Optimal Lower Bounds for Symmetric Modular Circuits

Benedikt Pago

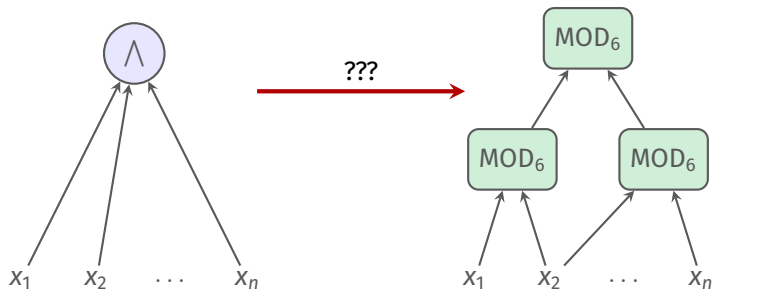
08.07.2026, ICALP 2026, Royal Holloway, University of London

University of Cambridge

The CC^0 versus ACC^0 question

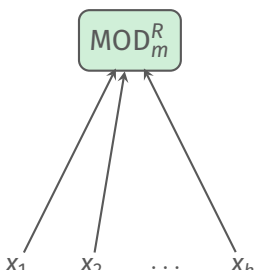
Can circuits with modular counting gates alone simulate Boolean operations efficiently?

(Barrington, Straubing, and 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 ask the question?

Definition

$\mathbf{CC^0}$: The class of all Boolean functions computable by families of polynomial-size depth-h MOD_m-circuits, for constant $h, m \in \mathbb{N}$.
$\mathbf{ACC^0}$: Like CC^0 but with $\{\mathrm{MOD}_m, \mathrm{AND}\}$-circuits.

- Determining the CC^0-complexity of AND_n would resolve the circuit complexity question "$\mathrm{CC}^0 = \mathrm{ACC}^0$?"

Why ask the question?

Definition

$\mathbf{CC^0}$: The class of all Boolean functions computable by families of polynomial-size depth-h MOD_m-circuits, for constant $h, m \in \mathbb{N}$.
$\mathbf{ACC^0}$: Like CC^0 but with $\{\mathrm{MOD}_m, \mathrm{AND}\}$-circuits.

- Determining the CC^0-complexity of AND_n would resolve the circuit complexity question "$\mathrm{CC}^0 = \mathrm{ACC}^0$?"
- The dual question (simulation of MOD-gates by Boolean circuits) was resolved long ago.

(Håstad 1986)

Why ask the question?

Definition

$\mathbf{CC^0}$: The class of all Boolean functions computable by families of polynomial-size depth-h MOD_m-circuits, for constant $h, m \in \mathbb{N}$.
$\mathbf{ACC^0}$: Like CC^0 but with $\{\mathrm{MOD}_m, \mathrm{AND}\}$-circuits.

- Determining the CC^0-complexity of AND_n would resolve the circuit complexity question "$\mathrm{CC}^0 = \mathrm{ACC}^0$?"
- The dual question (simulation of MOD-gates by Boolean circuits) was resolved long ago. (Håstad 1986)
- Lower bounds imply faster algorithms for solving equations over groups, and for CSPs with global modular constraints. (Idziak, Kawałek, Krzaczkowski, and Weiß 2022 Brakensiek, Gopi, and Guruswami 2022)

Why ask the question?

Definition

$\mathbf{CC^0}$: The class of all Boolean functions computable by families of polynomial-size depth-h MOD_m-circuits, for constant $h, m \in \mathbb{N}$.
$\mathbf{ACC^0}$: Like CC^0 but with $\{\mathrm{MOD}_m, \mathrm{AND}\}$-circuits.

- Determining the CC^0-complexity of AND_n would resolve the circuit complexity question "$\mathrm{CC}^0 = \mathrm{ACC}^0$?"
- The dual question (simulation of MOD-gates by Boolean circuits) was resolved long ago. (Håstad 1986)
- Lower bounds imply faster algorithms for solving equations over groups, and for CSPs with global modular constraints. (Idziak, Kawałek, Krzaczkowski, and Weiß 2022 Brakensiek, Gopi, and Guruswami 2022)
- Upper bounds can be used to construct better locally-decodable codes. (Grolmusz 2000; Efremenko 2012)

Why should AND not be easy?

