

A (Biased) Survey of Space Complexity and Time-Space Trade-offs in Proof Complexity

Jakob Nordström

School of Computer Science and Communication
KTH Royal Institute of Technology
SE-100 44 Stockholm, Sweden

Abstract. This presentation is intended as a survey of results on proof space and time-space trade-offs in proof complexity. We will try to provide some proof sketches to give a flavour of the proof methods used, but also explain the limitations of current techniques and state some tantalising problems that remain open.

The field of proof complexity was founded by Cook and Reckhow [14] with the goal of ultimately separating P and NP (by obtaining the stronger separation of $\text{NP} \neq \text{coNP}$). It is thus natural that the main complexity measure of interest in proof complexity has been, and is, that of *proof size*. However, proof complexity also has natural connections to applied SAT solving, since most current SAT solvers are (explicitly or implicitly) based on proof systems that are well-studied in proof complexity. The most significant example of this is arguably provided by current state-of-the-art SAT solvers using *conflict-driven clause learning (CDCL)* [3, 22, 23], which effectively can be seen to search for proofs in the resolution proof system [10].

Proof size is of paramount importance in the context of SAT solving as well, since it can be seen to yield lower bounds on running time, but another resource which is absolutely crucial for SAT solvers is memory consumption. For this reason, it was asked in the late 1990s whether memory usage could be modelled in proof complexity, so that a mathematical study of this measure could yield interesting insights. This indeed turned out to be the case, and research in this area has revealed intriguing connections between different complexity measures that are also of intrinsic interest to proof complexity.

This presentation will attempt to give a survey of some of the results in this area of research, and the purpose of these notes is to collect the references on which the presentation is based. Readers interested in more details can also refer to, for instance, the survey [26].

1 The Resolution Proof System

Esteban and Torán [17] were the first to present what turned out to be a very useful and natural measure of *proof space* for resolution, measured as the maximal

number of clauses needed in memory during verification of a proof. This (clause) space measure was soon generalized to other proof systems by Alekhovich et al. [1]. It is not hard to show that the space complexity of a formula is at most linear measured in the number of variables (and hence also measured in terms of formula size). Optimal (up to constant factors) linear lower bounds on resolution space were established in [1, 17] and by Ben-Sasson and Galesi [7] for several well-studied families of CNF formulas. Atserias and Dalmau [2] later proved that all of these results could in fact be derived as immediate consequences of lower bounds on *proof width* (measured as the size of a largest clause in a resolution proof). The sequence of papers [24, 27, 8] showed that while sufficient, width lower bounds are not a necessary condition for space lower bound. This was established by exhibiting formulas with small width complexity but large space complexity.

Combining [2] and [8] one can deduce that formulas with low space complexity must also have short proofs, but that the converse is false in the strongest sense possible. A natural question related to this is whether proof size and proof space can be optimized simultaneously or whether there are trade-offs between the two measures. The first results in this direction were presented in [6, 25], although they only applied in limited settings. In the papers [4, 5, 9] it was finally shown that there are very strong trade-offs in the sense that there are formulas which have both short proofs and space-efficient proofs, but where minimizing one of the measures must by necessity cause a dramatic blow-up in the other.

Most of the above papers focus on the clause space measure defined in [17]. Another natural measure is the *total space* of a proof as introduced in [1], counting not just clauses but the total number of literals in these clauses. In a very recent paper, Bonacina et al. [12] established optimal quadratic lower bounds for this space measure.

2 Stronger Proof Systems

The clause space and total space measures as defined in [1, 17] can be generalized to stronger proof systems in a natural way. Unfortunately, as these proof systems grow stronger the analogues of clause space soon become uninteresting, and even for total space one can only get trivial bounds for strong enough systems as shown in [1]. However, for proof systems slightly stronger than resolution the study of these measures still make perfect sense. We discuss two such proof systems below.

One way of strengthening resolution is by adding algebraic reasoning to form the proof system *polynomial calculus* as defined in [1, 13].¹ In polynomial calculus, the disjunctive clauses of the input CNF formula are interpreted as multilinear polynomials (expanded out to sums of monomials), and one derives contradiction by showing that these polynomials have no common root. *Proof size*

¹ In these notes we will be somewhat sloppy and not distinguish between polynomial calculus (PC) [13] and the slightly more general proof system polynomial calculus resolution (PCR) [1], using the term “polynomial calculus” to refer to both.

in polynomial calculus is measured as the total number of monomials in a proof and the analogue of (clause) space in resolution is *(monomial) space*, measured as the number of monomials needed simultaneously in memory during proof verification.

