A (Biased) Proof Complexity Survey for SAT Practitioners

Jakob Nordström

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

Abstract. This talk is intended as a selective survey of proof complexity, focusing on some comparatively weak proof systems that are of particular interest in connection with SAT solving. We will review resolution, polynomial calculus, and cutting planes (related to conflict-driven clause learning, Gröbner basis computations, and pseudo-Boolean solvers, respectively) and some proof complexity measures that have been studied for these proof systems. We will also briefly discuss if and how these proof complexity measures could provide insights into SAT solver performance.

Proof complexity studies how hard it is to find succinct certificates for the unsatisfiability of formulas in conjunctive normal form (CNF), i.e., proofs that formulas always evaluate to false under any truth value assignment, where these proofs should be efficiently verifiable. It is generally believed that there cannot exist a proof system where such proofs can always be chosen of size at most polynomial in the formula size. If this belief could be proven correct, it would follow that $\mathsf{NP} \neq \mathsf{coNP}$, and hence $\mathsf{P} \neq \mathsf{NP}$, and this was the original reason research in proof complexity was initiated by Cook and Reckhow [18]. However, the goal of separating P and NP in this way remains very distant.

Another, perhaps more recent, motivation for proof complexity is the connection to applied SAT solving. Any algorithm for deciding SAT defines a proof system in the sense that the execution trace on an unsatisfiable instance is itself a polynomial-time verifiable witness (often referred to as a *refutation* rather than a *proof*). In the other direction, most SAT solvers in effect search for proofs in systems studied in proof complexity, and upper and lower bounds for these proof systems hence give information about the potential and limitations of such SAT solvers.

In addition to running time, an important concern in SAT solving is memory consumption. In proof complexity, time and memory are modelled by *proof size* and *proof space*. It therefore seems interesting to understand these two complexity measures and how they are related to each other, and such a study reveals intriguing connections that are also of intrinsic interest to proof complexity. In this context, it is natural to concentrate on comparatively weak proof systems that are, or could plausibly be, used as a basis for SAT solvers. This talk will focus on such proof systems, and the purpose of these notes is to summarize the main points. Readers interested in more details can refer to, e.g, the survey [31].

1 Resolution

The proof system *resolution* [13] lies at the foundation of state-of-the-art SAT solvers based on conflict-driven clause learning (CDCL) [5, 28, 30]. In resolution, one derives new clauses from the clauses of the original CNF formula until an explicit contradiction is reached. Haken [24] proved the first (sub)exponential lower bound on proof size (measured as the number of clauses in a proof), and truly exponential lower bounds—i.e., bounds $\exp(\Omega(n))$ in the size n of the formula—were later established in [16, 33].

The study of space in resolution was initiated by Esteban and Torán [20], measuring the space of a proof (informally) as the maximum number of clauses needing to be kept in memory during proof verification. Alekhnovich et al. [1] later extended the concept of space to a more general setting, including other proof systems. The (clause) space measure can be shown to be at most linear in the formula size, and matching lower bounds were proven in [1, 8, 20].

Ben-Sasson and Wigderson [11] instead focused on *width*, measured as the size of largest clause in a proof. It is easy to show that upper bounds on width imply upper bounds on size. More interestingly, [11] established the converse that strong enough lower bounds on width imply strong lower bounds on size, and used this to rederive essentially all known size lower bounds in terms of width. The relation between size and width was elucidated further in [4, 15].

Atserias and Dalmau [3] proved that width also yields lower bounds on space[1] and that all previous space lower bounds could be obtained in this way. This demonstrates that width plays a key role in understanding both size and space. It should be noted, however, that in contrast to the relation between width and size the connection between width and space does not go in both directions, and an essentially optimal separation of the two measures was obtained in [9].

Regarding the connections between size and space, it follows from [3] that formulas of low space complexity also have short proofs. For the subsystem of *tree-like resolution*, where each line in the proof can only be used once, [20] showed that size upper bounds also imply space upper bounds, but for general resolution [9] established that this is false in the strongest possible sense. There have also been strong size-space trade-offs proven in [6, 7, 10].