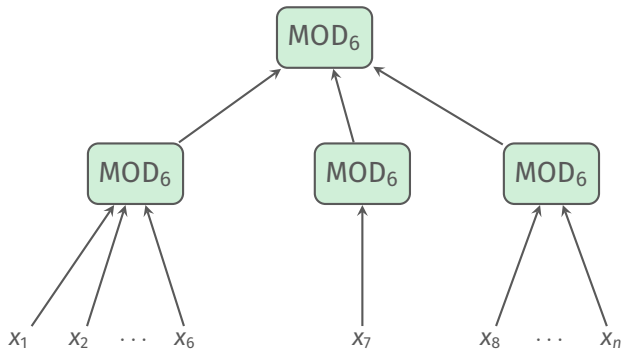
Conjecture ("Exponential Size Hypothesis")

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 $2^{\Omega(n^\varepsilon)}$.

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 $2^{\Omega(n^\varepsilon)}$.

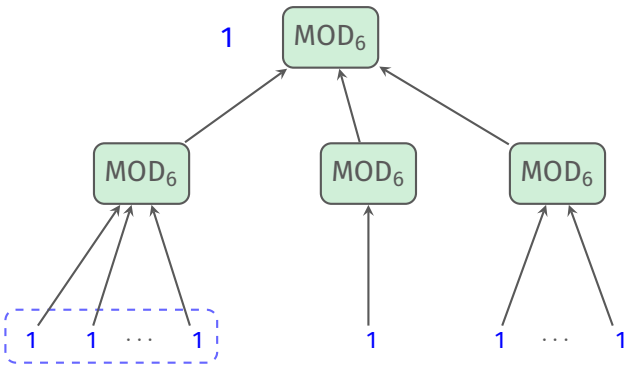


How not to express AND_n

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 $2^{\Omega(n^\varepsilon)}$.

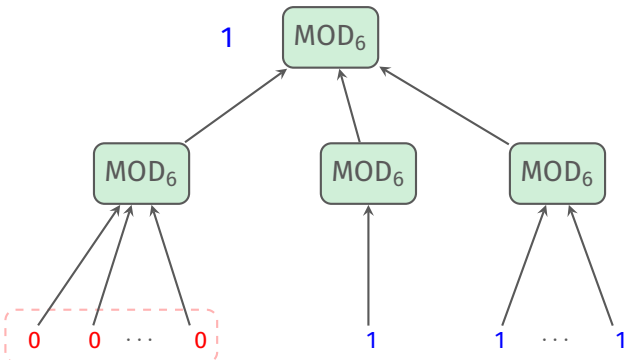


How not to express AND_n

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

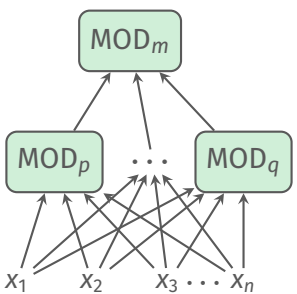
Upper bounds

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 $2^{\mathcal{O}(n^{1/r} \cdot \log n)}$.*



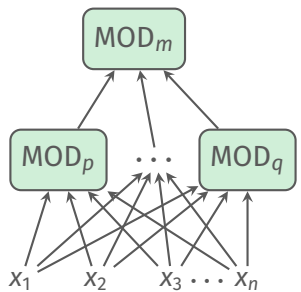
Depth-2 construction

Best known constructions:

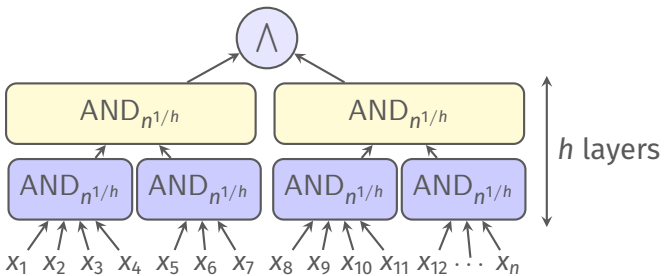
Theorem (Idziak, Kawałek, and Krzaczkowski 2022)

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 $2^{\mathcal{O}(n^{1/(h\cdot(r-1))} \cdot \log n)}$.*



