Report from Dagstuhl Seminar 18051

Proof Complexity

Edited by

Albert Atserias[1], Jakob Nordström[2], Pavel Pudlák[3], and Rahul Santhanam[4]

1 **UPC – Barcelona, ES,** atserias@cs.upc.edu
2 **KTH Royal Institute of Technology – Stockholm, SE,** jakobn@kth.se
3 **The Czech Academy of Sciences – Prague, CZ,** pudlak@math.cas.cz
4 **University of Oxford, GB,** rahul.santhanam@cs.ox.ac.uk

Abstract

The study of proof complexity was initiated in [Cook and Reckhow 1979] as a way to attack the P vs. NP problem, and in the ensuing decades many powerful techniques have been discovered for analyzing different proof systems. Proof complexity also gives a way of studying subsystems of Peano Arithmetic where the power of mathematical reasoning is restricted, and to quantify how complex different mathematical theorems are measured in terms of the strength of the methods of reasoning required to establish their validity. Moreover, it allows to analyse the power and limitations of satisfiability algorithms (SAT solvers) used in industrial applications with formulas containing up to millions of variables.

During the last 10–15 years the area of proof complexity has seen a revival with many exciting results, and new connections have also been revealed with other areas such as, e.g., cryptography, algebraic complexity theory, communication complexity, and combinatorial optimization. While many longstanding open problems from the 1980s and 1990s still remain unsolved, recent progress gives hope that the area may be ripe for decisive breakthroughs. This workshop, gathering researchers from different strands of the proof complexity community, gave opportunities to take stock of where we stand and discuss the way ahead.

Seminar January 28–February 2, 2018 – https://www.dagstuhl.de/18051
2012 ACM Subject Classification Theory of computation → Proof complexity
Keywords and phrases bounded arithmetic, computational complexity, logic, proof complexity, satisfiability algorithms
Digital Object Identifier 10.4230/DagRep.8.1.124
Edited in cooperation with Marc Vinyals

1 Executive Summary

Albert Atserias
Jakob Nordström
Pavel Pudlák
Rahul Santhanam

This workshop brought together the whole proof complexity community spanning from Frege proof systems and circuit-inspired lower bounds via geometric and algebraic proof systems all the way to bounded arithmetic. In this executive summary, we first give an overview of proof complexity, and then describe the goals of the seminar week. Finally, we discuss the relation to previous workshops and conferences.

Topic of the Seminar

Ever since the groundbreaking NP-completeness paper of Cook [18], the problem of deciding whether a given propositional logic formula is satisfiable or not has been on centre stage in theoretical computer science. During the last two decades, SATISFIABILITY has also developed from a problem of mainly theoretical interest into a practical approach for solving applied problems. Although all known Boolean satisfiability solvers (SAT solvers) have exponential running time in the worst case, enormous progress in performance has led to satisfiability algorithms becoming a standard tool for solving large-scale problems in, for example, hardware and software verification, artificial intelligence, bioinformatics, operations research, and sometimes even pure mathematics.

The study of proof complexity originated with the seminal paper of Cook and Reckhow [19]. In its most general form, a proof system for a formal language L is a predicate $P(x, \pi)$, computable in time polynomial in the sizes $|x|$ and $|\pi|$ of the input, and having the property that for all $x \in L$ there exists a string π (a *proof*) for which $P(x, \pi)$ evaluates to true, whereas for any$x \notin L$ it should hold for all strings π that $P(x, \pi)$ evaluates to false. A proof system is said to be polynomially bounded if for every $x \in L$ there exists a proof π_x for x that has size at most polynomial in $|x|$. A *propositional proof system* is a proof system for the language of tautologies in propositional logic, i.e., for formulas that always evaluate to true no matter how the values true and false are assigned to variables in the formula.

From a theoretical point of view, one important motivation for proof complexity is the intimate connection with the fundamental problem of P versus NP. Since NP is exactly the set of languages with polynomially bounded proof systems, and since TAUTOLOGY can be seen to be the dual problem of SATISFIABILITY, we have the famous theorem of [19] that NP = coNP if and only if there exists a polynomially bounded propositional proof system. Thus, if it could be shown that there are no polynomially bounded proof systems for tautologies, P $\neq$ NP would follow as a corollary since P is closed under complement. One way of approaching this problem is to study stronger and stronger proof systems and try to prove superpolynomial lower bounds on proof size. However, although great progress has been made in the last couple of decades for a variety of proof systems, this goal still appears very distant.

A second theoretical motivation is that simple propositional proof systems provide analogues of subsystems of Peano Arithmetic where the power of mathematical reasoning is restricted. Of particular interest here are various bounded arithmetic systems, which in some sense are intended to capture feasible/polynomial-time reasoning. Proving strong lower bounds on propositional logic encodings of some combinatorial principle, say, in a propositional proof system can in this way show that establishing the validity of this principle requires more powerful mathematics than what is provided by the corresponding subsystem of Peano Arithmetic. One can thus quantify how "deep" different mathematical truths are, as well as shed light on the limits of our (human, rather than automated) proof techniques. At the same time, since it is an empirically verified fact that low-complexity proofs generalize better and are often more constructive, classifying which truths have feasible proofs is also a way to approach the classification of algorithmic problems by their computational complexity. The precise sense in which this can be formalized into a tool for the complexity theorist is one of the goals of bounded arithmetic.

A third prominent motivation for the study of proof complexity is also algorithmic but of a more practical nature. As was mentioned above, designing efficient algorithms for proving tautologies–or, equivalently, testing satisfiability–is a very important problem not only in the theory of computation but also in applied research and industry. All SAT solvers, regardless

of whether they produce a written proof or not, explicitly or implicitly define a system in which proofs are searched for and rules which determine what proofs in this system look like. Proof complexity analyses what it takes to simply write down and verify the proofs that such a solver might find, ignoring the computational effort needed to actually find them. Thus, a lower bound for a proof system tells us that any algorithm, even an optimal (non-deterministic) one magically making all the right choices, must necessarily use at least the amount of a certain resource specified by this bound. In the other direction, theoretical upper bounds on some proof complexity measure give us hope of finding good proof search algorithms with respect to this measure, provided that we can design algorithms that search for proofs in the system in an efficient manner.

The field of proof complexity also has rich connections to algorithmic analysis, combinatorial optimization, cryptography, artificial intelligence, and mathematical logic. A few good sourcesproviding more details are [6, 17, 47].

A Very Selective Survey of Proof Complexity

Any propositional logic formula can be converted to a formula in conjunctive normal form (CNF) that is only linearly larger and is unsatisfiable if and only if the original formula is a tautology. Therefore, any sound and complete system that certifies the unsatisfiability of CNF formulas can be considered as a general propositional proof system.

The extensively studied *resolution* proof system, which appeared in [9] and began to be investigated in connection with automated theorem proving in the 1960s [21, 22, 48], is such a system where one derives new disjunctive clauses from an unsatisfiable CNF formula until an explicit contradiction is reached. Despite the apparent simplicity of resolution, the first superpolynomial lower bounds on proof size were obtained only after decades of study in 1985 [33], after which truly exponential size lower bounds soon followed in [15, 52]. It was shown in [8] that these lower bounds can be established by instead studying the *width* of proofs, i.e., the maximal size of clauses in the proofs, and arguing that any resolution proof for a certain formula must contain a large clause. It then follows by a generic argument that any such proof must also consist of very many clauses. Later research has led to a well-developed machinery for showing width lower bounds, and hence also size lower bounds, for resolution.

The more general proof system *polynomial calculus (PC)*, introduced in [1, 16],[1] instead uses algebraic geometry to reason about SAT. In polynomial calculus clauses are translated to multilinear polynomials over some (fixed) field, and a CNF formula F is shown to be unsatisfiable by proving that there is no common root for the polynomials corresponding to all the clauses, or equivalently that the multiplicative identity 1 lies in the ideal generated by these polynomials. Here the size of a proof is measured as the number of monomials in a proof when all polynomials are expanded out as linear combinations of monomials, and the width of a clause corresponds to the (total) *degree* of the polynomial representing the clause. It can be shown that PC is at least as strong as resolution with respect to both size and width/degree, and there are families of formulas for which PC is exponentially stronger.

In the work [36], which served, interestingly enough, as a precursor to [8], it was shown that strong lower bounds on the degree of polynomial calculus proofs are sufficient to establish strong size lower bounds. In contrast to the situation for resolution after [8], however, this

[1] Expert readers will note that we do not distinguish between PC [16] and PCR [1] below due to space constraints.

has not been followed by a corresponding development of a generally applicable machinery for proving degree lower bounds. For fields of characteristic distinct from 2 it is sometimes possible to obtain lower bounds by doing an affine transformation from $\{0,1\}$ to the "Fourier basis" $\{-1,+1\}$, an idea that seems to have appeared first in [13, 28]. For fields of arbitrary characteristic a powerful technique for general systems of polynomial equations was developed in [2], which when restricted to CNF formulas F yields that polynomial calculus proofs require high degree if the corresponding clause-variable incidence graphs $G(F)$ are good enough bipartite expander graphs. There are several provably hard formula families for which this criterion fails to apply, however, and even more formulas that are believed to be hard for both resolution and PC, but where lower bounds are only known for the former proof system and not the latter.

Another proof system that has been the focus of much research is *cutting planes (CP)*, which was introduced in [20] as a way of formalizing the integer linear programming algorithm in [14, 27]. Here the disjunctive clauses in a CNF formula are translated to linear inequalities, and these linear inequalities are then manipulated to derive a contradiction. Thus, questions about the satifiability of Boolean formulas are reduced to the geometry of polytopes over the real numbers. Cutting planes is easily seen to be as least as strong as resolution, since a CP proof can mimic any resolution proof line by line. An intriguing fact is that encodings of the *pigeonhole principle*, which are known to be hard to prove for resolution [33] and many other proof systems, are very easy to prove in cutting planes. It follows from this that not only is cutting planes never worse than resolution, but it can be exponentially stronger.