The most comprehensive study to date of the question if and how hardness with respect to these complexity measures for resolution is correlated with actual hardness as measured by CDCL running time would seem to be [27], but it seems fair to say that the results so far are somewhat inconclusive.

2 Polynomial Calculus

Resolution can be extended with algebraic reasoning to form the stronger proof system *polynomial calculus (PC)* as defined in [1, 17],[2] which corresponds to

[1] Note that this relation is nontrivial since space is measured as the number of *clauses*.

[2] We will be slightly sloppy in these notes and will not distinguish between polynomial calculus (PC) [17] and the slightly more general proof system polynomial calculus

Gröbner basis computations. In a PC proof, clauses are interpreted as multilinear polynomials (expanded out to sums of monomials), and one derives contradiction by showing that these polynomials have no common root. Intriguingly, while proof complexity-theoretic results seem to hold out the promise that SAT solvers based on polynomial calculus could be orders of magnitude faster than CDCL, such algebraic solvers have so far failed to be truly competitive (except for limited "hybrid versions" that incorporate reasoning in terms of linear equations into CDCL solvers).

Proof size in polynomial calculus is measured as the total number of monomials in a proof and the analogue of resolution space is the number of monomials needed simultaneously in memory during proof verification. Clause width in resolution translates into polynomial degree in PC. While size, space and width in resolution are fairly well understood, our understanding of the corresponding complexity measures in PC is more limited.

Impagliazzo et al. [26] showed that strong degree lower bounds imply strong size lower bounds. This is a parallel to the size-width relation for resolution in [11] discussed above, and in fact [11] can be seen as a translation of the bound in [26] from PC to resolution. This size-degree relation has been used to prove exponential lower bounds on size in a number of papers, with [2] perhaps providing the most general setting.

The first lower bounds on space were reported in [1], but only sublinear bounds and only for formulas of unbounded width. The first space lower bounds for k-CNF formulas were presented in [22], and asymptotically optimal (linear) lower bounds were finally proven by Bonacina and Galesi [14]. However, there are several formula families with high resolution space complexity for which the PC space complexity still remains unknown.

Regarding the relation between space and degree, it is open whether degree is a lower bound for space (which would be the analogue of what holds in resolution), but some limited results in this direction were proven in [21]. The same paper also established that the two measures can be separated in the sense that there are formulas of minimal (i.e., constant) degree complexity requiring maximal (i.e., linear) space.

As to size versus space in PC, it is open whether small space complexity implies small size complexity, but [21] showed that small size does not imply small space, just as for resolution. Strong size-space trade-offs have been shown in [7], essentially extending the results for resolution in [6, 10] but with slightly weaker parameters.

3 Cutting Planes

In the proof system *cutting planes (CP)* [19] clauses of a CNF formula are translated to linear inequalities and the formula is refuted by showing that the

resolution (PCR) [1], using the term "polynomial calculus" to refer to both. PC is the proof system that is actually used in practice, but PCR is often more natural to work with in the context of proof complexity.

polytope defined by these inequalities does not have any zero-one integer points (corresponding to satisfying assignments). As is the case for polynomial calculus, cutting planes is exponentially stronger than resolution viewed as a proof system, but we are not aware of any efficient implementations of cutting planes-based SAT solvers that are truly competitive with CDCL solvers on CNF inputs in general (although as shown in [12, 29] there are fairly natural formulas for which one can observe exponential gains in performance also in practice).

Cutting planes is much less well understood than both resolution and polynomial calculus. For proof size there is only one superpolynomial lower bound proven by Pudlák [32], but this result relies on a very specific technique that works only for formulas with a very particular structure. It remains a major challenge in proof complexity to prove lower bounds for other formulas such as random k-CNF formulas or so-called Tseitin formulas.

It is natural to define the *line space* of a CP 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 CP space. Also, it should perhaps be noted that there does not seem to exist any generalization of width/degree for cutting planes with interesting connections to size or space.

