Conditional Complexity Hardness: Monotone Circuit Size, Matrix Rigidity, and Tensor Rank

Nikolai Chukhin[†,‡], Alexander S. Kulikov[†], Ivan Mihajlin[†], Arina Smirnova[‡]

11.03.2026

[†] JetBrains Research
[‡] Neapolis University Pafos

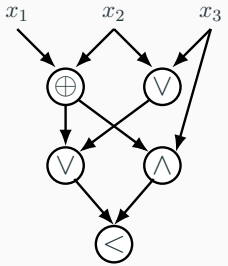
Motivation

Dream (I)
Show that there exists an *interesting* function that cannot be computed by any *fast* Turing machine.

Motivation

Dream (I)
Show that there exists an *interesting* function that cannot be computed by any *fast* Turing machine.

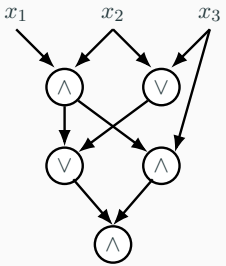
Dream (II)
Show that there exists an *explicit* function that cannot be computed by circuits of *linear size*.



Monotone Functions

Definition
A Boolean function $f\colon \{0,1\}^n \to \{0,1\}$ is *monotone* if $x \leq y$ coordinate-wise implies $f(x) \leq f(y)$.

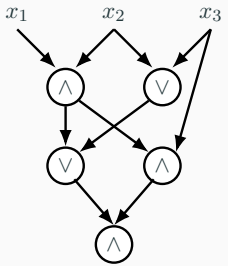
A Boolean circuit is *monotone* if it uses only $\wedge$ and $\vee$ gates.



Monotone Functions

Definition
A Boolean function $f\colon \{0,1\}^n \to \{0,1\}$ is *monotone* if $x \leq y$ coordinate-wise implies $f(x) \leq f(y)$.

A Boolean circuit is *monotone* if it uses only $\wedge$ and $\vee$ gates.

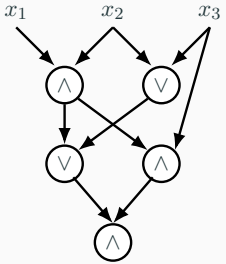


Theorem (Razborov, 1985 [2])
There is an explicit monotone function with monotone circuit size $n^{\Omega(\log n)}$.

Monotone Functions

Definition
A Boolean function $f\colon \{0,1\}^n \to \{0,1\}$ is *monotone* if $x \leq y$ coordinate-wise implies $f(x) \leq f(y)$.

A Boolean circuit is *monotone* if it uses only $\wedge$ and $\vee$ gates.

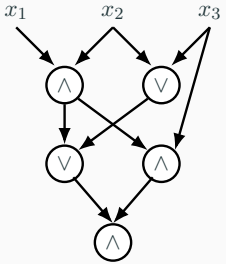


Theorem (Andreev, 1985 [3])
There is an explicit monotone function with monotone circuit size $2^{n^{1/8-o(1)}}$.

Monotone Functions

Definition
A Boolean function $f\colon \{0,1\}^n \to \{0,1\}$ is *monotone* if $x \leq y$ coordinate-wise implies $f(x) \leq f(y)$.

A Boolean circuit is *monotone* if it uses only $\wedge$ and $\vee$ gates.

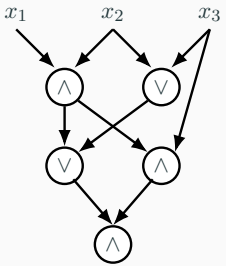


Theorem (Alon, Boppana, [4], Andreev [5], Harnik and Raz, 2000 [6])
There is an explicit monotone function with monotone circuit size $2^{n^{1/3-o(1)}}$.

Monotone Functions

Definition
A Boolean function $f\colon \{0,1\}^n \to \{0,1\}$ is *monotone* if $x \leq y$ coordinate-wise implies $f(x) \leq f(y)$.

A Boolean circuit is *monotone* if it uses only $\wedge$ and $\vee$ gates.



Theorem (Cavalar, Kumar and Rossman, 2022 [1])
There is an explicit monotone function with monotone circuit size $2^{\Omega(\sqrt{n}/\log n)}$.