Exponential lower bounds on proof length for cutting planes were first proven in [10] for the restricted subsystem CP*, where all coefficients in the linear inequalities can be at most polynomial in the formula size, and were later extended to general CP in [34, 44]. The proof technique in [44] is very specific, however, in that it works by *interpolating* monotone Boolean circuits for certain problems from CP proofs of related formulas with a very particular structure, and then appealing to lower bounds in circuit complexity. A longstanding open problem is to develop techniques that would apply to other formula families. For example, establishing that randomly sampled k-CNF formulas are hard to refute for CP, or that CP cannot efficiently prove the fact that the sum of all vertex degrees in an undirected graph is even (encoded in so-called *Tseitin formulas*), would constitute major breakthroughs.

We remark that there are also other proof systems inspired by linear and semidefinite programming, e.g., in [38, 39, 50], which are somewhat similar to but incomparable with cutting planes, and a deeper understanding of which appear even more challenging. Some notable early papers in proof complexity investigating these so-called *semialgebraic proof systems* were published around the turn of the millennium in [30, 31, 45], but then this area of research seems to have gone dormant. In the last few years, these proof systems have made an exciting reemergence in the context of hardness of approximation, revealing unexpected and intriguing connections between approximation and proof complexity. A precursor to this is the work by Schoenebeck [49], which gave strong integrality gaps in the so-called Lasserre SDP hierarchy using results from proof complexity. These results were later realized to be a rediscovery of results by Grigoriev [29] proving degree lower bounds for what he called the *Positivstellensatz Calculus* [31]. More recently we have the work of Barak et al. [4], which was the first to explicitly point out this intriguing connection between approximability and proof complexity. Following this paper, several papers have appeared that continue the fruitful exploration of the interplay between approximability and proof complexity. Results from this area also appeared in the invited talk of Boaz Barak at the International Congress of Mathematicians in 2014 (see [5]).

The paper [19] initiated research in proof complexity focused on a more general and powerful family of propositional proof systems called *Frege systems*. Such systems consist of a finite implicationally complete set of axioms and inference rules (let us say over connectives AND, OR, and NOT for concreteness), where new formulas are derived by substitution into the axioms and inference rules. Various forms of Frege systems (also called *Hilbert systems*) typically appear in logic textbooks, and typically the exact definitions vary. Such distinctions do not matter for our purposes, however—it was shown in [19] that all such systems are equivalent up to an at most polynomial blow-up in the proof size.

Frege systems are well beyond what we can prove nontrivial lower bounds for; the situation is similar to the problem of proving lower bound on the size of Boolean circuits. Therefore restricted versions of Frege systems have been studied. One natural restriction is to allow unbounded fan-in AND-OR formulas (where negations appear only in front of atomic variables) but to require that all formulas appearing in a proof have bounded depth (i.e., a bounded number of alternations between AND and OR). Such a model is an analogue of the bounded-depth circuits studied in circuit complexity, but first arose in the context of bounded first-order arithmetic in logic [12, 41]. For such *bounded-depth Frege systems* exponential lower bounds on proof size were obtained in [37, 42], but these lower bounds only work for depth smaller than $\log \log n$. This depth lower bound was very recently improved to $\sqrt{\log n}$ in [43], but in terms of the size lower bound this recent result is much weaker. By comparison, for the corresponding class in circuit complexity strong size lower bounds are known all the way up to depth $\log n / \log \log n$. Also, if one extends the set of connectives with exclusive or (also called parity) to obtain *bounded-depth Frege with parity gates*, then again no lower bounds are known, although strong lower bounds have been shown for the analogous class in circuit complexity [46, 51].

The quest for lower bounds for bounded-depth Frege systems and beyond are mainly motivated by the P vs. NP problem. Regarding connections to SAT solving, it is mostly weaker proof systems such as resolution, polynomial calculus, and cutting planes that are of interest, whereas the variants of Frege systems discussed above do not seem to be suitable foundations for SAT solvers. The issue here is that not only do we want our proof system to be as powerful as possible, i.e., having short proofs for the formulas under consideration, but we also want to be able to *find these proofs efficiently.*

We quantify this theoretically by saying that a proof system is *automatizable* if there is an algorithm that finds proofs in this system in time polynomial in the length of an optimal proof. This seems to be the right notion: If there is no short proof of a formula in the system, then we cannot expect any algorithm to find a proof quickly, but if there is a short proof to be found we want an algorithm that is competitive with respect to the length of such a proof. Unfortunately, there seems to be a trade-off here in the sense that if a proof system is sufficiently powerful, then it is not automatizable. For instance, bounded-depth Frege systems are not automatizable under plausible computational complexity assumptions [11]. However, analogous results have later been shown also for resolution [3], and yet proof search is implemented successfully in this proof system in practice. This raises intriguing questions that seem to merit further study.

Goals of the Seminar

There is a rich selection of open problems that could be discussed at a workshop focused on proof complexity. Below we just give a few samples of such problems that came up during

the workshop–it should be emphasized that this list is very far from exhaustive and is only intended to serve as an illustration.

For starters, there are a number of NP-complete problems for which we would like to understand the hardness with respect to polynomial calculus and other algebraic proof systems. For the problem of cliques of constant size k in graphs, there is an obvious polynomial-time algorithm (since only $\binom{n}{k} \leq n^k$ possible candidate cliques need to be checked). Whether this brute-force algorithm is optimal or not is a deep question with connections to fixed-parameter tractability and parameterized proof complexity. This is completely open for polynomial calculus, and even for resolution. The ultimate goal here would be to prove average-case lower bounds for k-clique formulas over Erdős–Rényi random graphs $G(n, p)$ with edge probability just below the threshold $p = n^{-2/(k-1)}$ for the appearance of k-cliques.

In contrast to the clique problem, graph colouring is NP-complete already for a constant number 3 of colours. If we believe that $\mathsf{P} \neq \mathsf{NP}$, then, in particular, it seems reasonable to expect that this problem should be hard for polynomial calculus. No such results have been known, however. On the contrary, in the papers [23, 24, 25] recognized with the *INFORMS Computing Society Prize 2010*, the authors report that they used algebraic methods formalizable in polynomial calculus that "successfully solved graph problem instances having thousands of nodes and tens of thousands of edges" and that they could not find hard instances for these algorithms. This is very surprising. For resolution, it was shown in [7] that random graphs with the right edge density are exponentially hard to deal with, and it seems likely that the same should hold also for polynomial calculus. This appears to be a very challenging problem, however, but we hope that techniques from [2, 40] can be brought to bear on it.

For cutting planes, a longstanding open problem is to prove lower bounds for random k-CNF formulas or Tseitin formulas over expander graphs. An interesting direction in the last few years has been the development of new techniques for size-space trade-offs, showing that if short cutting planes proofs do exist, such proofs must at least have high space complexity in that they require a lot of memory to be verified. Such results were first obtained via a somewhat unexpected connection to communication complexity in [35], and have more recently been strengthened in [26, 32].

Admittedly, proving lower bounds for bounded-depth Frege systems and beyond is another formidable challenge, and it only seems prudent to say that this is a high-risk proposal. However, the very recent, and exciting, progress in [43] give hope that new techniques might be developed to attack also this problem.

Relation to Previous Dagstuhl Seminars

The area of proof complexity has a large intersection with computational complexity theory, and are two recurring workshops at Dagstuhl dedicated to complexity theory broadly construed, namely *Computational Complexity of Discrete Problems* and *Algebraic Methods in Computational Complexity*. However, these two workshops have had very limited coverage of topics related to proof complexity in the past.

On the more applied side, there have been two workshops *SAT and Interactions* and *Theory and Practice of SAT Solving* that have explored the connections between computational complexity and more applied satisfiability algorithms as used in industry (so-called SAT solvers). These workshops have focused on very weak proof systems, however, which are the ones that are of interest in connection to SAT solving, but have not made any connections to stronger proof systems or to bounded arithmetic.

Although proof complexity has turned out to have deep connections to both complexity theory and SAT solving, proof complexity is an interesting and vibrant enough area to merit a seminar week in its own right. This workshop at Dagstuhl provided a unique opportunity for the community to meet during a full week focusing on the latest news in various subareas and major challenges going forward.

References

1. Michael Alekhnovich, Eli Ben-Sasson, Alexander A. Razborov, and Avi Wigderson. Space complexity in propositional calculus. *SIAM Journal on Computing*, 31(4):1184–1211, 2002. Preliminary version in *STOC '00*.
2. Michael Alekhnovich and Alexander A. Razborov. 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 in *FOCS '01*.
3. Michael Alekhnovich and Alexander A. Razborov. Resolution is not automatizable unless W[P] is tractable. *SIAM Journal on Computing*, 38(4):1347–1363, October 2008. Preliminary version in *FOCS '01*.
4. Boaz Barak, Fernando G. S. L. Brandão, Aram Wettroth Harrow, Jonathan A. Kelner, David Steurer, and Yuan Zhou. Hypercontractivity, sum-of-squares proofs, and their applications. In *Proceedings of the 44th Annual ACM Symposium on Theory of Computing (STOC '12)*, pages 307–326, May 2012.
5. Boaz Barak and David Steurer. Sum-of-squares proofs and the quest toward optimal algorithms. In *Proceedings of International Congress of Mathematicians (ICM)*, 2014.
6. Paul Beame. Proof complexity. In Steven Rudich and Avi Wigderson, editors, *Computational Complexity Theory*, volume 10 of *IAS/Park City Mathematics Series*, pages 199–246. American Mathematical Society, 2004.
7. Paul Beame, Joseph C. Culberson, David G. Mitchell, and Cristopher Moore. The resolution complexity of random graph k-colorability. *Discrete Applied Mathematics*, 153(1-3):25–47, December 2005.
8. Eli Ben-Sasson and Avi Wigderson. Short proofs are narrow—resolution made simple. *Journal of the ACM*, 48(2):149–169, March 2001. Preliminary version in *STOC '99*.
9. Archie Blake. *Canonical Expressions in Boolean Algebra*. PhD thesis, University of Chicago, 1937.
10. María Bonet, Toniann Pitassi, and Ran Raz. Lower bounds for cutting planes proofs with small coefficients. In *Proceedings of the 27th Annual ACM Symposium on Theory of Computing (STOC '95)*, pages 575–584, May 1995.
11. María Luisa Bonet, Carlos Domingo, Ricard Gavaldà, Alexis Maciel, and Toniann Pitassi. Non-automatizability of bounded-depth Frege proofs. In *Proceedings of the 14th Annual IEEE Conference on Computational Complexity (CCC '99)*, pages 15–23, May 1999.
12. Samuel R. Buss. *Bounded Arithmetic*. Bibliopolis, Naples, 1986. Revision of PhD thesis.
13. Samuel R. Buss, Dima Grigoriev, Russell Impagliazzo, and Toniann Pitassi. Linear gaps between degrees for the polynomial calculus modulo distinct primes. *Journal of Computer and System Sciences*, 62(2):267–289, March 2001. Preliminary version in *CCC '99*.
14. Vašek Chvátal. Edmonds polytopes and a hierarchy of combinatorial problems. *Discrete Mathematics*, 4(1):305–337, 1973.
15. Vašek Chvátal and Endre Szemerédi. Many hard examples for resolution. *Journal of the ACM*, 35(4):759–768, October 1988.
16. Matthew Clegg, Jeffery Edmonds, and Russell Impagliazzo. Using the Groebner basis algorithm to find proofs of unsatisfiability. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC '96)*, pages 174–183, May 1996.