Given the state of knowledge regarding proof size and space, maybe it is not too surprising that we also do not know much about size-space trade-offs. The recent papers [23, 25] developed new techniques for this problem by making a connection between size-space trade-offs and communication complexity, and used this connection to show results that could be interpreted as circumstantial evidence that similar trade-off results as for resolution could be expected to hold also for cutting planes. However, so far all that has been proven using the approach in [23, 25] 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. Alekhnovich, 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. Alekhnovich, M., Razborov, A.A.: Lower bounds for polynomial calculus: Non-binomial case. Proceedings of the Steklov Institute of Mathematics 242, 18–35 (2003), available at `http://people.cs.uchicago.edu/~razborov/files/misha.pdf`. Preliminary version appeared in *FOCS '01*.
3. 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*
4. Atserias, A., Lauria, M., Nordström, J.: Narrow proofs may be maximally long. In: Proceedings of the 29th Annual IEEE Conference on Computational Complexity (CCC '14) (Jun 2014), to appear

5. 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)
6. Beame, P., Beck, C., Impagliazzo, R.: Time-space tradeoffs in resolution: Superpolynomial lower bounds for superlinear space. In: Proceedings of the 44th Annual ACM Symposium on Theory of Computing (STOC '12). pp. 213–232 (May 2012)
7. 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)
8. 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*
9. 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)
10. 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/`.
11. Ben-Sasson, E., Wigderson, A.: Short proofs are narrow—resolution made simple. Journal of the ACM 48(2), 149–169 (Mar 2001), preliminary version appeared in *STOC '99*
12. Biere, A., Berre, D.L., Lonca, E., Manthey, N.: Detecting cardinality constraints in CNF. In: Proceedings of the 17th International Conference on Theory and Applications of Satisfiability Testing (SAT '14) (Jul 2014), to appear
13. Blake, A.: Canonical Expressions in Boolean Algebra. Ph.D. thesis, University of Chicago (1937)
14. 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)
15. Bonet, M.L., Galesi, N.: Optimality of size-width tradeoffs for resolution. Computational Complexity 10(4), 261–276 (Dec 2001), preliminary version appeared in *FOCS '99*
16. Chvátal, V., Szemerédi, E.: Many hard examples for resolution. Journal of the ACM 35(4), 759–768 (Oct 1988)
17. 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)
18. Cook, S.A., Reckhow, R.: The relative efficiency of propositional proof systems. Journal of Symbolic Logic 44(1), 36–50 (Mar 1979)
19. Cook, W., Coullard, C.R., Turán, G.: On the complexity of cutting-plane proofs. Discrete Applied Mathematics 18(1), 25–38 (Nov 1987)
20. Esteban, J.L., Torán, J.: Space bounds for resolution. Information and Computation 171(1), 84–97 (2001), preliminary versions of these results appeared in *STACS '99* and *CSL '99*
21. 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)

22. 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)
23. 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
24. Haken, A.: The intractability of resolution. Theoretical Computer Science 39(2-3), 297–308 (Aug 1985)
25. 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)
26. Impagliazzo, R., Pudlák, P., Sgall, J.: Lower bounds for the polynomial calculus and the Gröbner basis algorithm. Computational Complexity 8(2), 127–144 (1999)
27. Järvisalo, M., Matsliah, A., Nordström, J., Živný, S.: Relating proof complexity measures and practical hardness of SAT. In: Proceedings of the 18th International Conference on Principles and Practice of Constraint Programming (CP '12). Lecture Notes in Computer Science, vol. 7514, pp. 316–331. Springer (Oct 2012)
28. Marques-Silva, J.P., Sakallah, K.A.: GRASP—a new search algorithm for satisfiability. In: Proceedings of the IEEE/ACM International Conference on Computer-Aided Design (ICCAD '96). pp. 220–227 (Nov 1996)
29. Mikša, M., Nordström, J.: Long proofs of (seemingly) simple formulas. In: Proceedings of the 17th International Conference on Theory and Applications of Satisfiability Testing (SAT '14) (Jul 2014), to appear
30. 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)
31. Nordström, J.: Pebble games, proof complexity and time-space trade-offs. Logical Methods in Computer Science 9, 15:1–15:63 (Sep 2013)
32. Pudlák, P.: Lower bounds for resolution and cutting plane proofs and monotone computations. Journal of Symbolic Logic 62(3), 981–998 (Sep 1997)
33. Urquhart, A.: Hard examples for resolution. Journal of the ACM 34(1), 209–219 (Jan 1987)