Advances in circuit lower bounds via symmetry

Benedikt Pago

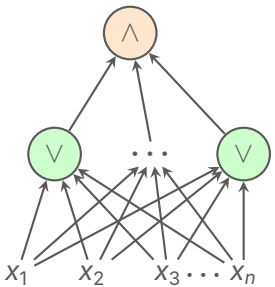
29.10.2026, Algorithms and Complexity Theory Seminar, Oxford

University of Cambridge



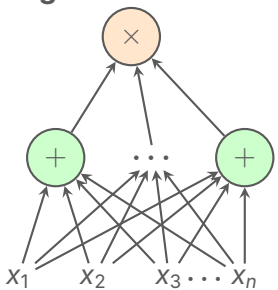
Circuit complexity

Boolean circuits:



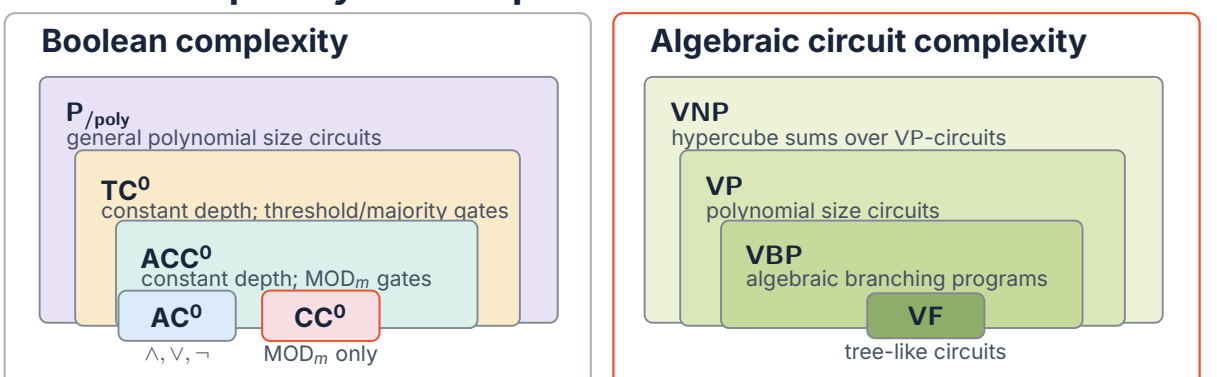
- Compute Boolean functions.
- **Motivation:** $\mathsf{P} \subseteq \mathsf{P}_{/\mathrm{poly}}$, so lower bounds against $\mathsf{P}_{/\mathrm{poly}}$ could be a way to attack P vs NP.

Algebraic circuits:



- Compute syntactic polynomials.
- **Motivation:** Valiant suggested algebraic circuit lower bounds as a stepping stone towards the Boolean case.

Circuit complexity landscape



Algebraic complexity

The central problem of algebraic complexity

Determinant

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

Circuit complexity: $\operatorname{poly}(n)$ (even more: $\det \in \mathrm{VBP}$).

Permanent

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

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

Conjecture (Valiant, 1979)

No poly-size circuits for perm_n exist ($\mathrm{VP} \neq \mathrm{VNP}$).

Lower bounds for restricted circuit models

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

[Jerrum and Snir 1982]

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

[Grigoriev and Karpinski 1998]

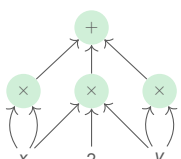
But: Both methods yield similar lower bounds for the determinant.

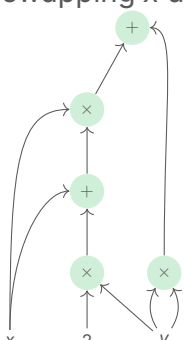
Theorem (Dawar, Wilsenach 2020)

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

Symmetric 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.