17 Peter Clote and Evangelos Kranakis. *Boolean Functions and Computation Models*. Springer, 2002.

18 Stephen A. Cook. The complexity of theorem-proving procedures. In *Proceedings of the 3rd Annual ACM Symposium on Theory of Computing (STOC '71)*, pages 151–158, 1971.

19 Stephen A. Cook and Robert Reckhow. The relative efficiency of propositional proof systems. *Journal of Symbolic Logic*, 44(1):36–50, March 1979.

20 William Cook, Collette Rene Coullard, and György Turán. On the complexity of cutting-plane proofs. *Discrete Applied Mathematics*, 18(1):25–38, November 1987.

21 Martin Davis, George Logemann, and Donald Loveland. A machine program for theorem proving. *Communications of the ACM*, 5(7):394–397, July 1962.

22 Martin Davis and Hilary Putnam. A computing procedure for quantification theory. *Journal of the ACM*, 7(3):201–215, 1960.

23 Jesús A. De Loera, Jon Lee, Peter N. Malkin, and Susan Margulies. Hilbert's Nullstellensatz and an algorithm for proving combinatorial infeasibility. In *Proceedings of the 21st International Symposium on Symbolic and Algebraic Computation (ISSAC '08)*, pages 197–206, July 2008.

24 Jesús A. De Loera, Jon Lee, Peter N. Malkin, and Susan Margulies. Computing infeasibility certificates for combinatorial problems through Hilbert's Nullstellensatz. *Journal of Symbolic Computation*, 46(11):1260–1283, November 2011.

25 Jesús A. De Loera, Jon Lee, Susan Margulies, and Shmuel Onn. Expressing combinatorial problems by systems of polynomial equations and Hilbert's Nullstellensatz. *Combinatorics, Probability and Computing*, 18(04):551–582, July 2009.

26 Susanna F. de Rezende, Jakob Nordström, and Marc Vinyals. How limited interaction hinders real communication (and what it means for proof and circuit complexity). In *Proceedings of the 57th Annual IEEE Symposium on Foundations of Computer Science (FOCS '16)*, pages 295–304, October 2016.

27 Ralph E. Gomory. An algorithm for integer solutions of linear programs. In R.L. Graves and P. Wolfe, editors, *Recent Advances in Mathematical Programming*, pages 269–302. McGraw-Hill, New York, 1963.

28 Dima Grigoriev. Tseitin's tautologies and lower bounds for Nullstellensatz proofs. In *Proceedings of the 39th Annual IEEE Symposium on Foundations of Computer Science (FOCS '98)*, pages 648–652, November 1998.

29 Dima Grigoriev. Linear lower bound on degrees of Positivstellensatz calculus proofs for the parity. *Theoretical Computer Science*, 259(1–2):613–622, May 2001.

30 Dima Grigoriev, Edward A. Hirsch, and Dmitrii V. Pasechnik. Complexity of semialgebraic proofs. *Moscow Mathematical Journal*, 2(4):647–679, 2002. Preliminary version in *STACS '02*.

31 Dima Grigoriev and Nicolai Vorobjov. Complexity of Null- and Positivstellensatz proofs. *Annals of Pure and Applied Logic*, 113(1–3):153–160, December 2001.

32 Mika Göös and Toniann Pitassi. Communication lower bounds via critical block sensitivity. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing (STOC '14)*, pages 847–856, May 2014.

33 Armin Haken. The intractability of resolution. *Theoretical Computer Science*, 39(2-3):297–308, August 1985.

34 Armin Haken and Stephen A. Cook. An exponential lower bound for the size of monotone real circuits. *Journal of Computer and System Sciences*, 58(2):326–335, 1999.

35 Trinh Huynh and Jakob Nordström. 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)*, pages 233–248, May 2012.

36 Russell Impagliazzo, Pavel Pudlák, and Jiří Sgall. Lower bounds for the polynomial calculus and the Gröbner basis algorithm. *Computational Complexity*, 8(2):127–144, 1999.

37 Jan Krajíček, Pavel Pudlák, and Alan R. Woods. An exponential lower bound to the size of bounded depth Frege proofs of the pigeonhole principle. *Random Structures and Algorithms*, 7(1):15–40, 1995. Preliminary version in *STOC '92*.

38 Jean B. Lasserre. An explicit exact SDP relaxation for nonlinear 0-1 programs. In *Proceedings of the 8th International Conference on Integer Programming and Combinatorial Optimization (IPCO '01)*, volume 2081 of *Lecture Notes in Computer Science*, pages 293–303. Springer, June 2001.

39 László Lovász and Alexander Schrijver. Cones of matrices and set-functions and 0-1 optimization. *SIAM Journal on Optimization*, 1(2):166–190, 1991.

40 Mladen Mikša and Jakob Nordström. A generalized method for proving polynomial calculus degree lower bounds. In *Proceedings of the 30th Annual Computational Complexity Conference (CCC '15)*, volume 33 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 467–487, June 2015.

41 Jeff B. Paris and Alex J. Wilkie. Counting problems in bounded arithmetic. In *Methods in Mathematical Logic: Proceedings of the 6th Latin American Symposium on Mathematical Logic*, volume 1130 of *Lecture Notes in Mathematics*, pages 317–340. Springer, 1985.

42 Toniann Pitassi, Paul Beame, and Russell Impagliazzo. Exponential lower bounds for the pigeonhole principle. *Computational Complexity*, 3:97–140, 1993. Preliminary version in *STOC '92*.

43 Toniann Pitassi, Benjamin Rossman, Rocco Servedio, and Li-Yang Tan. Poly-logarithmic Frege depth lower bounds. In *Proceedings of the 48th Annual ACM Symposium on Theory of Computing (STOC '16)*, pages 644–657, June 2016.

44 Pavel Pudlák. Lower bounds for resolution and cutting plane proofs and monotone computations. *Journal of Symbolic Logic*, 62(3):981–998, September 1997.

45 Pavel Pudlák. On the complexity of propositional calculus. In S. Barry Cooper and John K. Truss, editors, *Sets and Proofs*, volume 258 of *London Mathematical Society Lecture Note Series*, pages 197–218. Cambridge University Press, 1999.

46 Alexander A. Razborov. Lower bounds on the size of bounded depth networks over a complete basis with logical addition. *Matematicheskie Zametki*, 41(4):598–607, 1987. English Translation in *Mathematical Notes of the Academy of Sciences of the USSR*, 41(4):333–338, 1987.

47 Alexander A. Razborov. Proof complexity and beyond. *ACM SIGACT News*, 47(2):66–86, June 2016.

48 John Alan Robinson. A machine-oriented logic based on the resolution principle. *Journal of the ACM*, 12(1):23–41, January 1965.

49 Grant Schoenebeck. Linear level Lasserre lower bounds for certain k-CSPs. In *Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science (FOCS '08)*, pages 593–602, October 2008.

50 Hanif D. Sherali and Warren P. Adams. A hierarchy of relaxations between the continuous and convex hull representations for zero-one programming problems. *SIAM Journal on Discrete Mathematics*, 3:411–430, 1990.

51 Roman Smolensky. Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In *Proceedings of the 19th Annual ACM Symposium on Theory of Computing (STOC '87)*, pages 77–82, 1987.

52 Alasdair Urquhart. Hard examples for resolution. *Journal of the ACM*, 34(1):209–219, January 1987.

2 Contents

3 Overview of Presentations Given During the Seminar Week

In this section we list the talks given during the seminar week. As can be seen from a comparison with Section 1, a number of presentations could report progress on long-standing open problems.

In addition to the list of "official" presentations below, there were also a number of more informal presentations and discussions on various topics (including, but not limited to, the open problems mentioned in Section 4).

3.1 Some Classic SOS Gems with Proofs

Albert Atserias (UPC – Barcelona, ES)

This will be a blackboard lecture-like talk in which I will define the version of Sums-of-Squares (SOS) proof that I want to discuss, and cover the proofs of two beautiful results about it in (an usual amount of?) detail. The first gem is a surprising new result of Berkholz [1], with an equally surprising simple proof, that shows that SOS simulates Polynomial Calculus over the reals with Boolean-valued variables. The second gem is the beautiful construction of Grigoriev [2], as rediscovered by Schoenebeck [3], for showing that systems of parity equations that are hard for resolution are also hard for SOS.