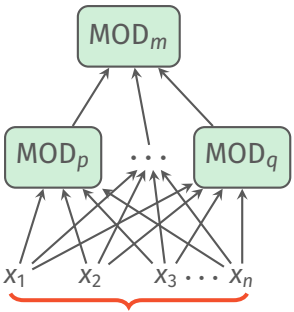
Depth-2 construction



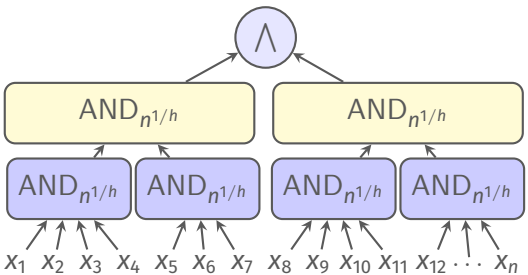
Depth-$(h+1)$ construction

Symmetries of the upper bound constructions

Both constructions are *symmetric* under different permutation groups:

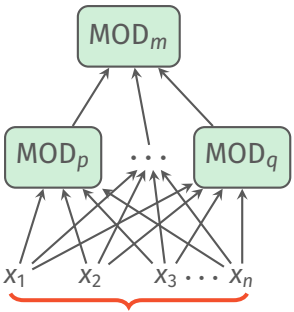


Sym$_n$-symmetric

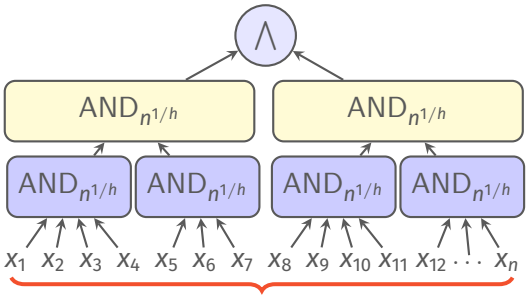


Symmetries of the upper bound constructions

Both constructions are *symmetric* under different permutation groups:



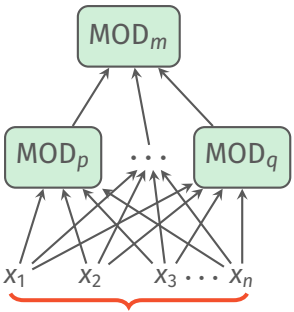
Sym$_n$-symmetric



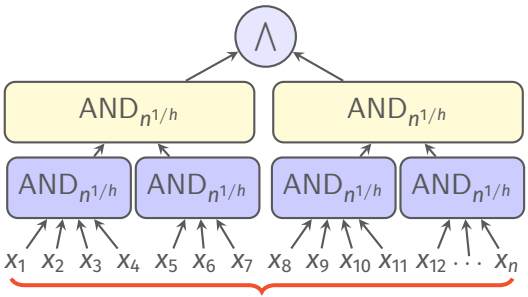
symmetric under the **Sym**$_n$-stabiliser of the nested block structure

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

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 $2^{\Omega(n^{1/(h \cdot r)} \cdot \log n)}$.*

Main result

Theorem

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 $2^{\Omega(n^{1/(h \cdot r)} \cdot \log n)}$.*

$\Rightarrow$ The optimal $\mathbf{Sym}_n$-symmetric construction only has depth 2
– answers a question from (Kawałek and Weiß 2025).

Main result

Theorem

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 $2^{\Omega(n^{1/(h \cdot r)} \cdot \log n)}$.*

$\Rightarrow$ The optimal $\mathbf{Sym}_n$-symmetric construction only has depth 2
– answers a question from (Kawałek and Weiß 2025).

$\Rightarrow$ The nested-block-symmetric construction from IKK-2022 is not size-optimal:
$2^{\Omega(n^{1/(h \cdot r)} \cdot \log n)}$ versus $2^{\mathcal{O}(n^{1/(h \cdot (r-1))} \cdot \log n)}$; but its size can be reduced by doubling the depth.

Main result

Theorem

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.

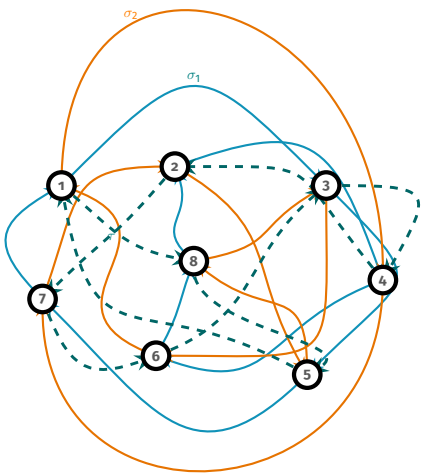
- *If C is $\mathbf{Sym}_n$-symmetric, then its size is at least $2^{\Omega(n^{1/r} \cdot \log n)}$.*
- *If C is nested-block-symmetric with nesting depth h, then its size is at least $2^{\Omega(n^{1/(h \cdot r)} \cdot \log n)}$.*

$\Rightarrow$ The optimal $\mathbf{Sym}_n$-symmetric construction only has depth 2
– answers a question from (Kawałek and Weiß 2025).