The first lower bounds on space in polynomial calculus were reported in [1], but only sublinear bounds and only for formulas of unbounded width. For CNF formulas of constant width the first space lower bounds appeared only in [19]. Asymptotically optimal (linear) lower bounds were finally proven by Bonacina and Galesi [11] with some further extensions in [18]. However, there still remain several formula families with high resolution space complexity for which the space complexity in polynomial calculus remains unknown.

As to the relation between size and space, it is open whether small space complexity implies small size complexity, but [18] showed that small size does not imply small space, just as for resolution. Strong size-space trade-offs have been shown in [5], essentially extending the results for resolution in [4, 9] but with slightly weaker parameters.

In the *cutting planes* proof system [15] clauses of a CNF formula are translated to linear inequalities and the formula is refuted by showing that the polytope defined by these inequalities does not contain any zero-one integer points. Cutting planes is much less well understood than both resolution and polynomial calculus, and even for proof size there is essentially only one superpolynomial lower bound proven by Pudlák [28] using so called *monotone interpolation*.

It is natural to define the *line space* of a cutting planes proof to be the maximal number of linear inequalities that need to be kept in memory simultaneously during the proof. Just as for monomial space in polynomial calculus, line space in cutting planes is easily seen to be a generalization of clause space in resolution and is hence upper bounded by the clause space complexity. As far as we are aware, however, no lower bounds are known for cutting planes space.

Perhaps somewhat surprisingly, questions about size-space trade-offs for cutting planes (and stronger proof systems) have turned out to be related to communication complexity, as shown in the recent papers [20, 21]. However, so far all that has been proven using this approach are conditional space lower bounds, i.e., space lower bounds that seem likely to hold unconditionally, but which can so far be established only for cutting planes proofs of polynomial size.

References

1. Alekhovich, M., Ben-Sasson, E., Razborov, A.A., Wigderson, A.: Space complexity in propositional calculus. SIAM Journal on Computing 31(4), 1184–1211 (2002), preliminary version appeared in *STOC '00*
2. Atserias, A., Dalmau, V.: A combinatorial characterization of resolution width. Journal of Computer and System Sciences 74(3), 323–334 (May 2008), preliminary version appeared in *CCC '03*
3. Bayardo Jr., R.J., Schrag, R.: Using CSP look-back techniques to solve real-world SAT instances. In: Proceedings of the 14th National Conference on Artificial Intelligence (AAAI '97). pp. 203–208 (Jul 1997)