References

1 Christoph Berkholz: *The Relation between Polynomial Calculus, Sherali-Adams, and Sum-of-Squares Proofs.* STACS 2018: 11:1–11:14
2 Dima Grigoriev: *Tseitin's Tautologies and Lower Bounds for Nullstellensatz Proofs.* FOCS 1998: 648–652
3 Grant Schoenebeck: *Linear Level Lasserre Lower Bounds for Certain k-CSPs.* FOCS 2008: 593–602

3.2 Hard Principles from Bounded Arithmetic

Arnold Beckmann (Swansea University, GB)

This talk is intended as a second tutorial on Bounded Arithmetic following that of Neil Thapen. It will focus on how Bounded Arithmetic is useful for obtaining hard principles for propositional proof systems. We will touch on reflection principles and related techniques, and demonstrate their usefulness with a few examples. The main part of the tutorial will concentrate on total NP search problems and their relation to Bounded Arithmetic. We will review recent characterisations of classes of total NP search problems whose totality can be proven in certain Bounded Arithmetic theories, and demonstrate through examples how complete problems for such classes lead to hard problems for propositional proof systems corresponding to Bounded Arithmetic theories.

3.3 What's Different in QBF from Propositional Proof Complexity?

Olaf Beyersdorff (University of Leeds, GB)

Main reference Olaf Beyersdorff, Joshua Blinkhorn: "Genuine Lower Bounds for QBF Expansion", in Proc. of the 35th Symposium on Theoretical Aspects of Computer Science, STACS 2018, February 28 to March 3, 2018, Caen, France, LIPIcs, Vol. 96, pp. 12:1–12:15, Schloss Dagstuhl – Leibniz-Zentrum fuer Informatik, 2018.
URL http://dx.doi.org/10.4230/LIPIcs.STACS.2018.12

The aim of the talk is to discuss QBF proof complexity in comparison to propositional proof complexity. In particular, I will talk about different ideas for QBF resolution systems, the hard formulas we currently have, what is a genuine QBF lower bound and what techniques we have to show them. As an example of a genuine lower bound I will explain the size-cost-capacity technique [1].

References

1 Olaf Beyersdorff, Joshua Blinkhorn, Luke Hinde: *Size, Cost and Capacity: A Semantic Technique for Hard Random QBFs.* ITCS 2018: 9:1–9:18

3.4 Clique Is Hard on Average for Regular Resolution

Ilario Bonacina (UPC – Barcelona, ES)

Joint work of Albert Atserias, Ilario Bonacina, Susanna de Rezende, Massimo Lauria, Jakob Nordström, Alexander Razborov
Main reference Albert Atserias, Ilario Bonacina, Susanna F. de Rezende, Massimo Lauria, Jakob Nordström, Alexander A. Razborov: "Clique is hard on average for regular resolution", in Proc. of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018, pp. 866–877, ACM, 2018.
URL http://dx.doi.org/10.1145/3188745.3188856

Deciding whether a graph G with n vertices has a k-clique is one of the most basic computational problems on graphs. In this work we show that certifying k-clique-freeness of Erdős–Rényi random graphs is hard for regular resolution. More precisely we show that for $k \ll \sqrt{n}$ regular resolution asymptotically almost surely requires length $n^{\Omega(k)}$ to establish that an Erdős–Rényi random graph (with appropriate edge density) does not contain a k-clique. This asymptotically optimal result implies unconditional lower bounds on the running time of several state-of-the-art algorithms used in practice.

3.5 Proof Complexity Lower Bounds from Algebraic Circuit Complexity

Michael A. Forbes (University of Illinois – Urbana-Champaign, US)

Joint work of Michael A. Forbes, Amir Shpilka, Iddo Tzameret, Avi Wigderson
Main reference Michael A. Forbes, Amir Shpilka, Iddo Tzameret, Avi Wigderson: "Proof Complexity Lower Bounds from Algebraic Circuit Complexity", in Proc. of the 31st Conference on Computational Complexity, CCC 2016, May 29 to June 1, 2016, Tokyo, Japan, LIPIcs, Vol. 50, pp. 32:1–32:17, Schloss Dagstuhl – Leibniz-Zentrum fuer Informatik, 2016.
URL http://dx.doi.org/10.4230/LIPIcs.CCC.2016.32

We give upper and lower bounds on the power of subsystems of the Ideal Proof System (IPS), the algebraic proof system recently proposed by Grochow and Pitassi [1], where the circuits comprising the proof come from various restricted algebraic circuit classes. This mimics an established research direction in the boolean setting for subsystems of Extended Frege proofs, where proof-lines are circuits from restricted boolean circuit classes. Except one, all of the subsystems considered in this paper can simulate the well-studied Nullstellensatz proof system, and prior to this work there were no known lower bounds when measuring proof size by the algebraic complexity of the polynomials (except with respect to degree, or to sparsity).

We give two general methods of converting certain algebraic lower bounds into proof complexity ones. Our methods require stronger notions of lower bounds, which lower bound a polynomial as well as an entire family of polynomials it defines. Our techniques are reminiscent of existing methods for converting boolean circuit lower bounds into related proof complexity results, such as feasible interpolation. We obtain the relevant types of lower bounds for a variety of classes (sparse polynomials, depth-3 powering formulas, read-once oblivious algebraic branching programs, and multilinear formulas), and infer the relevant proof complexity results. We complement our lower bounds by giving short refutations of the previously-studied subset-sum axiom using IPS subsystems, allowing us to conclude strict separations between some of these subsystems.

References

1 Joshua A. Grochow, Toniann Pitassi: Circuit Complexity, Proof Complexity, and Polynomial Identity Testing. FOCS 2014: 110–119

3.6 On Small-Depth Frege Proofs for Tseitin for Grids

Johan Hastad (KTH Royal Institute of Technology – Stockholm, SE)

Main reference Johan Håstad: "On Small-Depth Frege Proofs for Tseitin for Grids", in Proc. of the 58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017, Berkeley, CA, USA, October 15-17, 2017, pp. 97–108, IEEE Computer Society, 2017.
URL http://dx.doi.org/10.1109/FOCS.2017.18

We prove a lower bound on the size of a small depth Frege refutation of the Tseitin contradiction on the grid. We conclude that polynomial size such refutations must use formulas of almost logarithmic depth.

3.7 Introduction to Semialgebraic Proof Systems

Edward A. Hirsch (Steklov Institute – St. Petersburg, RU)

In this tutorial, I will define semialgebraic proof systems, explain how they work, and survey main results in the area.

3.8 Random Formulas and Interpolation in Cutting Planes

Pavel Hrubes (The Czech Academy of Sciences – Prague, CZ)

Joint work of Pavel Hrubes, Pavel Pudlák
Main reference Pavel Hrubes, Pavel Pudlák: "Random Formulas, Monotone Circuits, and Interpolation", in Proc. of the 58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017, Berkeley, CA, USA, October 15-17, 2017, pp. 121–131, IEEE Computer Society, 2017.
URL https://doi.org/10.1109/FOCS.2017.20

I will discuss the interpolation technique and how it can be adapted to prove new lower bounds for the Cutting Planes proof system. This includes the weak Bit Pigeon Hole Principle and random $\log n$-CNFs.

3.9 Parameter-free Bounded Induction

Emil Jerabek (The Czech Academy of Sciences – Prague, CZ)

We will have a look at some fragments of bounded arithmetic axiomatized by induction and polynomial induction schemata without parameters.

3.10 Bounded-depth Frege with Parity Gates and Subsystems Thereof

Leszek Kolodziejczyk (University of Warsaw, PL)

Proving superpolynomial lower bounds for bounded-depth systems with a parity connective is one of the most famous long-standing open problems in proof complexity. I will review some known results about bounded-depth Frege with parity and its subsystems. In the process, I will try to motivate a few open problems in the area.

3.11 Automatizability

Massimo Lauria (Sapienza University of Rome, IT)

We give a tutorial on the concept of automatizability of proof systems, i.e. the possibility of finding relatively short proof efficiently. We survey known results and sketch the proof that resolution is not automatizable, by [1]. We conclude by surveying the results about the closely related concept of weak automatizability, and by discussing its connections with interpolation.

References

1 Michael Alekhnovich, Alexander A. Razborov *Resolution is Not Automatizable Unless $W[P]$ is Tractable* FOCS 2001: 210–219

3.12 Are Short Proofs Narrow? QBF Resolution Is Not so Simple

Meena Mahajan (Institute of Mathematical Sciences – Chennai, IN)

Joint work of Olaf Beyersdorff, Leroy Chew, Meena Mahajan, Anil Shukla
Main reference Olaf Beyersdorff, Leroy Chew, Meena Mahajan, Anil Shukla: "Are Short Proofs Narrow? QBF Resolution Is *Not* So Simple", ACM Trans. Comput. Log., Vol. 19(1), pp. 1:1–1:26, 2018.
URL http://dx.doi.org/10.1145/3157053

One of the main techniques for proving size and space lower bounds in classical resolution proceeds via width: the results of Ben-Sasson and Wigderson [1] and of Atserias and Dalmau [2] show that lower bounds on width imply lower bounds on size and space respectively. We assess the effectiveness of such a technique for the QBF system QRes (used to prove QBFs false). Along the way, we show that the QBF proof systems Forall-Expansion+Resolution and IR-calc, provably separated in general, have the same power in their tree-like versions.

References

1 Eli Ben-Sasson, Avi Wigderson: *Short proofs are narrow – resolution made simple.* J. ACM 48(2): 149–169 (2001)
2 Albert Atserias, Víctor Dalmau: *A combinatorial characterization of resolution width.* J. Comput. Syst. Sci. 74(3): 323–334 (2008)

3.13 Partially Definable Forcing

Moritz Müller (Universität Wien, AT)

The talk explains a general method of forcing to construct models of weak arithmetics relevant for propositional proof complexity. Proofs of independence results of Paris-Wilkie, Riis and Ajtai are naturally embedded in this framework.