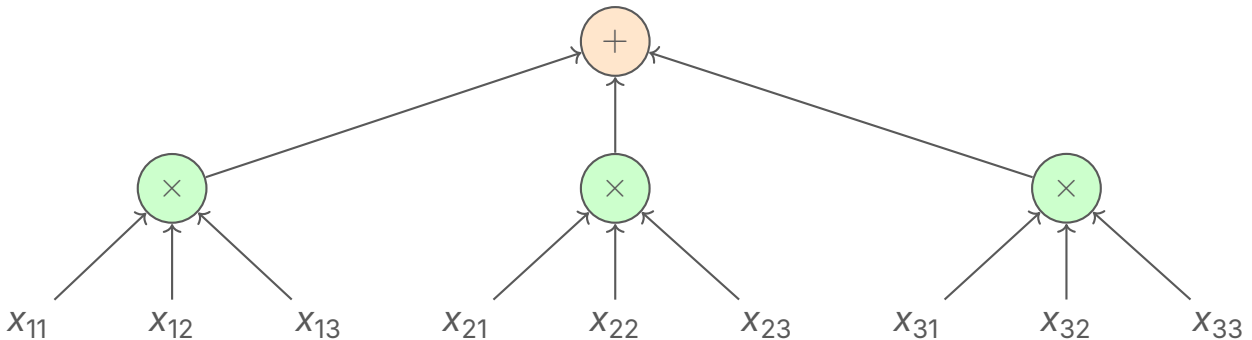
Definition

For X a set of variables, $\Gamma \leq \mathbf{Sym}(X)$ a permutation group,

- a polynomial $p \in \mathbb{F}[X]$ is Γ-*symmetric* if $\pi(p) = p$ for every $\pi \in \Gamma$,
- a circuit C computing p is Γ-*symmetric* if for every $\pi \in \Gamma$, there exists a circuit automorphism of C that acts like π on the input variables of C.

For a *matrix polynomial* p over $X_n = \{x_{ij} \mid i, j \in [n]\}$, 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 $x_{\pi(i)\sigma(j)}$.

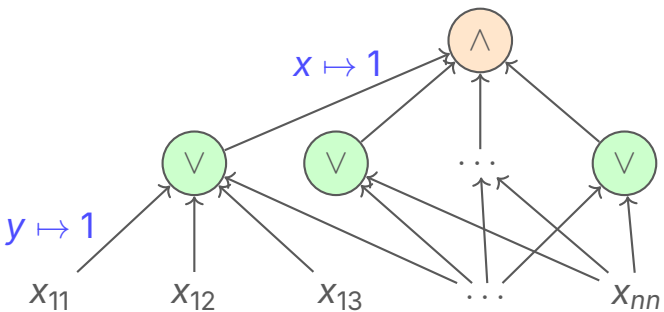


A $\mathbf{Sym}_3 \times \mathbf{Sym}_3$-symmetric circuit

Symmetric circuits and logic

Sentences of *first-order logic* over (bipartite) graphs uniformly define families of matrix-symmetric Boolean circuits:

$\psi = \forall x \exists y\ Exy$ evaluated in an $(n \times n)$-adjacency matrix $(x_{ij})_{i,j \in [n]}$:



- Every FO-sentence with k variables defines a uniform symmetric circuit family $(C_n)_{n\in\mathbb{N}}$, where in each C_n, each gate can be annotated with an *assignment* $\alpha\colon [k] \to [n]$ to the *free variables* of the respective subformula.
- **Group-theoretic support theorem:** This is true in general symmetric circuit families of (orbit) size $\leq n^k$:

Theorem

Fix a constant $k \in \mathbb{N}$ and a family $(C_n)_{n\in\mathbb{N}}$ of $\mathbf{Sym}_n \times \mathbf{Sym}_n$-symmetric circuits. Let g be a gate in C_n and assume:

$$|\,\mathbf{Orb}(g)| = |\{(\pi,\sigma)(g) \mid (\pi,\sigma) \in \mathbf{Sym}_n \times \mathbf{Sym}_n\}| \leq n^k.$$

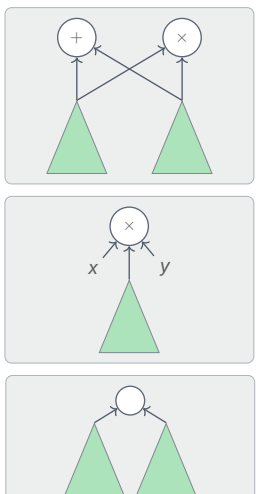
Then there are up to k rows and columns of $(x_{ij})_{i,j\in[n]}$, the so-called support of g, such that any permutation that fixes these also fixes g.