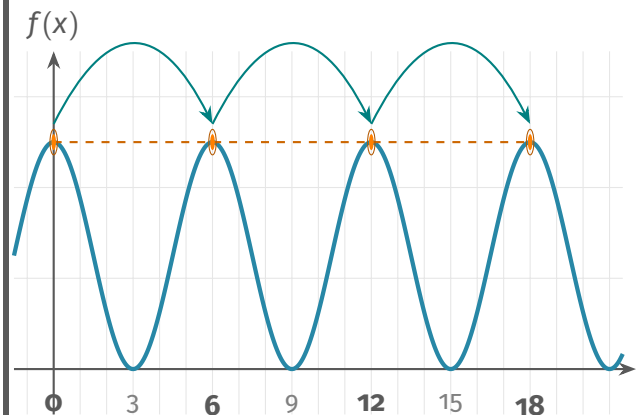
$\Rightarrow$ The nested-block-symmetric construction from IKK-2022 is not size-optimal:
$2^{\Omega(n^{1/(h \cdot r)} \cdot \log n)}$ versus $2^{\mathcal{O}(n^{1/(h \cdot (r-1))} \cdot \log n)}$; but its size can be reduced by doubling the depth.

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

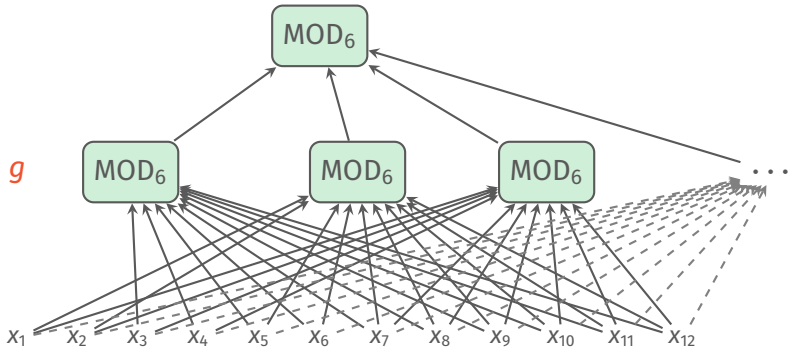
Group-theoretic support theorems

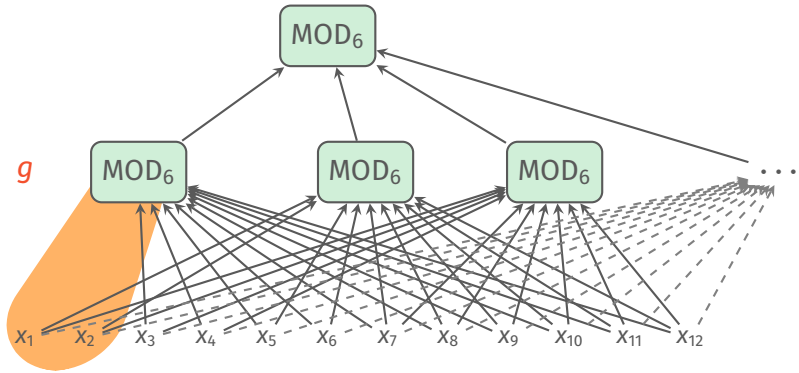


Periodicity of modular functions



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

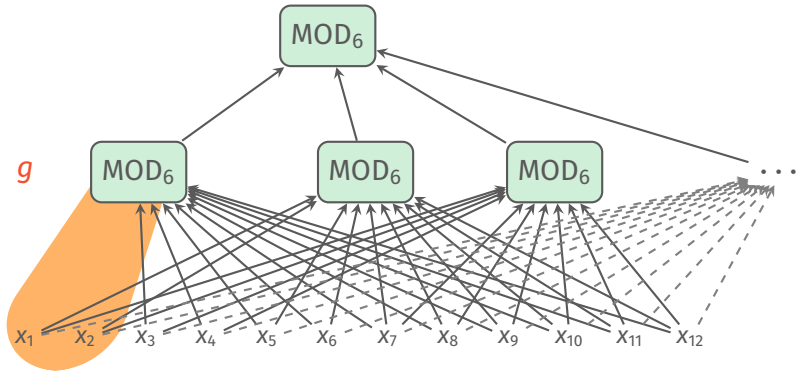

MOD6
g
MOD6
MOD6
MOD6
x1
x2
x3
x4
x5
x6
x7
x8
x9
x10
x11
x12



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

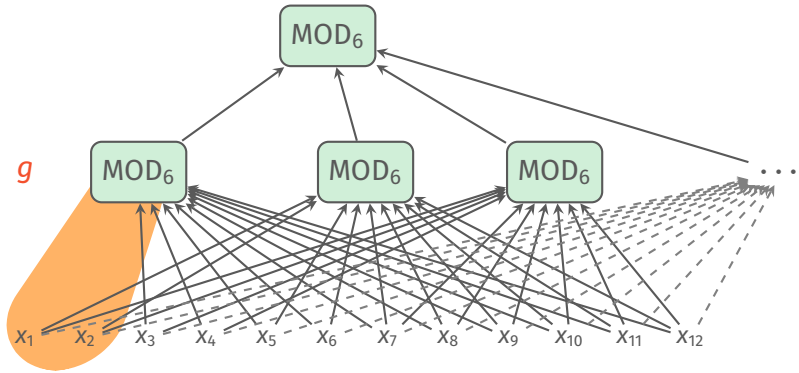
smallest set whose stabiliser fixes g

function computed at g
depends only on # of 1s
outside of support



$\text{support}(g) = \{x_1, x_2\}$
smallest set whose stabiliser fixes g

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.

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!

Proof

Lemma

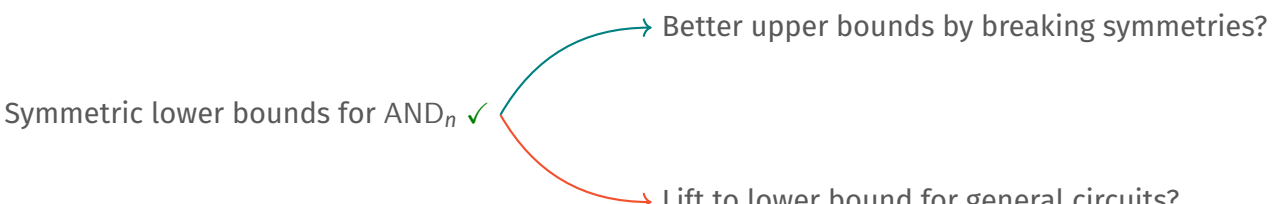
symmetric circuit size $\approx$ *support size of gates* $\approx$ *period length of gate functions.*

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

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

Future work

Solve CC^0 vs ACC^0!



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.
- Brakensiek, Joshua, Sivakanth Gopi, and Venkatesan Guruswami (2022). **"Constraint Satisfaction Problems with Global Modular Constraints: Algorithms and Hardness via Polynomial Representations".** In: *SIAM Journal on Computing* 51.3, pp. 577–626.
