Sunflower Theorems in Monotone Circuit Complexity

Student: **Bruno Pasqualotto Cavalar**[1]
Advisor: **Yoshiharu Kohayakawa**[1]

[1]Instituto de Matemática e Estatística – Universidade de São Paulo (USP)
São Paulo – SP – Brazil

Bruno.Pasqualotto-Cavalar@warwick.ac.uk, yoshi@ime.usp.br

Abstract. *Monotone Boolean circuits form one of the largest natural circuit classes for which we are able to prove exponential size lower bounds. Such lower bounds play a pivotal role in complexity theory, being a proxy for lower bounds on communication complexity, proof complexity and optimisation. For over 20 years, the best known lower bound on the size of monotone circuits computing an explicit n-bit monotone function was $\exp(n^{1/3-o(1)})$. In this work, we present the first lower bound on monotone circuit size of order $\exp(n^{1/2-o(1)})$. The proof employs the approximation method of Razborov and recent robust sunflower bounds. We also give the first tight bound of $n^{\Theta(k)}$ on the monotone complexity of the clique problem when k is large.*

1. Introduction

1.1. Complexity theory

One of the most fundamental contributions of theoretical computer science is the notion of an *algorithm*. Many of the most innovative creations of our age came about by the discovery of an efficient algorithm for an interesting computational problem. Yet, even though algorithms have been heavily studied for decades, their limitations are not well understood.

The limitations of algorithms under various computational models are studied in *Computational Complexity Theory* [Arora and Barak 2009]. Progress in this area is inextricably connected to many real-world applications, such as cryptography, where the security of transactions rely on the hardness of computational problems. Complexity theory is also strongly connected to many fields of mathematics, a connection we explored in this thesis.

1.2. Circuit complexity

One of the most ubiquitous computational models studied in complexity theory is the *Boolean circuit*. In a Boolean circuit, each computation step corresponds to a logical Boolean operation (**AND**, **OR** and **NOT**). We call such step a *gate*, and the number of gates in a circuit is called the *size* of the circuit. The final gate of the circuit contains the result of the computation, which is interpreted as the computation of a *Boolean function* $f : \{0,1\}^n \to \{0,1\}$, which maps n-bit Boolean strings to either 0 or 1.

In Circuit Complexity Theory (see [Jukna 2012]), we are interested in the minimum number of gates necessary to compute a given Boolean function. Since any algorithm can be implemented in a Boolean circuit with little loss of efficiency

(see [Arora and Barak 2009, Chapter 6]), lower bounds for the size of circuits solving a given problem imply the *nonexistence* of efficient algorithms for that problem.

The study of circuit complexity has many applications. Because of the connection between the nonexistence of efficient algorithms and circuit lower bounds, the study of circuits give an approach to the well-known problem of separating **P** and **NP**, which is arguably one of the most important problems in theoretical computer science. The complexity of circuits has also been studied in the context of cryptography, distributed computing, learning theory and quantum computation (See [Kushilevitz et al. 1996, Karchmer and Wigderson 1988, Oliveira and Santhanam 2017, Arunachalam et al. 2020] for a representative list).

Proving lower bounds for the size of circuits is thus the main goal of circuit complexity theory. However, this has also proved to be a very hard problem. So far, the best existing lower bound on the size of general Boolean circuits computing an explicit Boolean function f on n bits is $5n$ [Jukna 2012, Section 1.5.2]. For this reason, much of the research in circuit complexity focuses in restricted classes of circuits, where we have been more succesful in proving lower bounds.

1.3. Monotone circuits

A widely studied circuit class is that of *monotone circuits*, which forbid negations in the computation (i.e., **NOT** gates are not allowed). Monotone circuits are one of the largest natural circuit classes for which we have been able to prove strong lower bounds. Besides being a natural computational model, monotone circuits play a pivotal role in computational complexity, being a proxy for lower bounds in communication complexity, proof complexity and optimisation [Raz and Wigderson 1992, Krajíček 1997, Göös et al. 2018].

Monotone circuits compute *monotone Boolean functions*. A Boolean function $f : \{0,1\}^n \to \{0,1\}$ is said to be *monotone* if, for all $x, y \in \{0,1\}^n$ such that $x \leqslant y$, we have $f(x) \leqslant f(y)$.[1] One of the best known monotone Boolean functions is $\mathsf{Clique}(n,k) : \{0,1\}^{\binom{n}{2}} \to \{0,1\}$, which outputs 1 if and only if a given graph G (encoded by its adjacency matrix) contains a clique of size k. This function is known to be in **NP**, which means that any superpolynomial lower bound on the size of general circuits computing it implies that $\mathbf{P} \neq \mathbf{NP}$.