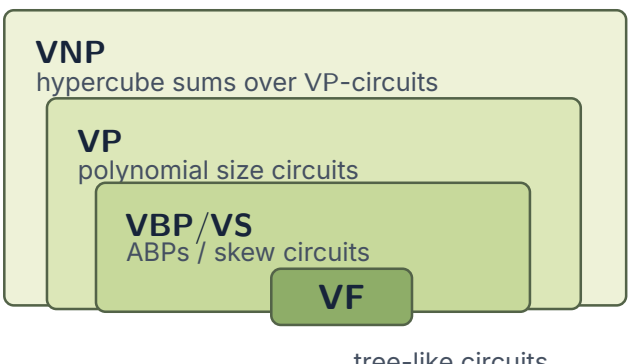
Consequence of the support theorem: Lower bound techniques from finite model theory carry over to symmetric circuits.

In particular, the following *equivalence relations on graphs* are the same:

- k-dimensional Weisfeiler Leman equivalence
- indistinguishability in $(k+1)$-variable counting logic ($\equiv_{\mathcal{C}^{k+1}}$)
- *homomorphism indistinguishability* over patterns of treewidth $\leq k$
- Duplicator wins the bijective $(k+1)$-pebble game
- indistinguishability by *matrix-symmetric circuits* of support size $k+1$ ($\approx n^{k+1}$ circuit size)

Algebraic complexity hierarchy





Symmetric versions of algebraic complexity classes

Definition

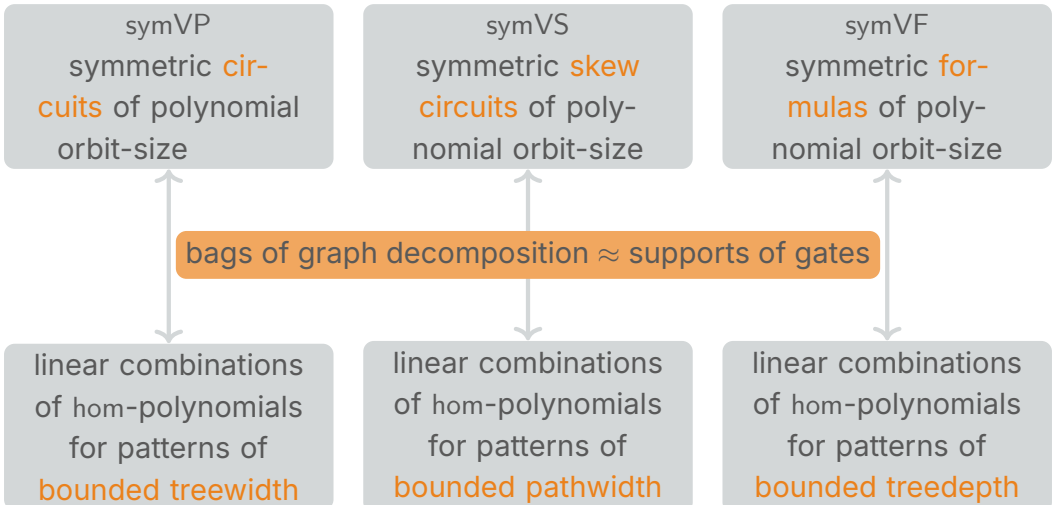
A family $(p_n)_{n\in\mathbb{N}}$ of matrix-symmetric polynomials is in...

- $\mathrm{sym}\mathsf{VP}$ if it is computable with matrix-symmetric circuits of polynomial orbit size,
- $\mathrm{sym}\mathsf{VS}$ if it is computable with matrix-symmetric skew circuits of polynomial orbit size,
- $\mathrm{sym}\mathsf{VF}$ if it is computable with matrix-symmetric tree-like circuits of polynomial orbit size.

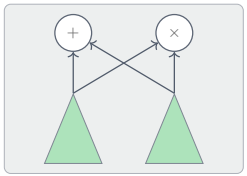
Theorem (ICALP 2020, ITCS 2026, STOC 2026)

$$\mathsf{symVF} \subsetneq \mathsf{symVS} \subsetneq \mathsf{symVP} \subsetneq \mathsf{VNP}\,.$$

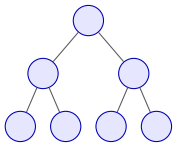
- $\mathsf{symVP} \subsetneq \mathsf{VNP}$: $\mathrm{perm}_n \notin \mathsf{symVP}$ because there are graphs G, H such that $\mathrm{perm}_n(G) \neq \mathrm{perm}_n(H)$, but $G \equiv_{\mathcal{C}^k} H$. [Dawar, Wilsenach 2020]
- **Other separations:** Characterisation of $\mathsf{symVF}, \mathsf{symVS}, \mathsf{symVP}$ in terms of *homomorphism polynomials*. [Dawar, P., Seppelt; Dwivedi, P., Seppelt, 2026].
- For a pattern graph F, and $n \in \mathbb{N}$, $\mathbf{hom}_{F,n}(\bar{x}_{ij})$ is a polynomial such that for any n-vertex graph G, $\mathrm{hom}_{F,n}(G)$ is the *number of homomorphisms* from F to G.