Connections Between Lower and Upper Bounds

Theorem (Karp–Lipton, 1980 [7])
If $\mathsf{P} = \mathsf{NP}$*, then* EXP *requires circuits of size* $\Omega(2^n/n)$.

Connections Between Lower and Upper Bounds

Theorem (Karp–Lipton, 1980 [7])
If $\mathsf{P} = \mathsf{NP}$*, then* EXP *requires circuits of size* $\Omega(2^n/n)$.

Theorem (Informal, Williams, 2013 [8, 9, 10])
If $\mathsf{Circuit\ SAT}$ *is in time* $O(2^n/n^{10})$*, then* $\mathsf{NEXP} \not\subseteq \mathsf{P/poly}$.

Connections Between Lower and Upper Bounds

Theorem (Karp–Lipton, 1980 [7])
If $\mathsf{P} = \mathsf{NP}$*, then* EXP *requires circuits of size* $\Omega(2^n/n)$.

Theorem (Informal, Williams, 2013 [8, 9, 10])
If $\mathsf{Circuit\ SAT}$ *is in time* $O(2^n/n^{10})$*, then* $\mathsf{NEXP} \not\subseteq \mathsf{P/poly}$.

Theorem (Jahanjou, Miles and Viola, 2018 [11])
If k-SAT *can be solved in co-nondeterministic time* $O(2^{(1-\varepsilon)n})$*, then* E^{NP} *requires series-parallel Boolean circuits of size* $\omega(n)$.

Connections Between Lower and Upper Bounds (II)

Theorem (Williams, 2024 [12])
If k-SAT cannot be solved in time $O(2^{(1-\varepsilon)n})$, then $\underline{\mathsf{ETHR} \circ \mathsf{ETHR}}$ *circuit lower bound.*

Corollary (Williams, 2024 [12])
At least one of the following two circuit lower bounds holds:

1. E^{NP} *requires series-parallel circuits of size* $\omega(n)$*;*
2. *There exists* $\varepsilon > 0$ *such that the Boolean Inner Product on n-bit vectors does not have* $2^{\varepsilon n}$*-size* $\mathrm{ETHR} \circ \mathrm{ETHR}$ *circuits.*

Connections Between Lower and Upper Bounds (II)

Theorem (Williams, 2024 [12])
If k-SAT *cannot be solved in time* $O(2^{(1-\varepsilon)n})$*, then* ETHR $\circ$ ETHR *circuit lower bound.*

Corollary (Williams, 2024 [12])
At least one of the following two circuit lower bounds holds:

1. E^{NP} *requires series-parallel circuits of size* $\omega(n)$*;*
2. *There exists* $\varepsilon > 0$ *such that the Boolean Inner Product on* n*-bit vectors does not have* $2^{\varepsilon n}$*-size* ETHR $\circ$ ETHR *circuits.*

Theorem (Belova et al., 2024 [13])
If MAX-k-SAT *cannot be solved in co-nondeterministic time* $O(2^{(1-\varepsilon)n})$*, then arithmetic circuit lower bounds.*

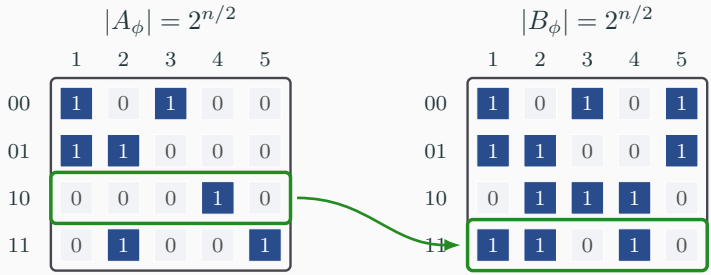
Our Result on Monotone Circuits

Theorem (Cavalar, Kumar and Rossman, 2022 [1])
There is a monotone function $f \in \mathsf{P}$ with monotone circuit size $2^{\Omega(\sqrt{n}/\log n)}$.

Theorem
If, for some $\varepsilon > 0$ and $k \in \mathbb{Z}_{\geq 3}$, k-SAT cannot be solved in co-nondeterministic time $O(2^{(1/2+\varepsilon)n})$, then there exists a monotone Boolean function family in coNP of monotone circuit size $2^{\Omega(n/\log n)}$.