4. Beame, P., Beck, C., Impagliazzo, R.: Time-space tradeoffs in resolution: Super-polynomial lower bounds for superlinear space. In: Proceedings of the 44th Annual ACM Symposium on Theory of Computing (STOC '12). pp. 213–232 (May 2012)
5. Beck, C., Nordström, J., Tang, B.: Some trade-off results for polynomial calculus. In: Proceedings of the 45th Annual ACM Symposium on Theory of Computing (STOC '13). pp. 813–822 (May 2013)
6. Ben-Sasson, E.: Size-space tradeoffs for resolution. *SIAM Journal on Computing* 38(6), 2511–2525 (May 2009), preliminary version appeared in *STOC '02*
7. Ben-Sasson, E., Galesi, N.: Space complexity of random formulae in resolution. *Random Structures and Algorithms* 23(1), 92–109 (Aug 2003), preliminary version appeared in *CCC '01*
8. Ben-Sasson, E., Nordström, J.: Short proofs may be spacious: An optimal separation of space and length in resolution. In: Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science (FOCS '08). pp. 709–718 (Oct 2008)
9. Ben-Sasson, E., Nordström, J.: Understanding space in proof complexity: Separations and trade-offs via substitutions. In: Proceedings of the 2nd Symposium on Innovations in Computer Science (ICS '11). pp. 401–416 (Jan 2011), full-length version available at <http://eccc.hpi-web.de/report/2010/125/>.
10. Blake, A.: Canonical Expressions in Boolean Algebra. Ph.D. thesis, University of Chicago (1937)
11. Bonacina, I., Galesi, N.: Pseudo-partitions, transversality and locality: A combinatorial characterization for the space measure in algebraic proof systems. In: Proceedings of the 4th Conference on Innovations in Theoretical Computer Science (ITCS '13). pp. 455–472 (Jan 2013)
12. Bonacina, I., Galesi, N., Thapen, N.: Total space in resolution. Technical Report TR14-038, Electronic Colloquium on Computational Complexity (ECCC) (Mar 2014)
13. Clegg, M., Edmonds, J., Impagliazzo, R.: Using the Groebner basis algorithm to find proofs of unsatisfiability. In: Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC '96). pp. 174–183 (May 1996)
14. Cook, S.A., Reckhow, R.: The relative efficiency of propositional proof systems. *Journal of Symbolic Logic* 44(1), 36–50 (Mar 1979)
15. Cook, W., Coullard, C.R., Turán, G.: On the complexity of cutting-plane proofs. *Discrete Applied Mathematics* 18(1), 25–38 (Nov 1987)
16. Esteban, J.L., Torán, J.: Space bounds for resolution. In: Proceedings of the 16th International Symposium on Theoretical Aspects of Computer Science (STACS '99). *Lecture Notes in Computer Science*, vol. 1563, pp. 551–560. Springer (1999)
17. Esteban, J.L., Torán, J.: Space bounds for resolution. *Information and Computation* 171(1), 84–97 (2001), based on the conference papers in *STACS '99* [16] and *CSL '99* [29]
18. Filmus, Y., Lauria, M., Mikša, M., Nordström, J., Vinyals, M.: Towards an understanding of polynomial calculus: New separations and lower bounds (extended abstract). In: Proceedings of the 40th International Colloquium on Automata, Languages and Programming (ICALP '13). *Lecture Notes in Computer Science*, vol. 7965, pp. 437–448. Springer (Jul 2013)
19. Filmus, Y., Lauria, M., Nordström, J., Thapen, N., Ron-Zewi, N.: Space complexity in polynomial calculus (extended abstract). In: Proceedings of the 27th Annual IEEE Conference on Computational Complexity (CCC '12). pp. 334–344 (Jun 2012)

20. Göös, M., Pitassi, T.: Communication lower bounds via critical block sensitivity. In: Proceedings of the 46th Annual ACM Symposium on Theory of Computing (STOC '14) (May 2014), to appear
21. Huynh, T., Nordström, J.: On the virtue of succinct proofs: Amplifying communication complexity hardness to time-space trade-offs in proof complexity (extended abstract). In: Proceedings of the 44th Annual ACM Symposium on Theory of Computing (STOC '12). pp. 233–248 (May 2012)
22. Marques-Silva, J.P., Sakallah, K.A.: GRASP: A search algorithm for propositional satisfiability. *IEEE Transactions on Computers* 48(5), 506–521 (May 1999), preliminary version appeared in *ICCAD '96*
23. Moskewicz, M.W., Madigan, C.F., Zhao, Y., Zhang, L., Malik, S.: Chaff: Engineering an efficient SAT solver. In: Proceedings of the 38th Design Automation Conference (DAC '01). pp. 530–535 (Jun 2001)
24. Nordström, J.: Narrow proofs may be spacious: Separating space and width in resolution. *SIAM Journal on Computing* 39(1), 59–121 (May 2009), preliminary version appeared in *STOC '06*
25. Nordström, J.: A simplified way of proving trade-off results for resolution. *Information Processing Letters* 109(18), 1030–1035 (Aug 2009), preliminary version appeared in ECCC report TR07-114, 2007
26. Nordström, J.: Pebble games, proof complexity and time-space trade-offs. *Logical Methods in Computer Science* 9, 15:1–15:63 (Sep 2013)
27. Nordström, J., Håstad, J.: Towards an optimal separation of space and length in resolution. *Theory of Computing* 9, 471–557 (May 2013), preliminary version appeared in *STOC '08*
28. Pudlák, P.: Lower bounds for resolution and cutting plane proofs and monotone computations. *Journal of Symbolic Logic* 62(3), 981–998 (Sep 1997)
29. Torán, J.: Lower bounds for space in resolution. In: Proceedings of the 13th International Workshop on Computer Science Logic (CSL '99). *Lecture Notes in Computer Science*, vol. 1683, pp. 362–373. Springer (1999)