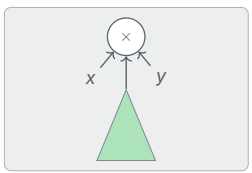

symVP
symmetric circuits of polynomial orbit-size
symVS
symmetric skew circuits of polynomial orbit-size
symVF
symmetric formulas of polynomial orbit-size
bags of graph decomposition ≈ supports of gates
linear combinations of hom-polynomials for patterns of bounded treewidth
linear combinations of hom-polynomials for patterns of bounded pathwidth
linear combinations of hom-polynomials for patterns of bounded treedepth

Graph decompositions and circuit shapes



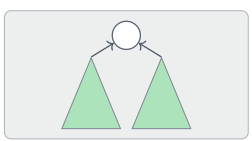
symVP ≈ treewidth



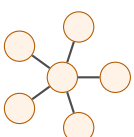


symVS ≈ pathwidth





symVF ≈ treedepth



Proof of the separation result

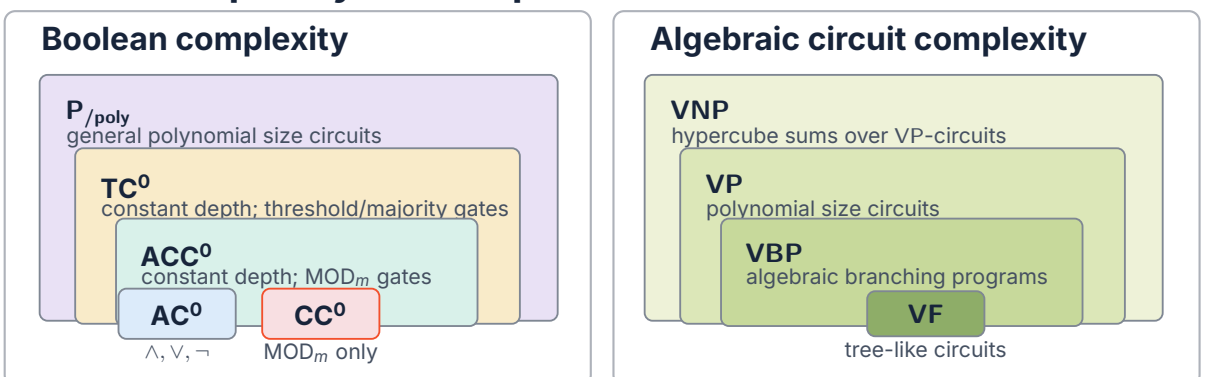
Theorem

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

- $\mathrm{symVS} \subsetneq \mathrm{symVP}$: Find polynomials $p_n \coloneqq \sum_F \alpha_F \cdot \mathrm{hom}_{F,n}$ such that $\mathbf{tw}(F) < \infty$, but $p_n \neq \sum_F \alpha_F \cdot \mathrm{hom}_{F,n}$ whenever $\mathbf{pw}(F) < \infty$.
- Choose F_n as the binary tree with n leaves, and $p_n \coloneqq \mathrm{hom}_{F_n,n}$.
- $\mathbf{tw}(F_n) = 1$, but one can show that $\mathrm{hom}_{F_n,n}$ is **not** a linear combination of bounded-pathwidth hom-polynomials.
- $\mathrm{symVF} \subsetneq \mathrm{symVS}$: analogous for pathwidth versus treedepth.