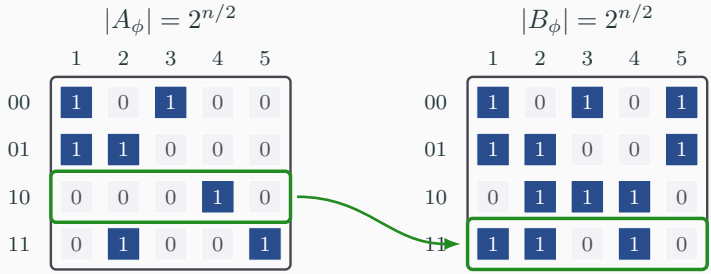
$$\phi(x_1, x_2, x_3, x_4) = (x_1 \vee \overline{x_3} \vee x_4) \wedge (\overline{x_2} \vee x_3 \vee x_4) \wedge (x_1 \vee x_2 \vee \overline{x_4}) \\ \wedge (\overline{x_1} \vee x_2 \vee x_3) \wedge (\overline{x_1} \vee \overline{x_2} \vee \overline{x_3})$$

$$\phi(x_1, x_2, x_3, x_4) = (x_1 \vee \overline{x_3} \vee x_4) \wedge (\overline{x_2} \vee x_3 \vee x_4) \wedge (x_1 \vee x_2 \vee \overline{x_4}) \wedge (\overline{x_1} \vee x_2 \vee x_3) \wedge (\overline{x_1} \vee \overline{x_2} \vee \overline{x_3})$$



$A_\phi(a)[k] = 0$ iff a satisfies C_k on the first half,

$B_\phi(b)[k] = 1$ iff b satisfies C_k on the second half.

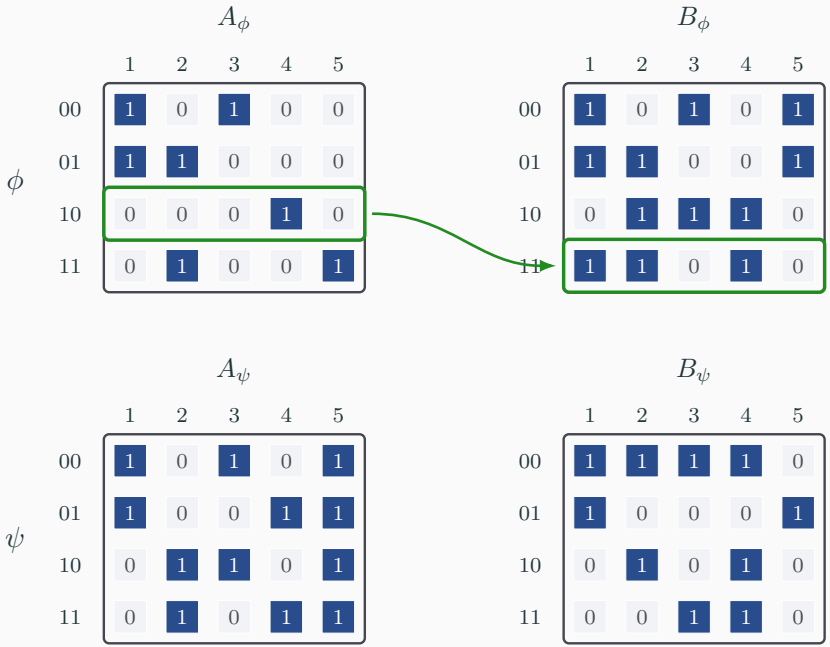


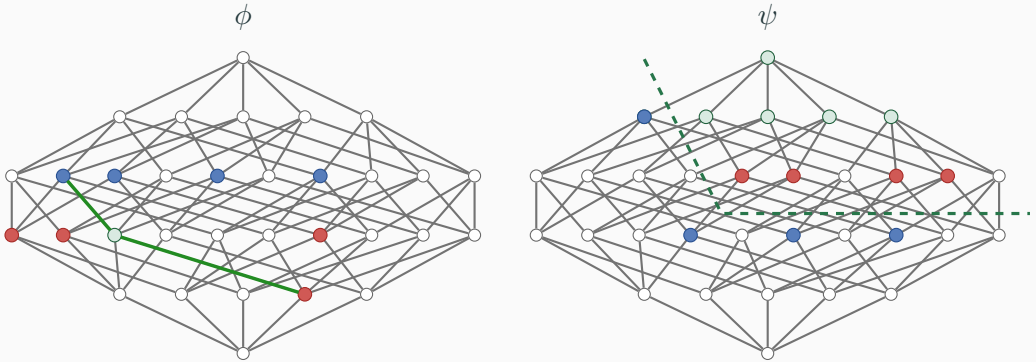
$A_\phi(a)[k] = 0$ iff a satisfies C_k on the first half,