1.4. Lower bounds for monotone circuits

The first *superpolynomial* lower bound[2] on the size of monotone circuits computing an n-bit Boolean function was given by [Razborov 1985]. He showed that any monotone circuit computing $\mathsf{Clique}(n,k)$ must have size $n^{\Omega(k)}$ when $k \leqslant \log n$. To achieve this, he developed a technique now called *approximation method*, making use of the *sunflower lemma* of Erdős and Rado [Erdős and Rado 1960].

Soon after, [Alon and Boppana 1987] extended Razborov's result by proving an $n^{\Omega(\sqrt{k})}$ lower bound for $\mathsf{Clique}(n,k)$ for all $k \leq n^{2/3-o(1)}$. Taking $k = n^{2/3-o(1)}$, this lower bound is $2^{\Omega(n^{1/3-o(1)})}$. Another paper [Andreev 1987] from the same time period

[1] We write $x \leqslant y$ whenever $x_i \leqslant y_i$ for all $i \in [n]$.

[2] I.e., a lower bound of the form n^{ω}, where $\omega = \omega(n) \to \infty$ as $n \to \infty$.

proved an $2^{\Omega(n^{1/3}/\log n)}$ lower bound for an explicit n-variate monotone function. Using a different technique, [Harnik and Raz 2000] proved a lower bound of $2^{\Omega((n/\log n)^{1/3})}$ for a family of n-variate functions in **NP**.

1.5. Our results

Prior to our work, state-of-the-art monotone circuit lower bounds had been stuck at $2^{\Omega(n^{1/3-o(1)})}$ since 1987. Joint work of the student and his coauthors [Cavalar et al. 2020] proved the first $2^{\Omega(n^{1/2-o(1)})}$ lower bound for an n-bit function in **NP**, which breaks a record of over 30 years. We are also able to prove an $n^{\Theta(k)}$ bound for the $\mathsf{Clique}(n,k)$ function when $k \leqslant n^{1/3-o(1)}$, thus proving the first tight bound on the monotone complexity of the clique problem for large k. This improves the result of [Alon and Boppana 1987] for $k \leqslant n^{1/3-o(1)}$.

1.6. Distinction

This work was accepted for presentation at the LATIN 2020[3] conference, an international conference of theoretical computer science. LATIN 2020 was the 14th edition of this conference series, which began in 1992. These 30 years of history give it a traditional place among theoretical computer science conferences. The work of the student and his coauthors was distinguished in this prestigious conference with the *Alejandro López-Ortiz Best Paper Award*. The work was also invited to the special issue of the journal *Algorithmica* dedicated to the LATIN 2020 conference.

1.7. The thesis

In the master thesis, entitled *Sunflowers Theorems in Monotone Circuit Complexity*, the student gives a self-contained exposition of his work on [Cavalar et al. 2020], discussing the main combinatorial structure behind those results. The thesis emphasizes the role of these structures in monotone circuit lower bounds, showing how better bounds for these structures directly imply better monotone circuit lower bounds. Moreover, the thesis also introduces a novel concept of *abstract sunflowers*, which is then used to generalize all the known applications of the *approximation method* of Razborov, one of the main existing techniques used to obtain monotone circuit lower bounds.

1.8. Other remarks

This thesis was advised by *Yoshiharu Kohayakawa* at *Instituto de Matemática e Estatística da Universidade de São Paulo (USP)*. Part of these results were obtained during a visit of the student to the University of Toronto, in collaboration with Benjamin Rossman and Mrinal Kumar. The thesis was defended in September 2020. The thesis is now available at the digital library of USP[4].

2. Sunflowers and the approximation method

Razborov's approach [Razborov 1985] inaugurated a technique which became known as the *approximation method.* Given a monotone circuit C of "small size", it consists in constructing gate-by-gate, in a bottom-up fashion, another circuit $\widetilde{C}$ that approximates C on

[3] `https://latin2020.ime.usp.br/`

[4] See `https://doi.org/10.11606/D.45.2020.tde-25112020-162107`.

a set of inputs of interest. One then exploits the structure of this approximating circuit to prove that it differs from $\mathsf{Clique}(n,k)$ under the same distribution, thus implying that no "small" circuit C can compute this function. For monotone circuit lower bounds, showing that $\widetilde{C}$ does indeed approximate C is usually the hardest part, involving the use of a combinatorial lemma – which, in the case of [Razborov 1985], was the *sunflower lemma* of Erdős and Rado [Erdős and Rado 1960]. This technique was leveraged to obtain lower bounds for a host of other monotone problems by [Alon and Boppana 1987]. They employ a weaker notion of "sunflowers" (which we call here *lopsided sunflowers*), proving a better corresponding bound.