3.14 Lower Bound Techniques for Nullstellensatz and Polynomial Calculus

Jakob Nordström (KTH Royal Institute of Technology – Stockholm, SE)

This talk is intended to give a high-level survey of techniques for proving lower bounds for Nullstellensatz and polynomial calculus. In particular, we will focus on the method in [1] for obtaining degree lower bounds in polynomial calculus using pseudo-ideals and pseudo-reductions, and on some further extensions presented in [2].

References

1 Michael Alekhnovich, Alexander Razborov: *Lower Bounds for Polynomial Calculus: Non-Binomial Case*. Proceedings of the Steklov Institute of Mathematics 242: 18-35 (2003)
2 Mladen Miksa, Jakob Nordström: *A Generalized Method for Proving Polynomial Calculus Degree Lower Bounds*. Conference on Computational Complexity 2015: 467-487

3.15 Supercritical Space-Width Trade-offs for Resolution

Jakob Nordström (KTH Royal Institute of Technology – Stockholm, SE)

Joint work of Christoph Berkholz, Jakob Nordström
Main reference Christoph Berkholz, Jakob Nordström: "Supercritical Space-Width Trade-Offs for Resolution", in Proc. of the 43rd International Colloquium on Automata, Languages, and Programming, ICALP 2016, July 11-15, 2016, Rome, Italy, LIPIcs, Vol. 55, pp. 57:1–57:14, Schloss Dagstuhl – Leibniz-Zentrum fuer Informatik, 2016.
URL https://doi.org/10.4230/LIPIcs.ICALP.2016.57

We show that there are CNF formulas which can be refuted in resolution in both small space and small width, but for which any small-width resolution proof must have space exceeding by far the linear worst-case upper bound. This significantly strengthens the space-width trade-offs in [1], and provides one more example of trade-offs in the "supercritical" regime above worst case recently identified by [2]. We obtain our results by using Razborov's new hardness condensation technique and combining it with the space lower bounds in [3].

(This talk should have been given by Christoph Berkholz, who unfortunately had to cancel his participation on short notice.)

References

1 Eli Ben-Sasson: *Size space tradeoffs for resolution*. SIAM Journal on Computing 28(6): 2511–2525 (2009)
2 Alexander A. Razborov: *A New Kind of Tradeoffs in Propositional Proof Complexity*. J. ACM 63(2): 16:1–16:14 (2016)
3 Eli Ben-Sasson, Jakob Nordström: *Short Proofs May Be Spacious: An Optimal Separation of Space and Length in Resolution*. FOCS 2008: 709–718

3.16 Sum-of-Squares, Counting Logics and Graph Isomorphism

Joanna Ochremiak (University Paris-Diderot, FR)

Joint work of Albert Atserias, Joanna Ochremiak
Main reference Albert Atserias, Joanna Ochremiak: "Definable Ellipsoid Method, Sums-of-Squares Proofs, and the Isomorphism Problem", CoRR, Vol. abs/1802.02388, 2018.
URL http://arxiv.org/abs/1802.02388

I will discuss recent joint work with Albert Atserias on connections between equivalence in finite variable logics with counting and semidefinite relaxations of the graph isomorphism problem.

3.17 Provability of Weak Circuit Lower Bounds

Jan Pich (Universität Wien, AT)

Joint work of Moritz Müller, Jan Pich
Main reference Moritz Müller, Ján Pich: "Feasibly constructive proofs of succinct weak circuit lower bounds", Electronic Colloquium on Computational Complexity (ECCC), Vol. 24, p. 144, 2017.
URL https://eccc.weizmann.ac.il/report/2017/144

The existing circuit lower bounds for explicit Boolean functions are very constructive, as captured in the notion of natural proofs. Following initial work of Razborov and Krajíček [1, 2], we investigate the constructive aspects of circuit lower bounds from the perspective of mathematical logic and show that AC^0, $\mathrm{AC}^0[p]$ and monotone circuit lower bounds expressed by $\forall\Sigma^b_1$ formulas are provable in Jerabek's theory of approximate counting APC_1. Consequently, we obtain short proofs of poly(n)-size tautologies expressing these circuit lower bounds, where n is the number of inputs of the circuit. These proofs take place in a slight extension of Extended Frege system. In case of Razborov-Smolensky's lower bound, we give a succinct version of natural proofs against $\mathrm{AC}^0[p]$ with proofs in a propositional proof system known as WF.

References

1 Alexander Razborov: *Bounded arithmetic and lower bounds in Boolean complexity.* Feasible Mathematics II, 344–386 (1995)
2 Jan Krajíček: *Bounded arithmetic, propositional logic, and complexity theory.* Cambridge University Press, 1995.

3.18 Sum of Squares Lower Bounds from Symmetry and a Good Story

Aaron Potechin (KTH Royal Institute of Technology – Stockholm, SE)

Main reference Aaron Potechin: "Sum of squares lower bounds from symmetry and a good story", CoRR, Vol. abs/1711.11469, 2017.
URL http://arxiv.org/abs/1711.11469

The sum of squares hierarchy is a hierarchy of semidefinite programs which has the three advantages of being broadly applicable (it can be applied whenever the problem can be

phrased in terms of polynomial equations over $\mathbb{R}$), powerful (it captures the best known algorithms for several problems including max cut, sparsest cut, and unique games), and in some sense, simple (all it is really using is the fact that squares are non-negative over $\mathbb{R}$). The sum of squares hierarchy can also be viewed as the Positivstellensatz proof system.

3.19 Lifting Nullstellensatz Degree to Monotone Span Program Size

Robert Robere (University of Toronto, CA)

Joint work of Toniann Pitassi, Robert Robere
Main reference Toniann Pitassi, Robert Robere: "Lifting nullstellensatz to monotone span programs over any field", in Proc. of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018, pp. 1207–1219, ACM, 2018.
URL http://dx.doi.org/10.1145/3188745.3188914

Karchmer and Wigderson introduced an elegant model of computation, called span programs, which capture the complexity of computing with linear algebra over a field $\mathbb{F}$. In this talk, we discuss some recent work in which we characterize the monotone span program size of certain "structured" boolean functions in terms of Nullstellensatz degree over any field. This characterization leads to the resolution of a number of open problems on the complexity of span programs, including

- A superpolynomial separation between non-monotone span programs and span programs over characteristic 2,
- An exponential separation between monotone span programs over any field and monotone circuits, and
- A strongly exponential separation between monotone span programs over fields with different characteristic.

3.20 Monotone Circuit Lower Bounds from Resolution

Dmitry Sokolov (KTH Royal Institute of Technology – Stockholm, SE)

Joint work of Ankit Garg, Mika Göös, Pritish Kamath, Dmitry Sokolov
Main reference Ankit Garg, Mika Göös, Pritish Kamath, Dmitry Sokolov: "Monotone circuit lower bounds from resolution", in Proc. of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018, pp. 902–911, ACM, 2018.
URL http://dx.doi.org/10.1145/3188745.3188838

For any unsatisfiable CNF formula F that is hard to refute in the resolution proof system, we show that a gadget-composed version of F is hard to refute in any proof system whose lines are computed by efficient communication protocols (in particular, as in cutting planes)—or, equivalently, that a monotone function associated with F has large monotone circuit complexity.

This result is essentially a lifting theorem for "decision dags" and "dag communication protocols."

3.21 Bounded Arithmetic and Propositional Upper Bounds

Neil Thapen (The Czech Academy of Sciences – Prague, CZ)

I will talk about how bounded arithmetic can be used to prove, and understand, propositional upper bounds. I will briefly survey some results of this kind, and then talk in some detail about an example, a simple first-order theory that captures the kind of reasoning you can do in resolution. In particular, if you can prove something in the theory, then you get polynomial size resolution refutations. The other direction also holds, modulo some issues of uniformity, and the construction generalizes to other fragments of AC^0-Frege.

3.22 Bounded Arithmetic Does Not Collapse to Approximate Counting

Neil Thapen (The Czech Academy of Sciences – Prague, CZ)

Joint work of Leszek Kolodziejczyk; Neil Thapen

We adapt the "fixing lemma", a simple switching lemma used recently to show lower bounds for random resolution, to show that Jerabek's theory of approximate counting does not prove the CPLS principle (coloured polynomial local search). This settles an open problem by showing that bounded arithmetic is strictly stronger than approximate counting, if we compare the strength of theories by looking at their $\forall\Sigma^{b}_{1}$ consequences.

3.23 Cops-Robber games and the resolution of Tseitin formulas

Jacobo Torán (Universität Ulm, DE)

Joint work of Nicola Galesi, Navid Talebanfard, Jacobo Torán
Main reference Nicola Galesi, Navid Talebanfard, Jacobo Torán: "Cops-Robber Games and the Resolution of Tseitin Formulas", in Proc. of the Theory and Applications of Satisfiability Testing – SAT 2018 – 21st International Conference, SAT 2018, Held as Part of the Federated Logic Conference, FloC 2018, Oxford, UK, July 9-12, 2018, Proceedings, Lecture Notes in Computer Science, Vol. 10929, pp. 311–326, Springer, 2018.
URL http://dx.doi.org/10.1007/978-3-319-94144-8_19

We characterize several complexity measures for the resolution of Tseitin formulas in terms of a two person cop-robber game. Our game is a slight variation of the the one Seymour and Thomas used in order to characterize the tree-width parameter. For any undirected graph, by counting the number of cops needed in our game in order to catch a robber in it, we are able to exactly characterize the width, variable space and depth measures for the resolution of the Tseitin formula corresponding to that graph. We also give an exact game characterization of resolution variable space for any formula.

We show that our game can be played in a monotonous way. This implies that the corresponding resolution measures on Tseitin formulas correspond to those under the restriction of regular resolution.

Using our characterizations we improve the existing complexity bounds for Tseitin formulas showing that resolution width, depth and variable space coincide up to a logarithmic factor, and that variable space is bounded by the clause space times a logarithmic factor.