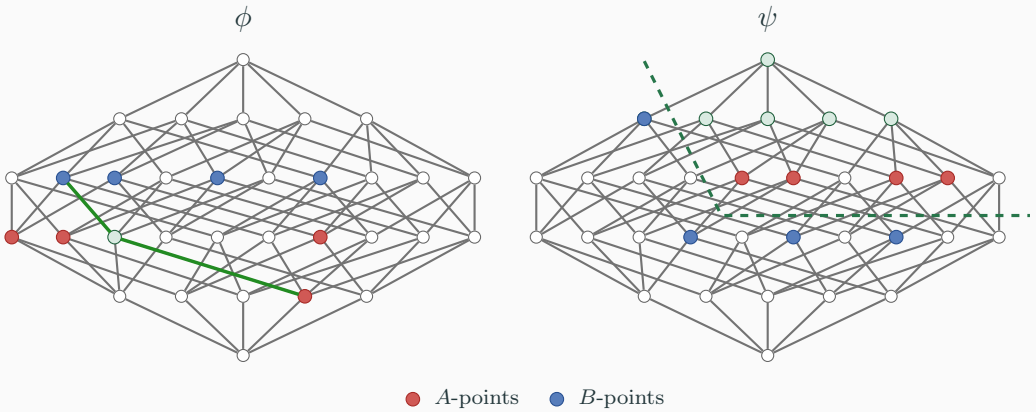
$B_\phi(b)[k] = 1$ iff b satisfies C_k on the second half.

Claim

The formula $\phi \in \mathsf{SAT}$ iff there is a pair $x \in A_\phi, y \in B_\phi \colon x \leq y$.


A_ϕ
B_ϕ
ϕ
A_ψ
B_ψ
ψ
1 2 3 4 5
00 01 10 11


ϕ
ψ
A-points
B-points



Claim

The formula $\phi \in \mathsf{UNSAT}$ iff there exists a monotone $f_\phi : \{0,1\}^{\#\text{clauses}} \to \{0,1\}$ such that $f_\phi(A_\phi) = 1$ and $f_\phi(B_\phi) = 0$.

Outline

Given k-SAT formula ϕ:

- Construct A_ϕ, B_ϕ.
- Guess monotone circuit computing f_ϕ.
- Check that $f_\phi(a) = 1 \; \forall a \in A_\phi$ and $f_\phi(b) = 0 \; \forall b \in B_\phi$.

Outline

Given k-SAT formula ϕ:

- Construct A_ϕ, B_ϕ.
- Guess monotone circuit computing f_ϕ.
- Check that $f_\phi(a) = 1\ \forall a \in A_\phi$ and $f_\phi(b) = 0\ \forall b \in B_\phi$.

Corollary
At least one of the following two circuit lower bounds holds:

1. E^{NP} *requires series-parallel circuits of size* $\omega(n)$*;*
2. *There is an explicit monotone function* $f \in \mathrm{coNP}$ *that requires monotone circuits of size* $2^{\Omega(n/\log n)}$.

Matrix Rigidity and Tensor Rank

Definition
For a matrix $M \in \mathbb{F}^{a \times b}$, we say that it has r-rigidity s if it is necessary to change at least s entries of M to reduce its rank to r. That is, for each decomposition $M = R + S$ such that $\text{rank}(R) \leq r$, it follows that $|S| \geq s$.