Another type of sunflowers, called *robust sunflowers*, was developed by Rossman [Rossman 2014] with the purpose of achieving better lower bounds for $\mathsf{Clique}(n,k)$ on random graphs. Robust sunflowers found applications not only in monotone circuit complexity, but also in DNF sparsification [Gopalan et al. 2013] randomness extractors [Li et al. 2018], and lifting theorems [Lovett et al. 2020]. A recent breakthrough of [Alweiss et al. 2020] significantly improved the upper bound on the size of uniform families without robust sunflowers. Subsequent works [Rao 2020, Tao 2020] improved their bound to a final, tight bound.

In our work [Cavalar et al. 2020], we show how these recent developments in sunflower theorems lead to better monotone circuit lower bounds. We apply the approximation method with *robust sunflowers* to prove the following theorem:

Theorem 1. There exists a monotone Boolean function $f : \{0,1\}^n \to \{0,1\}$ in **NP** such that any monotone circuit computing f has size at least $2^{\Omega(n^{1/2}/\log n)}$.

By applying the same technique with a variant of robust sunflowers that we call *clique-sunflowers*, we are able to prove an $n^{\Theta(k)}$ lower bound for the $\mathsf{Clique}(n,k)$ function when $k \leqslant n^{1/3-o(1)}$.

Theorem 2. For any fixed $0 < \delta < 1/3$ and all $k \leqslant n^{1/3-\delta}$, the monotone circuit complexity of $\mathsf{Clique}(n,k)$ is $\Omega(n^{\delta^2 k/2})$.

In the thesis, we give a generalized presentation of this and other results, by framing all known applications of the approximation method as making use of a notion we call *abstract sunflowers*. Attention to this generalized notion may lead to even better lower bounds in the future, as we also discuss with more detail in the thesis.

3. Better lower bounds for a function in NP

To the best of our knowledge, the following table summarizes the progress of the strongest monotone circuit lower bounds so far.

Reference	Technique	Result
[Bloniarz 1980]	Gate elimination	$4n$
[Tiekenheinrich 1984]	Gate elimination	$4n$
[Razborov 1985]	Approximation method w/ sunflowers	$n^{\Omega(\log n)}$
[Andreev 1985]	Approximation method w/ lopsided sunflowers	$2^{\tilde{\Omega}(n^{1/8})}$
[Alon and Boppana 1987]	Approximation method w/ lopsided sunflowers	$2^{\tilde{\Omega}(n^{1/4})}$
[Andreev 1987]	Approximation method w/ lopsided sunflowers	$2^{\tilde{\Omega}(n^{1/3})}$
[Harnik and Raz 2000]	Monotone switching lemma	$2^{\tilde{\Omega}(n^{1/3})}$

Reference	Technique	Result
[Cavalar et al. 2020]	Approximation method w/ robust sunflowers	$2^{\tilde{\Omega}(n^{1/2})}$

The lower bound of [Harnik and Raz 2000] holds for a family of explicit n-variate functions defined using a small probability space of random variables with bounded independence. Our lower bound of $2^{\tilde{\Omega}(n^{1/2})}$ holds for the same function considered by [Harnik and Raz 2000].

4. Better lower bounds for clique

The following table summarizes the history of lower bounds on the monotone complexity of $\mathsf{Clique}(n, k)$.

Reference	Range of k	Technique	Result
[Razborov 1985]	$\leqslant \log n$	Appr. method w/ sunflowers	$n^{\Omega(k)}$
[Alon and Boppana 1987]	$\leqslant n^{2/3}/4$	Appr. method w/ lop. sunflowers	$n^{\Omega(\sqrt{k})}$
[Cavalar et al. 2020]	$\leqslant n^{1/3-\delta}$	Appr. method w/ clq. sunflowers	$n^{\Omega(\delta^2 k)}$

We remark that a recent work of [Krajíček and Oliveira 2018] showed that any lower bound for $\mathsf{Clique}(n, k)$ better than $n^{\Omega(\sqrt{k})}$ for large k must avoid the approximation method altogether or consider a different set of distributions. We achieve our lower bound by considering the Erdős-Rényi p-biased random graph, together with our notion of *clique-sunflowers*.