3.24 Nullstellensatz is Polynomially Equivalent to Sum-of-Squares over Algebraic Circuits

Iddo Tzameret (Royal Holloway, University of London, GB)

Joint work of Edward Hirsch, Iddo Tzameret

We consider the relative strength of algebraic and semi-algebraic proof systems when the complexity of proofs is measured by algebraic circuit size (in contrast to degree). We show that under this measure, Nullstellensatz simulates Sum-of-Squares proofs and Sherali-Adams. This contrasts known separations between the Nullstellensatz and Sum-of-Squares in the degree regime.

3.25 Proof Systems for Pseudo-Boolean SAT Solving

Marc Vinyals (TIFR Mumbai, IN)

Joint work of Marc Vinyals, Jan Elffers, Jesús Giráldez-Cru, Stephan Gocht, Jakob Nordström
Main reference Marc Vinyals, Jan Elffers, Jesús Giráldez-Cru, Stephan Gocht, Jakob Nordström: "In Between Resolution and Cutting Planes: A Study of Proof Systems for Pseudo-Boolean SAT Solving", in Proc. of the Theory and Applications of Satisfiability Testing – SAT 2018 – 21st International Conference, SAT 2018, Held as Part of the Federated Logic Conference, FloC 2018, Oxford, UK, July 9-12, 2018, Proceedings, Lecture Notes in Computer Science, Vol. 10929, pp. 292–310, Springer, 2018.
URL http://dx.doi.org/10.1007/978-3-319-94144-8_18

Current SAT solvers reason within the resolution proof system, and that gives them a big advantage with respect to DPLL solvers, which are limited to tree-like resolution. Pseudo-Boolean solvers can reason within cutting planes, hence they are potentially more powerful, but implementation constraints dictate that they are limited to a subset of inference rules. A natural question, then, is whether these rules are enough to exploit the full power of cutting planes.

In this talk we identify subsystems of cutting planes that arise from these limited rules and we classify them, showing in particular that pseudo-Boolean solvers are limited to resolution if their input is encoded adversarially. Additionally we craft formulas that we conjecture able to separate these proof systems at a more fundamental level.

4 A List of Some Open Problems

Below follows a (non-exhaustive) list of open research problems discussed during the seminar week. We have collected them in this report in the hope that this can serve as a convenient point of reference for the community, and in the longer term perhaps inspire the collection of open problems in proof complexity in a community research wiki or similar.

4.1 Simulation/Separation of Semi-algebraic Proof Systems

Paul Beame (University of Washington – Seattle, WA, beame@cs.washington.edu)

4.1.1 Preliminaries

I will assume familiarity with semi-algebraic proof systems: Cutting Planes, LS, LS+, Sherali-Adams, and SOS proof systems, as well as Tseitin tautologies.

4.1.2 Problems

With the exception of recent work on extension complexity lower bounds, much of the discussion of semi-algebraic proof systems is focused on rank (or degree) and not on proof size.

▶ **Open Problem 1.** *Can LS, LS+, or SOS proofs p-simulate Cutting Planes proofs for translations of Boolean formulas?*

Buss and Clote [1] showed that Cutting Planes proofs are polynomially equivalent to a restricted form of such proofs in which the division rule is only applied with divisor 2. One natural family of Boolean formulas that use this inference consists of the Tseitin formulas on bounded-degree graphs. Another particularly natural graph property to consider is the matching principle on K_{2n+1} which is known as the Parity Principle: "There is no perfect matching on K_{2n+1}". This is expressed as the following system of inequalities which is a direct translation of the clausal forms:

$$\begin{aligned}
\sum_{i\in e} x_e &\geq 1 \qquad 1 \leq i \leq 2n+1,\ e \in \binom{[2n+1]}{2} \\
x_e + x_f &\leq 1 \qquad e, f \in \binom{[2n+1]}{2},\ e \cap f \neq \emptyset \\
x_e &\geq 0 \qquad e \in \binom{[2n+1]}{2} \\
x_e &\leq 1 \qquad e \in \binom{[2n+1]}{2}
\end{aligned}$$

It is easy for all of the semi-algebraic proof systems above to derive

$$\sum_{i\in e} x_e \leq 1 \qquad 1 \leq i \leq 2n+1,\ e \in \binom{[2n+1]}{2}$$

in small size. Then by adding these inequalities one obtains:

$$2 \sum_{e\in\binom{[2n+1]}{2}} x_e \leq 2n+1$$

In Cutting Planes with divisor 2 one can now round this to obtain:

$$\sum_{e \in \binom{[2n+1]}{2}} x_e \leq n$$

and using this one easily obtains a contradiction in any of the systems. The only hard part is the division rule. Therefore it is natural to ask:

▶ **Open Problem 2.** *Are there polynomial-size LS, LS+, or SOS proofs of the Parity Principle?*

This was essentially asked by Lovasz at the 1996 Oberwolfach complexity theory workshop for the case of LS, LS+ by asking about proofs of stable set size bounds for a particular family of graphs, the line graphs of K_{2n+1}, which is an equivalent question to the one for the Parity Principle. It seems reasonable to conjecture that the answer to both of the above open problems is no.

Since the only hard part of this inference is the one line of division by 2, Open Problem 1 could be resolved depending on the outcome of the following:

▶ **Open Problem 3.** *For what values of m and n do LS, LS+, or SOS proofs have polynomial-size proofs of the following of inference?*

Given

$$\begin{aligned} 2\sum_{i=1}^{n} x_i &\leq 2m+1, \\ x_i &\geq 0 \qquad 1 \leq i \leq n \\ x_i &\leq 1 \qquad 1 \leq i \leq n \end{aligned}$$

infer

$$\sum_{i=1}^{n} x_i \leq m$$

Note that Grigoriev's work [2] on Postivstellensatz (SOS) proofs of the above constraints, which he calls the knapsack inequalities, yields large rank lower bounds for the case that m is near $n/2$ (within roughly $\pm\sqrt{n}$). By the extension complexity results of Lee, Raghavendra, and Steurer [3] this implies exponential size lower bounds in this case. In the case of the Parity Principle, m is $\Theta(\sqrt{n})$ so it is not covered by that bound.

References

1 Samuel R. Buss and Peter Clote. Cutting planes, connectivity, and threshold logic. *Arch. Math. Log.*, 35(1):33–62, 1996.

2 Dima Grigoriev. Complexity of positivstellensatz proofs for the knapsack. *Computational Complexity*, 10(2):139–154, 2001

3 James R. Lee, Prasad Raghavendra, and David Steurer. Lower bounds on the size of semidefinite programming relaxations. In *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing, STOC 2015, Portland, OR, USA, June 14-17, 2015*, pages 567–576, 2015.

4.2 Geometric Lower Bounds for Cutting Planes

Yuval Filmus (Technion – Haifa, IL, yuvalfi@cs.technion.ac.il)

Come up with a lower bound technique for cutting planes that, as opposed to the interpolation method or DAG-like communication, does not a reduction to circuit complexity. For example, a geometric method based on properties of polytopes, like algebraic decision tree lower bounds.

4.3 The Effect of Arity on the Power of Semantic Cutting Planes

Yuval Filmus (Technion – Haifa, IL, yuvalfi@cs.technion.ac.il)

4.3.1 Preliminaries

Cutting planes is usually defined with the syntactic rules *addition* and *division*. The first rule allows deducing from $\sum_i a'_i x_i \geq b'$ and $\sum_i a''_i x_i \geq b''$ the line $\sum_i (c'a'_i + c''a''_i)x_i \geq c'b' + c''b''$ for all integers $c', c'' \geq 0$, and the second rule allows deducing from $\sum_i ca_i x_i \geq b$ the line $\sum_i a_i x_i \geq \lceil b/c \rceil$ for all $c \geq 1$.

One can augment these rules with semantic rules. The proof system *k-ary semantic cutting planes* allows deducing a line L from lines $L_1, \ldots, L_k$ as long as every $0,1$-assignment which satisfies $L_1, \ldots, L_k$ also satisfies L. Note that when $k = 2$, the syntactic rules are no longer necessary, and that when $k = 1$, we only need the syntactic rule of addition.

Filmus, Hrubeš and Lauria [1] showed that unary semantic cutting planes cannot be p-simulated by syntactic cutting planes, and proved exponential lower bounds on n^ϵ-ary semantic cutting planes.

4.3.2 Problem

▶ **Open Problem 4.** *Let $1 \leq k_1 < k_2$ be constants. Does k_1-ary semantic cutting planes p-simulate k_2-ary semantic cutting planes?*

Hrubeš and Pudlák [2] gave an affirmative answer for the analogous question on monotone real circuits.

References

1 Yuval Filmus, Pavel Hrubeš, Massimo Lauria: *Semantic versus Syntactic Cutting Planes.* STACS 2016: 35:1–35:13

2 Pavel Hrubeš, Pavel Pudlák *A note on monotone circuits.* Inf. Process. Lett. 131: 15–19 (2018)

4.4 Questions on Ideal Proof Systems

Joshua A. Grochow (University of Colorado – Boulder, USA, jgrochow@colorado.edu)

4.4.1 Preliminaries

▶ **Definition 1** (Ideal Proof System [4, Def. 1.9] (cf. [5, 6]))**.** An *IPS certificate* that a polynomial $G(\vec{x}) \in \mathbb{F}[\vec{x}]$ is in the ideal [respectively, radical of the ideal] generated by $F_1(\vec{x}), \ldots, F_m(\vec{x})$ is a polynomial $C(\vec{x}, \vec{y})$ such that
1. $C(\vec{x}, \vec{0}) = 0$, and
2. $C(\vec{x}, F_1(\vec{x}), \ldots, F_m(\vec{x})) = G(\vec{x})$ [respectively, $G(\vec{x})^k$ for any $k > 0$].

An *IPS derivation* of G [resp. G^k] from $F_1, \ldots, F_m$ is a circuit computing some IPS certificate that $G \in \langle F_1, \ldots, F_m \rangle$ [resp., $G \in \sqrt{\langle F_1, \ldots, F_m \rangle}$].