Definition
For a tensor $\mathcal{A} \in \mathbb{F}^{n \times n \times n}$, we define its rank, $\text{rank}(\mathcal{A})$, as the smallest integer r such that there exist r tuples of vectors $a_l, b_l, c_l \in \mathbb{F}^n$ for which

$$\mathcal{A} = \sum_{l \in [r]} a_l \otimes b_l \otimes c_l,$$

or equivalently,

$$\mathcal{A}[i, j, k] = \sum_{l \in [r]} a_l[i] b_l[j] c_l[k].$$

Theorem (Shokrollahi, Spielman and Stemann, 1997 [14])
Polynomial-time construction of r-rigidity $n^2/(r\log(n/r))$ matrices for every r.

Theorem (Goldreich and Tal, 2018 [15])
A random $n \times n$ Toeplitz matrix over $\mathbb{F}_2$ has r-rigidity $n^3/(r^2 \log n)$ for $r \geq \sqrt{n}$.

Theorem (Shokrollahi, Spielman and Stemann, 1997 [14])
Polynomial-time construction of r-rigidity $n^2/(r\log(n/r))$ matrices for every r.

Theorem (Goldreich and Tal, 2018 [15])
A random $n \times n$ Toeplitz matrix over $\mathbb{F}_2$ has r-rigidity $n^3/(r^2 \log n)$ for $r \geq \sqrt{n}$.

Theorem
If MAX-3-SAT *cannot be solved in co-nondeterministic time $O(2^{(1-\varepsilon)n})$ for any $\varepsilon > 0$, then for all $\delta > 0$ there exists an efficient generator for matrices of $k^{\frac{1}{2}-\delta}$-rigidity $k^{2-\delta}$.*

Theorem
If MAX-3-SAT *cannot be solved in co-nondeterministic time* $O(2^{(1-\varepsilon)n})$ *for any* $\varepsilon > 0$*, then for all* $\delta > 0$ *there exists an efficient generator for matrices of* $k^{\frac{1}{2}-\delta}$*-rigidity* $k^{2-\delta}$*.*

Theorem
If MAX-3-SAT *cannot be solved in co-nondeterministic time* $O(2^{(1-\varepsilon)n})$ *for any* $\varepsilon > 0$*, then for all* $\delta > 0$ *and some* $\Delta > 0$ *there exists either an efficient generator for:*

- *matrices of* $k^{1-\delta}$*-rigidity* $k^{2-\delta}$*, or*
- 3*-dimensional tensors of rank* $k^{1+\Delta}$*.*

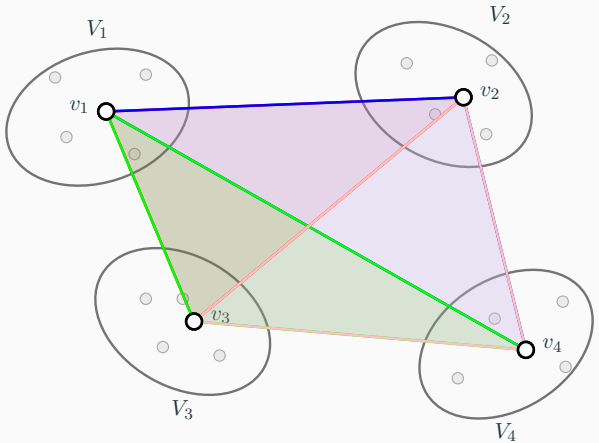
Proof Idea

Given 3-SAT formula ϕ, $t \in \mathbb{N}$, construct a 4-partite 3-uniform hypergraph having a 4-clique iff one can satisfy exactly t clauses in ϕ [16, 17].

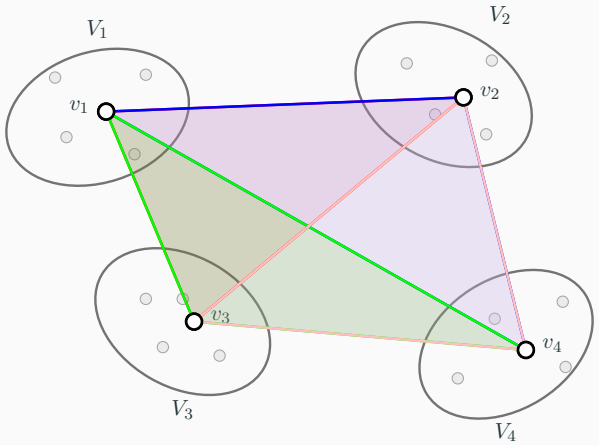
Proof Idea

Given 3-SAT formula ϕ, $t \in \mathbb{N}$, construct a 4-partite 3-uniform hypergraph having a 4-clique iff one can satisfy exactly t clauses in ϕ [16, 17].