References

Alon, N. and Boppana, R. B. (1987). The monotone circuit complexity of Boolean functions. *Combinatorica*, 7(1):1–22.

Alweiss, R., Lovett, S., Wu, K., and Zhang, J. (2020). Improved bounds for the sunflower lemma. In *Proceedings of STOC*, pages 624–630, New York, NY, USA.

Andreev, A. (1987). A method for obtaining efficient lower bounds for monotone complexity. *Algebra and Logic*, 26(1):1–18.

Andreev, A. E. (1985). A method for obtaining lower bounds on the complexity of individual monotone functions. *Dokl. Akad. Nauk SSSR*, 282(5):1033–1037.

Arora, S. and Barak, B. (2009). *Computational complexity*. Cambridge University Press, Cambridge. A modern approach.

Arunachalam, S., Grilo, A. B., Gur, T., Oliveira, I. C., and Sundaram, A. (2020). Quantum learning algorithms imply circuit lower bounds. *arXiv:2012.01920 [quant-ph]*.

Bloniarz, P. A. (1980). The complexity of monotone boolean functions and an algorithm for finding shortest paths on a graph. Technical report, USA. Ph.D. Thesis.

Cavalar, B. P., Kumar, M., and Rossman, B. (2020). Monotone Circuit Lower Bounds from Robust Sunflowers. In *LATIN 2020: Theoretical Informatics*, pages 311–322, Cham. Springer.

Erdős, P. and Rado, R. (1960). Intersection theorems for systems of sets. *J. London Math. Soc.*, 35:85–90.

Gopalan, P., Meka, R., and Reingold, O. (2013). DNF sparsification and a faster deterministic counting algorithm. *Computational Complexity*, 22(2):275–310.

Göös, M., Jain, R., and Watson, T. (2018). Extension Complexity of Independent Set Polytopes. *SIAM Journal on Computing*, 47(1):241–269.

Harnik, D. and Raz, R. (2000). Higher lower bounds on monotone size. In *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*, pages 378–387. ACM, New York.

Jukna, S. (2012). *Boolean function complexity*, volume 27 of *Algorithms and Combinatorics*. Springer, Heidelberg. Advances and frontiers.

Karchmer, M. and Wigderson, A. (1988). Monotone Circuits for Connectivity Require Super-logarithmic Depth. In *Proceedings of STOC*, pages 539–550, New York, NY, USA. ACM.

Krajíček, J. and Oliveira, I. C. (2018). On monotone circuits with local oracles and clique lower bounds. *Chic. J. Theoret. Comput. Sci.*, pages Art. 1, 18.

Krajíček, J. (1997). Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic. *The Journal of Symbolic Logic*, 62(2):457–486.

Kushilevitz, E., Ostrovsky, R., and Rosén, A. (1996). Characterizing linear size circuits in terms of privacy. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing*, STOC '96, pages 541–550, New York, NY, USA.

Li, X., Lovett, S., and Zhang, J. (2018). Sunflowers and quasi-sunflowers from randomness extractors. In *APPROX-RANDOM*, volume 116 of *LIPIcs*, pages 51:1–13.

Lovett, S., Meka, R., Mertz, I., Pitassi, T., and Zhang, J. (2020). Lifting with Sunflowers. Technical Report 111.

Oliveira, I. C. and Santhanam, R. (2017). Conspiracies between learning algorithms, circuit lower bounds, and pseudorandomness. In *Proceedings of the 32nd Computational Complexity Conference*, CCC '17, pages 1–49, Dagstuhl, DEU.

Rao, A. (2020). Coding for sunflowers. *Discrete Anal.*, pages Paper No. 2, 8.

Raz, R. and Wigderson, A. (1992). Monotone circuits for matching require linear depth. *Journal of the ACM*, 39(3):736–744.

Razborov, A. A. (1985). Lower bounds on the monotone complexity of some Boolean functions. *Dokl. Akad. Nauk SSSR*, 281(4):798–801.

Rossman, B. (2014). The monotone complexity of k-clique on random graphs. *SIAM J. Comput.*, 43(1):256–279.

Tao, T. (2020). The sunflower lemma via shannon entropy. *Blogpost*.

Tiekenheinrich, J. (1984). A $4n$-lower bound on the mononotone network complexity of a oneoutput boolean function. *Information Processing Letters*, 18:201–201.