- Efremenko, Klim (2012). **"3-Query Locally Decodable Codes of Subexponential Length".** In: *SIAM Journal on Computing* 41.6, pp. 1694–1703. DOI: 10.1137/090772721.
- Grolmusz, Vince (2000). **"Superpolynomial size set-systems with restricted intersections mod 6 and explicit Ramsey graphs".** In: *Combinatorica* 20.1, pp. 71–86. DOI: 10.1007/s004930070032.
- Håstad, Johan (1986). **"Computational limitations for small depth circuits".** PhD thesis. Massachusetts Institute of Technology.

Bibliography ii

- 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.
- Idziak, Paweł M., Piotr Kawałek, Jacek Krzaczkowski, and Armin Weiß (2022). **"Satisfiability Problems for Finite Groups".** In: *49th International Colloquium on Automata, Languages, and Programming (ICALP 2022)*. Vol. 229. LIPIcs. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 127:1–127:20. ISBN: 978-3-95977-235-8. DOI: 10.4230/LIPIcs.ICALP.2022.127.
- Kawałek, Piotr and Armin Weiß (2025). **"Violating Constant Degree Hypothesis Requires Breaking Symmetry".** In: *42nd International Symposium on Theoretical Aspects of Computer Science (STACS 2025)*. Vol. 327. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 58:1–58:21. ISBN: 978-3-95977-365-2. DOI: 10.4230/LIPIcs.STACS.2025.58.

Tardos, Gábor and David A. Mix Barrington (1998). **"A Lower Bound on the Mod 6 Degree of the Or Function".** In: *Comput. Complex.* 7.2, pp. 99–108. DOI: 10.1007/PL00001597. URL: https://doi.org/10.1007/PL00001597.