$$|V_1| = |V_2| = |V_3| = |V_4| = 2^{n/4}$$



Proof Idea



$$\sum_{v_1,v_2,v_3,v_4 \in \{0,1\}^{n/4}} A_0[v_1, v_2, v_3] \cdot A_1[v_2, v_3, v_4] \cdot A_2[v_3, v_4, v_1] \cdot A_3[v_4, v_1, v_2] > 0.$$

Contributions

We show how to construct hard objects from lower bounds for algorithms:

- Hardness of satisfiability algorithms yields explicit monotone functions with large monotone circuit complexity.
- Hardness of MAX-3-SAT yields explicit matrices with high rigidity, and possibly tensors with high rank.

More broadly: algorithmic lower bounds imply nonuniform lower bounds.

Bibliography i

[1] Bruno Pasqualotto Cavalar, Mrinal Kumar, and Benjamin Rossman. **"Monotone Circuit Lower Bounds from Robust Sunflowers".** In: *Algorithmica* 84.12 (2022), pp. 3655–3685.

[2] Alexander Razborov. **"Lower bounds on the monotone complexity of some Boolean function".** In: *Soviet Math. Dokl.* Vol. 31. 1985, pp. 354–357.

[3] Alexander E. Andreev. **"A method for obtaining lower bounds on the complexity of individual monotone functions".** In: *Doklady Akademii Nauk* 282.5 (1985), pp. 1033–1037.

[4] Noga Alon and Ravi B. Boppana. **"The monotone circuit complexity of Boolean functions".** In: *Comb.* 7.1 (1987), pp. 1–22.

Bibliography ii

[5] Alexander E. Andreev. **"A method for obtaining efficient lower bounds for monotone complexity".** In: *Algebra and Logic* 26.1 (1987), pp. 1–18.

[6] Danny Harnik and Ran Raz. **"Higher lower bounds on monotone size".** In: *STOC*. ACM, 2000, pp. 378–387.

[7] Richard M. Karp and Richard J. Lipton. **"Some Connections between Nonuniform and Uniform Complexity Classes".** In: *STOC*. ACM, 1980, pp. 302–309.

[8] R. Ryan Williams. **"Improving Exhaustive Search Implies Superpolynomial Lower Bounds".** In: *SIAM J. Comput.* 42.3 (2013), pp. 1218–1244.

[9] Ryan Williams. **"Nonuniform ACC circuit lower bounds".** In: *Journal of the ACM (JACM)* 61.1 (2014), pp. 1–32.

[10] Ryan Williams. **"Natural proofs versus derandomization".** In: *Proceedings of the forty-fifth annual ACM symposium on Theory of computing*. 2013, pp. 21–30.

[11] Hamidreza Jahanjou, Eric Miles, and Emanuele Viola. **"Local reduction".** In: *Inf. Comput.* 261 (2018), pp. 281–295.

[12] Ryan Williams. **"The Orthogonal Vectors Conjecture and Non-Uniform Circuit Lower Bounds".** In: *FOCS*. IEEE, 2024, pp. 1372–1387.

Bibliography iv

[13] Tatiana Belova et al. **"Computations with polynomial evaluation oracle: ruling out superlinear SETH-based lower bounds".** In: *SODA*. SIAM, 2024, pp. 1834–1853.

[14] Mohammad Amin Shokrollahi, Daniel A. Spielman, and Volker Stemann. **"A Remark on Matrix Rigidity".** In: *Inf. Process. Lett.* 64.6 (1997), pp. 283–285.

[15] Oded Goldreich and Avishay Tal. **"Matrix rigidity of random Toeplitz matrices".** In: *Comput. Complex.* 27.2 (2018), pp. 305–350.

[16] R. Ryan Williams. **"Algorithms and resource requirements for fundamental problems".** PhD thesis. Carnegie Mellon University, 2007.

[17] Andrea Lincoln, Virginia Vassilevska Williams, and R. Ryan Williams. **"Tight Hardness for Shortest Cycles and Paths in Sparse Graphs".** In: *SODA*. SIAM, 2018, pp. 1236–1252.