When applied as a proof system of unsatisfiability of Boolean formulas, we translate a CNF φ into a system of equations as follows, and an IPS proof is a derivation that 1 is in the ideal generated by the following polynomials. We translate a clause κ of φ into a single algebraic equation $F(\vec{x})$ as follows: $x \mapsto 1 - x$, $x \vee y \mapsto xy$. This translation has the property that a $\{0,1\}$ assignment satisfies κ if and only if it satisfies the equation $F = 0$. Let $\kappa_1, \ldots, \kappa_m$ denote all the clauses of φ, and let F_i be the corresponding polynomials. Then the system of equations we consider is $F_1(\vec{x}) = \cdots = F_m(\vec{x}) = x_1^2 - x_1 = \cdots = x_n^2 - x_n = 0$. The latter equations force any solution to this system of equations to be $\{0,1\}$-valued. (Note that, in principle, Boolean tautologies can be refuted without the Boolean axioms $x_i^2 - x_i$, but we do not know how this affects the complexity of the proofs in general.)

To motivate the following variant of IPS, we may consider

$$F_1(x_1, \ldots, x_n), \ldots, F_m(x_1, \ldots, x_n)$$

as a polynomial map $F = (F_1, \ldots, F_m) \colon \mathbb{F}^n \to \mathbb{F}^m$. Then this system of polynomials has a common zero if and only if $\vec{0}$ is the image of F. In fact, Grochow and Pitassi [4, Appendix B] show that for any system of equations coming from an unsatisfiable Boolean CNF, the system of polynomials has a common zero if and only if $\vec{0}$ is in the *closure* of the image of F. This holds regardless of whether the equations include $x_i^2 - x_i = 0$, $x_i^2 - 1 = 0$, or neither of these, though at the moment the proof only works over algebraically closed fields and over dense subfields of $\mathbb{C}$ (such as $\mathbb{Q}(i)$).

▶ **Definition 2** (The Geometric Ideal Proof System [4, App. B])**.** A *geometric IPS certificate* that a system of $\mathbb{F}$-polynomial equations $F_1(\vec{x}) = \cdots = F_m(\vec{x}) = 0$ is unsatisfiable over $\overline{\mathbb{F}}$ is a polynomial $C \in \mathbb{F}[y_1, \ldots, y_m]$ such that
1. $C(0, 0, \ldots, 0) = 1$, and
2. $C(F_1(\vec{x}), \ldots, F_m(\vec{x})) = 0$. In other words, C is a polynomial relation amongst the F_i.

A *geometric IPS proof* of the unsatisfiability of $F_1 = \cdots = F_m = 0$, or a *geometric IPS refutation* of $F_1 = \cdots = F_m = 0$, is an $\mathbb{F}$-algebraic circuit on inputs $y_1, \ldots, y_m$ computing some geometric certificate of unsatisfiability.

If C is a geometric certificate, then $1 - C$ is an IPS certificate that involves only the y_i. Hence the smallest circuit size of any geometric certificate is at least the smallest circuit size of any algebraic certificate. We do not know, however, if these complexity measures are polynomially related, as highlighted in a question below.

We call a system of equations "standard Boolean" if it includes $x_i^2 = x_i$ for all i, and "multiplicative Boolean" if it includes $x_i^2 = 1$ for all i; by "Boolean system of equations" we mean either of these.

4.4.2 Problems

▶ **Open Problem 5** (Hrubeš [7]). *Find a polynomial f that vanishes on $\{0,1\}^n$ such that any IPS certificate showing that $f \in \langle x_i^2 - x_i | x \in [n] \rangle$ requires super-polynomial algebraic circuit size.*

Of course, if the f is the translation of an unsatisfiable Boolean CNF, then its existence would imply VP $\neq$ VNP, and moreover such a CNF-translation f must exist assuming NP $\not\subseteq$ coAM. A conditional result would also be interesting here, so long as the condition is weaker than NP $\not\subseteq$ coAM; perhaps the most interesting would be finding such an f assuming only VP $\neq$ VNP.

▶ **Open Problem 6** ([4, Open Question 8.2]). *Let $\beta \notin \{0, \ldots, 2n\}$, and let $\mathbb{F}$ be a field of characteristic at least $2n+1$. Prove lower bounds on restricted versions of IPS certificates (as in, e. g., [1]) for the unsatisfiable system of equations*

$$x_1 + \cdots + x_n - x = x_{n+1} + \cdots + x_{2n} - x' = x + x' - \beta = x_1^2 - x_1 = \cdots = x_n^2 - x_n = 0.$$

▶ **Open Problem 7** ([4, Open Question A.12]). *Does every IPS certificate for the $n \times n$ Inversion Principle $XY = I \Rightarrow YX = I$ require computing a determinant? That is, is it the case that for every IPS certificate C, some determinant of size $n^{\Omega(1)}$ reduces to C by a $O(\log n)$-depth circuit reduction?*

A positive answer here would show that, indeed, the Inversion Principle does not have an IPS proof of logarithmic depth unless the determinant has polynomial-size algebraic formulas.

▶ **Open Problem 8** ([4, Open Question B.4]). *For Boolean systems of equations, is Geometric IPS polynomially equivalent to IPS? That is, is there always a geometric certificate whose circuit size is at most a polynomial in the circuit size of the smallest algebraic certificate?*

For radical membership, an exponential degree upper bound is known (often called Effective Nullstellensatz), and known to be tight, but we could ask about strengthening such bounds to circuit size. For ideal membership, we observed that a subexponential IPS size upper bound would violate the Space Hierarchy Theorem because ideal membership in general is EXPSPACE-complete. But for radical membership, we do not know how to rule this out.

▶ **Open Problem 9** ([4, Open Question 1.11]). *For any*

$$G(\vec{x}) \in \sqrt{\langle F_1(\vec{x}), \ldots, F_m(\vec{x}) \rangle}$$

is there always an IPS-certificate of subexponential size that G is in the radical *of $\langle F_1, \ldots, F_m \rangle$? Similarly, for $G, F_1, \ldots, F_m \in \mathbb{Z}[x_1, \ldots, x_n]$, is there a constant-free $\mathrm{IPS}_{\mathbb{Z}}$-certificate of subexponential size that $aG(\vec{x})$ is in the* radical *of the ideal $\langle F_1, \ldots, F_m \rangle$ for some integer a?*

▶ **Open Problem 10** ([4, General Question 7.4]). *Given a family of cosets of ideals $f_n^{(0)} + I_n$ (or more generally modules) of polynomials, with $I_n \subseteq R[x_1, \ldots, x_{poly(n)}]$, consider the function families $(f_n) \in (f_n^{(0)} + I_n)$ (meaning that $f_n \in f_n^{(0)} + I_n$ for all n) under any computational reducibility $\leq$ such as p-projections. What can the $\leq$ structure look like? For example:*

a. *When, if ever, is there such a unique $\leq$-minimum (even a single nontrivial example would be interesting)?*
b. *Can there be infinitely many incomparable $\leq$-minima?*
c. *Say a $\leq$-degree $\mathbf{d}$ is "saturated" in $(f_n^{(0)} + I_n)$ if every $\leq$-degree $\mathbf{d}' \geq \mathbf{d}$ has some representative in $f^{(0)} + I$. Must saturated degrees always exist? We suspect yes, given that one may multiply any element of I by arbitrarily complex polynomials.*
d. *What can the set of saturated degrees look like for a given $(f_n^{(0)} + I_n)$?*
e. *Must every $\leq$-degree in $f^{(0)} + I$ be* below *some saturated degree?*
f. *What can the $\leq$-structure of $f^{(0)} + I$ look like below a saturated degree?*
g. *...*

Problem 10 is of interest even when $f^{(0)} = 0$, that is, for ideals and modules of functions rather than their nontrivial cosets. For ideals, these questions are also related to algebraic natural proofs [2, 3].

References

1 Michael A. Forbes, Amir Shpilka, Iddo Tzameret, Avi Wigderson: *Proof Complexity Lower Bounds from Algebraic Circuit Complexity.* CCC 2016: 32:1–32:17
2 Michael A. Forbes, Amir Shpilka, Ben Lee Volk: *Succinct hitting sets and barriers to proving algebraic circuits lower bounds.* STOC 2017: 653–664
3 Joshua A. Grochow, Mrinal Kumar, Michael Saks, Shubhangi Saraf: *Towards an algebraic natural proofs barrier via polynomial identity testing.* Electronic Colloquium on Computational Complexity (ECCC) 24: 009 (2017)
4 Joshua A. Grochow, Toniann Pitassi: *Circuit complexity, proof complexity, and polynomial identity testing.* FOCS 2014
5 Toniann Pitassi: *Algebraic propositional proof systems.* Descriptive Complexity and Finite Models 1996: 215–244
6 Toniann Pitassi: *Propositional proof complexity and unsolvability of polynomial equations.* ICM 1998: 215–244
7 Pavel Hrubeš: *Arithmetic circuits and proof complexity* Algebraic Complexity Theory 2016

4.5 The Complexity of Linear Resolution

Jan Johannsen (Ludwig-Maximillians-Universität München, DE, jan.johannsen@ifi.lmu.de)

4.5.1 Preliminaries

A linear resolution refutation of a CNF formula F is a sequence of clauses $C_1, \ldots, C_m$ such that

- C_1 is a clause from F,
- C_m is the empty clause, and
- each clause C_{i+} is obtained by resolution from C_i and either a clause D from F, or an earlier clause C_j for $j < i$.

In other words, a resolution refutation is linear if in every resolution step, one of the used clauses is the one derived in the immediately preceding step.

It is now known that linear resolution p-simulates tree-like resolution, but is not simulated by regular resolution [1].

4.5.2 Problem

The relationship between linear and full resolution with respect to p-simulation is a long-standing open problem.

▶ **Open Problem 11.** *Is there a super-polynomial or even exponential separation between linear and unrestricted resolution? Or does linear resolution p-simulate unrestricted resolution?*

References

1 S. R. Buss, J. Johannsen, On Linear Resolution, *Journal on Satisfiability, Boolean Modeling and Computation*, 16:23–35, 2017.