Boolean circuits: Modular counting versus Boolean connectives

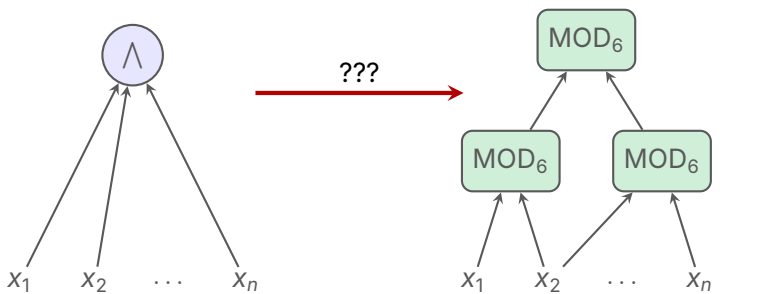
Circuit complexity landscape



The CC^0 versus ACC^0 question

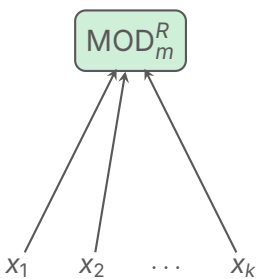
Can circuits with modular counting gates alone simulate Boolean operations efficiently?

[Barrington, Straubing, Thérien 1990]



Boolean AND Circuit **Boolean MOD_6 Circuit**

Modular counting gates



Definition (Boolean modular gates)

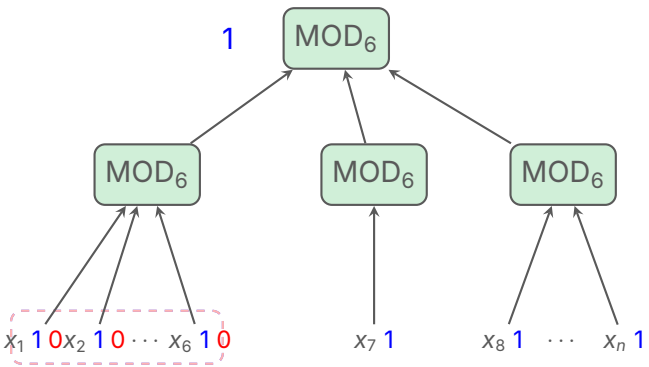
Let $m \in \mathbb{N}, R \subseteq \mathbb{Z}_m$.

$$\mathrm{MOD}_m^R(x_1, \cdots, x_k) = \begin{cases} 1 & \text{if } (\sum x_i \mod m) \in R \\ 0 & \text{otherwise} \end{cases}$$

Why should AND not be easy?

Conjecture ("Exponential Size Hypothesis")

For every depth h and modulus m, there exists $0 < \varepsilon \leq 1$ such that the $\mathrm{CC}_h[m]$-circuit complexity of AND_n is at least $2^{\Omega(n^\varepsilon)}$.



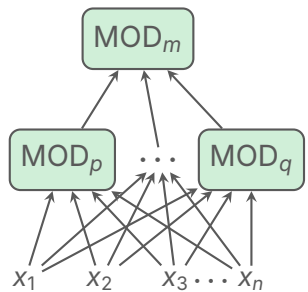
How not to express AND_n

Best known constructions:

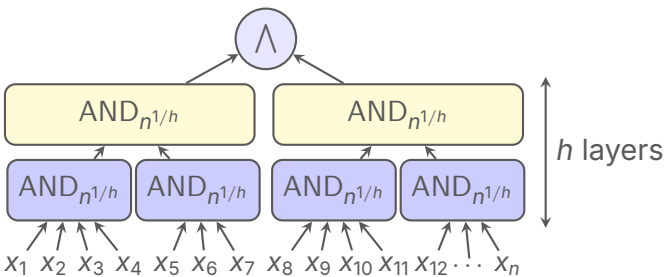
Theorem (Idziak, Kawałek, and Krzaczkowski 2022)

Fix a modulus $m \in \mathbb{N}$ and let $r \geq 2$ be the number of its prime divisors.
AND_n *can be computed by ...*

- *a* MOD_m*-circuit of depth 2 and size* $2^{\mathcal{O}(n^{1/r} \cdot \log n)}$.
- *for every* $h \in \mathbb{N}$*, a* MOD_m*-circuit of depth* $h+1$ *and size* $2^{\mathcal{O}(n^{1/(h\cdot(r-1))} \cdot \log n)}$.



