of polynomials $p_{n,m} \in \mathbb{Q}[\mathcal{X}_{n,m}]$, the following are equivalent:

1. *there exists a constant $k \in \mathbb{N}$ such that $p_{n,m} \in \mathfrak{T}^k_{n,m}$ for all $n, m \in \mathbb{N}$,*
2. *the $p_{n,m}$ admit $\mathbf{Sym}_n \times \mathbf{Sym}_m$-symmetric circuits of size polynomial in $n + m$.*

Theorem (Curticapean, Dell, Marx; 2017)

The problem of computing linear combinations of induced subgraph counts, parametrized by their size, is

- *in* FPT, *if it is expressible as a linear combination of homomorphism counts from bounded-treewidth graphs,*
- #W[1]-*hard, otherwise.*

Related work

Theorem (Curticapean, Dell, Marx; 2017)

The problem of computing linear combinations of induced subgraph counts, parametrized by their size, is

- *in* FPT, *if it is expressible as a linear combination of homomorphism counts from bounded-treewidth graphs,*
- #W[1]-*hard, otherwise.*

Differences to our result:

- Syntactic complexity of polynomials vs computational complexity of the counting functions.

Theorem (Curticapean, Dell, Marx; 2017)

The problem of computing linear combinations of induced subgraph counts, parametrized by their size, is

- *in* FPT, *if it is expressible as a linear combination of homomorphism counts from bounded-treewidth graphs,*
- #W[1]-*hard, otherwise.*

Differences to our result:

- Syntactic complexity of polynomials vs computational complexity of the counting functions.
- Polynomials $p_{n,m}$ can be different for each target graph size (n, m).

Theorem (Curticapean, Dell, Marx; 2017)

The problem of computing linear combinations of induced subgraph counts, parametrized by their size, is

- *in* FPT, *if it is expressible as a linear combination of homomorphism counts from bounded-treewidth graphs,*
- #W[1]-*hard, otherwise.*

Differences to our result:

- Syntactic complexity of polynomials vs computational complexity of the counting functions.
- Polynomials $p_{n,m}$ can be different for each target graph size (n, m).
- Our lower bound is unconditional.

Making the characterisation more explicit

Theorem

For every family of polynomials $p_{n,m} \in \mathbb{Q}[\mathcal{X}_{n,m}]$, the following are equivalent:

1. *there exists a constant $k \in \mathbb{N}$ such that $p_{n,m} \in \mathfrak{T}^k_{n,m}$ for all $n, m \in \mathbb{N}$,*
2. *the $p_{n,m}$ admit $\mathbf{Sym}_n \times \mathbf{Sym}_m$-symmetric circuits of orbit size polynomial in $n + m$.*

Problem: When is a polynomial (not) in $\mathfrak{T}^k_{n,m}$?

Making the characterisation more explicit

Theorem

For every family of polynomials $p_{n,m} \in \mathbb{Q}[\mathcal{X}_{n,m}]$, the following are equivalent:

1. *there exists a constant $k \in \mathbb{N}$ such that $p_{n,m} \in \mathfrak{T}^k_{n,m}$ for all $n, m \in \mathbb{N}$,*
2. *the $p_{n,m}$ admit $\mathbf{Sym}_n \times \mathbf{Sym}_m$-symmetric circuits of orbit size polynomial in $n + m$.*

Problem: When is a polynomial (not) in $\mathfrak{T}^k_{n,m}$?

- If $p_{n,m}$ is the *subgraph count polynomial* of a sublinear-size graph $F_{n,m}$, then $p_{n,m}$ is tractable iff $\mathrm{vc}(F_{n,m})$ is bounded by a constant.

Theorem

For every family of polynomials $p_{n,m} \in \mathbb{Q}[\mathcal{X}_{n,m}]$, the following are equivalent:

1. *there exists a constant $k \in \mathbb{N}$ such that $p_{n,m} \in \mathfrak{T}^k_{n,m}$ for all $n, m \in \mathbb{N}$,*
2. *the $p_{n,m}$ admit $\mathbf{Sym}_n \times \mathbf{Sym}_m$-symmetric circuits of orbit size polynomial in $n + m$.*

Problem: When is a polynomial (not) in $\mathfrak{T}^k_{n,m}$?

- If $p_{n,m}$ is the *subgraph count polynomial* of a sublinear-size graph $F_{n,m}$, then $p_{n,m}$ is tractable iff $\mathrm{vc}(F_{n,m})$ is bounded by a constant.
- **Conjecture:** In general, $\min\{\mathrm{vc}(F), \mathrm{vc}(\overline{F})\}$ is the criterion for tractability of subgraph polynomials.

Summary

- With respect to symmetric circuits, VP $\neq$ VNP (Dawar, Wilsenach; 2020).

Summary

- With respect to symmetric circuits, VP $\neq$ VNP (Dawar, Wilsenach; 2020).
- "Symmetric VP" can be characterised as the class of all polynomials expressible via *bounded-treewidth homomorphism counts*.

Summary

- With respect to symmetric circuits, VP $\neq$ VNP (Dawar, Wilsenach; 2020).
- "Symmetric VP" can be characterised as the class of all polynomials expressible via *bounded-treewidth homomorphism counts*.
- In special cases, such as subgraph polynomials, this translates to explicit criteria for super-polynomial lower bounds.

Summary

- With respect to symmetric circuits, VP $\neq$ VNP (Dawar, Wilsenach; 2020).
- “Symmetric VP” can be characterised as the class of all polynomials expressible via *bounded-treewidth homomorphism counts*.
- In special cases, such as subgraph polynomials, this translates to explicit criteria for super-polynomial lower bounds.
- **Application:** A (conditional) complexity dichotomy for the *immanant* polynomials due to Curticapean (2021) holds unconditionally for symmetric circuits.