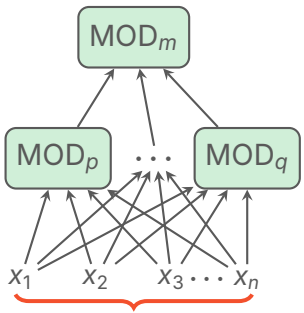
Depth-2 construction



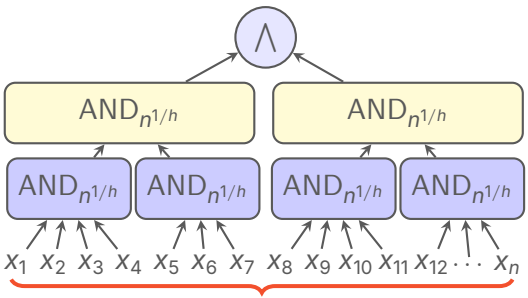
Depth-$(h+1)$ construction

Symmetries of the upper bound constructions

Both constructions are *symmetric* under different permutation groups:



Sym$_n$-symmetric



symmetric under the **Sym**$_n$-stabiliser of the nested block structure

---

Question: Are these circuits **size-optimal** for their respective symmetry groups?

Main result

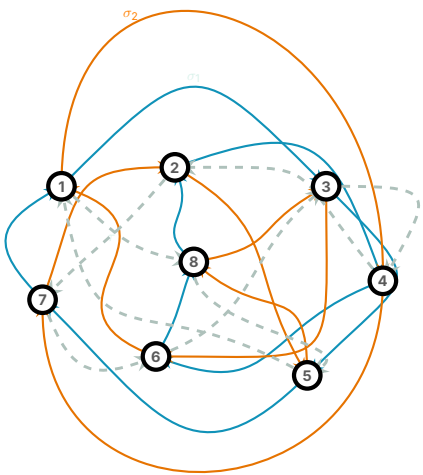
Theorem (P., ICALP 2026)

Fix a modulus $m \in \mathbb{N}$ and let $r \geq 2$ be the number of its prime divisors.
Let C be a MOD_m-circuit computing AND_n.

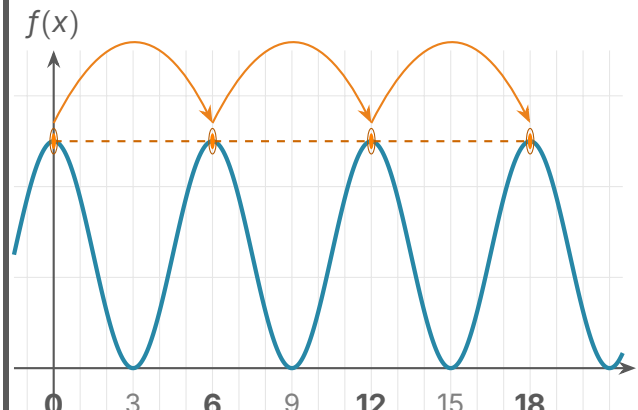
- *If C is $\mathbf{Sym}_n$-symmetric, then its size is at least $2^{\Omega(n^{1/r} \cdot \log n)}$.*
- *If C is nested-block-symmetric with nesting depth h, then its size is at least $2^{\Omega(n^{1/(h \cdot r)} \cdot \log n)}$.*

Both lower bounds are optimal, **Symmetric Exponential Size Hypothesis** confirmed.

Group-theoretic support theorems

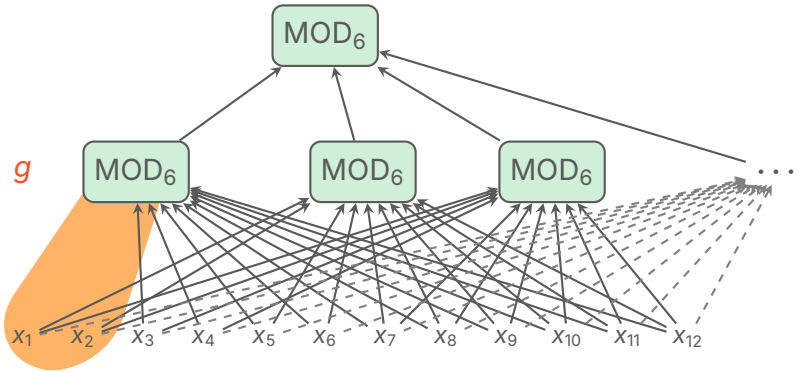


Periodicity of modular functions



$$f(0) = f(6) = f(12) = f(18) = \dots$$

function computed at g
depends only on # of 1s
outside of support
Periodicity: g(0) = g(6) = g(12) ...



$\text{support}(g) = \{x_1, x_2\}$

smallest set whose stabiliser fixes g

Proof

Lemma

symmetric circuit size $\approx$ support size of gates $\approx$ period length of gate functions.

A gate with period length $< n$ cannot compute AND_n!

$\Rightarrow$ To compute AND_n, periods, support sizes and hence circuits must be large.

Conclusion

- The Boolean separation $\mathrm{CC}^0 \neq \mathrm{ACC}^0$ and the algebraic separations between $\mathrm{VF}, \mathrm{VBP}, \mathrm{VP}, \mathrm{VNP}$ have been established for sufficiently symmetric circuits.
- **Future Goal 1:** Show lower bounds under *weaker symmetry assumptions*, i.e., smaller symmetry groups.
- **Future Goal 2:** Show *completeness* of symmetric circuits for interesting classes of polynomials/Boolean functions.
- Support theorem is the **bottleneck** – it only works for groups containing a copy of $\mathbf{Sym}_n$ or $\mathbf{Alt}_n$.

Bibliography i

- Barrington, David A. Mix, Howard Straubing, and Denis Thérien (1990). **"Non-Uniform Automata Over Groups".** In: *Information and Computation* 89.2, pp. 109–132. DOI: 10.1016/0890-5401(90)90007-5. URL: https://doi.org/10.1016/0890-5401(90)90007-5.
- Dawar, Anuj, Benedikt Pago, and Tim Seppelt (2026). **"Symmetric Algebraic Circuits and Homomorphism Polynomials".** In: *17th Innovations in Theoretical Computer Science Conference (ITCS 2026)*. Ed. by Shubhangi Saraf. Vol. 362. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 46:1–46:15. ISBN: 978-3-95977-410-9. DOI: 10.4230/LIPIcs.ITCS.2026.46. URL: https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.ITCS.2026.46.

- Dawar, Anuj and Gregory Wilsenach (2020). **"Symmetric Arithmetic Circuits".** In: *47th International Colloquium on Automata, Languages, and Programming (ICALP 2020)*. Ed. by Artur Czumaj, Anuj Dawar, and Emanuela Merelli. Vol. 168. Leibniz International Proceedings in Informatics (LIPIcs). ISSN: 1868-8969. Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 36:1–36:18. ISBN: 978-3-95977-138-2. DOI: 10.4230/LIPIcs.ICALP.2020.36. URL: https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.ICALP.2020.36.
- Dwivedi, Prateek, Benedikt Pago, and Tim Seppelt (2026). **"Lower Bounds in Algebraic Complexity via Symmetry and Homomorphism Polynomials".** In: *Proceedings of the 58th Annual ACM Symposium on Theory of Computing, STOC 2026, Salt Lake City, UT, USA, June 22-26, 2026*. Ed. by Aditya Bhaskara and Artur Czumaj. ACM, pp. 631–640. DOI: 10.1145/3798129.3800779. URL: https://doi.org/10.1145/3798129.3800779.

Bibliography iii

- Grigoriev, Dima and Marek Karpinski (1998). **"An Exponential Lower Bound for Depth 3 Arithmetic Circuits".** In: *Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing, Dallas, Texas, USA, May 23-26, 1998*. Ed. by Jeffrey Scott Vitter. ACM, pp. 577–582. DOI: 10.1145/276698.276872. URL: https://doi.org/10.1145/276698.276872.
- Idziak, Paweł M., Piotr Kawałek, and Jacek Krzaczkowski (2022). **"Complexity of Modular Circuits".** In: *Proceedings of LICS '22: 37th Annual ACM/IEEE Symposium on Logic in Computer Science*. ACM, 32:1–32:11. DOI: 10.1145/3531130.3533350. URL: https://doi.org/10.1145/3531130.3533350.
- Jerrum, Mark and Marc Snir (July 1982). **"Some Exact Complexity Results for Straight-Line Computations over Semirings".** en. In: *Journal of the ACM* 29.3, pp. 874–897. ISSN: 0004-5411, 1557-735X. DOI: 10.1145/322326.322341. URL: https://dl.acm.org/doi/10.1145/322326.322341.

Valiant, L. G. (1979). **“Completeness classes in algebra”.** en. In: *Proceedings of the eleventh annual ACM symposium on Theory of computing - STOC ’79*. Atlanta, Georgia, United States: ACM Press, pp. 249–261. doi: 10.1145/800135.804419.