4.6 New Hard Examples for Regular Resolution

Jan Johannsen (Ludwig-Maximillians-Universität München, DE, jan.johannsen@ifi.lmu.de)

4.6.1 Preliminaries

A (dag-like) resolution refutation is *regular* if on every path through the proof dag every variable is resolved on at most once. There are several examples that witness an exponential separation of regular from unrestricted dag-like resolution [1, 4].

An ongoing direction of research tries to analyse the complexity of refinements of resolution that correspond to contemporary SAT algorithms using conflict-driven clause learning. These refinements are between regular and full dag-like resolution w.r.t. size complexity. There are polynomial upper bounds in these systems for all the hard examples mentioned above [2, 3], so they can have an exponential speed-up over regular resolution.

4.6.2 Problem

An open question is to give a super-polynomial or exponential separation between these clause learning proof systems and full resolution. Any separating example needs to necessarily also separate regular from full resolution. But for all such known exaples we have polynomial upper bounds. So to attack this problem, we first need to solve the following:

▶ **Open Problem 12.** *Find new examples of families of formulas that have polynomial size resolution refutations, but require exponential size regular resolution refutations.*

References

1 Michael Alekhnovich, Jan Johannsen, Toniann Pitassi, Alasdair Urquhart. An exponential separation between regular and general resolution. *Theory of Computing*, **3**(5):81–102, 2007.
2 Maria Luisa Bonet, Samuel R. Buss, Jan Johannsen. Improved separations of regular resolution from clause learning proof systems. *Journal of Artificial Intelligence Research*, 49:669–703, 2014.
3 S. Buss, L. Kołodziejczyk, *Small stone in pool. Logical Methods in Computer Science*, 10(2), 2014, paper 16.
4 A. Urquhart, *A near-optimal separation of regular and general resolution*, SIAM Journal on Computing, 40 (2011), pp. 107–121.

4.7 R(Lin/$\mathbb{F}_2$) Lower Bounds via Randomised Feasible Interpolation

Igor C. Oliveira (University of Oxford, GB, igor.carboni.oliveira@cs.ox.ac.uk)

4.7.1 Preliminaries

We are interested in the problem of establishing (dag-like) lower bounds for R(Lin/$\mathbb{F}_2$), a proof system that corresponds to resolution extended with linear equations over the field $\mathbb{F}_2$. For more details about this proof system, we refer to Itsykson and Sokolov [1], where *tree-like* lower bounds are also described. (Note that the work of Buss, Kolodziejczyk, and Zdanowski [2] shows a collapse of $F_d[\oplus]$-Frege to depth three, which further motivates the study of R(Lin/$\mathbb{F}_2$) and its extensions.)

More recently, Krajíček [4] proposed an extension of the feasible interpolation technique that employs randomized communication complexity, and that allows one to reduce lower bounds for R(Lin/$\mathbb{F}_2$) and other proof systems to the investigation of monotone circuits with local oracles. This is an extension of monotone circuits that incorporates extra inputs (local oracles) to help the computation. While super-polynomial lower bounds against monotone circuits with local oracles for computational problems such as clique vs. colorings would provide lower bounds for R(Lin/$\mathbb{F}_2$), currently only restricted lower bounds against such circuits are known [3].

We refer to the last paper for a precise definition of this circuit model. Here we only recall that a parameter μ measures the power of the local oracles. (It is connected to the failure probability of certain randomised communication protocols derived from propositional proofs.) This parameter appears in the statement of the problem, described next.

4.7.2 Problems

Let $k \geq 3$ be a positive integer, $U_{n,k}$ be the set of n-vertex graphs corresponding to k-cliques, and $V_{n,k}$ be the set of complete $(k-1)$-partite graphs over n vertices. Show that any monotone circuit with local oracles and locality $\mu \leq 1/100$ that separates $U_{n,k}$ and $V_{n,k}$ must have super-polynomial size (say, for some super-constant function $k(n) \leq n$).

We are also interested in non-trivial results for $k = 3$ (triangles vs. complete bipartite graphs). While lower bounds in this regime will not have important consequences in proof complexity, they might shed light into the power and limitations of this circuit model, and further inform the randomised feasible interpolation program.

References

1 Dmitry Itsykson, Dmitry Sokolov: *Lower Bounds for Splittings by Linear Combinations.* MFCS (2) 2014: 372–383
2 S. R. Buss, L. A. Kołodziejczyk, K. Zdanowski: *Collapsing modular counting in bounded arithmetic and constant depth propositional proofs.* Transactions of the AMS 367 (2015), 7517–7563.
3 Jan Krajíček, Igor Carboni Oliveira: *On monotone circuits with local oracles and clique lower bounds.* CoRR abs/1704.06241 (2017)
4 Jan Krajíček: *Randomized feasible interpolation and monotone circuits with a local oracle.* CoRR abs/1611.08680 (2016)

4.8 Unprovability of Circuit Upper Bounds in Logical Theories

Igor C. Oliveira (University of Oxford, GB, igor.carboni.oliveira@cs.ox.ac.uk)

4.8.1 Preliminaries

It is believed that $\mathsf{NP} \not\subseteq \mathsf{P/poly}$, but it is consistent with our knowledge that $\mathsf{NTIME}[2^n] \subseteq \mathsf{SIZE}[O(n)]$. Given the lack of techniques for proving non-trivial lower bounds, we are interested in the logical complexity/(un)provability aspects of circuit complexity theory. This research program is a few decades old, but for brevity we restrict our discussion to a small number of references more directly connected to our problem.

Cook's theory PV [1] or its mild extensions seem to formalize a large fraction of contemporary complexity theory. (We refer to the recent work of Muller and Pich [2] for more background on the formalization of circuit complexity in bounded arithmetic.) It is therefore of interest to understand when a given conjecture is provable or at least consistent with PV. We believe that NP requires large circuits, but since we don't know how to establish this result at this point, can we at least show that PV does *not* prove that $\mathsf{NP} \subseteq \mathsf{SIZE}[100n]$?

Cook and Krajíček [3] established conditional results of this form for PV and S^1_2. More recently, Krajíček and Oliveira [4] unconditionally showed that PV does not prove that P (polynomial time) is contained in $\mathsf{SIZE}[n^k]$, when k is a fixed constant. In particular, there is a model $\mathfrak{M}$ of PV where a lot of complexity theory holds, and moreover in $\mathfrak{M}$ there are languages in P that cannot be computed by circuits of size n^{100}.

We would like to extend this theorem to an unprovability result for stronger logical theories. A natural candidate is the theory APC1 investigated by E. Jerabek and other authors. This theory extends PV and allows the formalization of many probabilistic constructions and randomised algorithms. Formally, APC1 adds to the axioms of PV a dual weak pigeonhole principle for polynomial-time function symbols. With enough work, this can be used to (approximately) formalize probabilities and events. We refer to Jerabek's related work and Muller and Pich [2] for further details.

4.8.2 Problem

Let $\mathsf{UP}_{k,c}(f)$ be the upper bound sentence (in the language of PV) from Krajíček and Oliveira [4] stating that the language encoded by the function symbol f can be computed by circuits of size at most $c \cdot n^k$. Show that for each $k \geq 1$ there is a function symbol g in the language of PV such that for no constant $c \geq 1$ APC1 proves the sentence $\mathsf{UP}_{k,c}(g)$.

We believe that a solution to this problem will require interesting new ideas from logic and complexity theory.

References

1 Stephen Cook: *Feasibly constructive proofs and the propositional calculus.* STOC 1975, 83–97.
2 Moritz Müller, Ján Pich: *Feasibly constructive proofs of succinct weak circuit lower bounds.* Electronic Colloquium on Computational Complexity (ECCC) 24: 144 (2017)
3 Stephen A. Cook, Jan Krajíček: Consequences of the provability of NP ⊆ P/poly. J. Symb. Log. 72(4): 1353–1371 (2007)
4 Jan Krajíček, Igor Carboni Oliveira: *Unprovability of circuit upper bounds in Cook's theory PV.* Logical Methods in Computer Science 13(1) (2017)

4.9 Dag Communication Lower Bounds

Dmitry Sokolov (KTH Royal Institute of Technology – Stockholm, SE, sokolovd@kth.se)

▶ **Definition 1.** Let $U, V \in \{0,1\}^n$ be two sets. Let us consider a triple (H, A, B), where H is a directed acyclic graph, $A : H \times U \to \mathbb{N}$ and $B : H \times V \to \mathbb{N}$. We say that vertex $h \in H$ is valid for pair $(x, y) \in U \times V$ iff $A(h, x) = B(h, y) = 1$. We call this triple a *EQ dag protocol* for the pair (U, V) and some relation $N : U \times V \to T$, where T is a finite set of "possible answers", if the following holds:

- H is an acyclic graph and the out-degree of all its vertices is at most 2;
- the leaves of H are marked by element of T;
- there is a *root* $s \in H$ with in-degree 0 and this vertex is valid for all pairs from $U \times V$;
- if $h \in H$ is valid for pair (x, y) and h is not a leaf then at least one child of h is valid for (x, y);
- if $h \in H$ is valid for pair (x, y), h is a leaf and h is marked by $t \in T$ then $t \in N(x, y)$.

The size of the game is the size of the graph H.

We say that we have *boolean dag protocol* iff vertex is valid in case that $A(h, x) = B(h, y) = 1$.

▶ **Definition 2.** Canonical search problem $Search_\varphi$ for an unsatisfiable formula $\varphi(x, y)$ in CNF: Alice receives values for the variables x, Bob receives values for the variables y, and their goal is to find a clause of φ such that it is unsatisfied by this substitution.

We know that in case of boolean protocols an analog of Karchmer–Wigderson Theorem holds for boolean protocols (for KW and KW^m relations) and (monotone) circuits. If we apply this protocols for canonical search problem this protocols capture the huge class of proof systems. And we can prove lower bound for boolean protocols.

▶ **Open Problem 13.** *Can one prove lower bounds on EQ dag protocols for $Search_\varphi$ or KW^m relations?*

▶ **Open Problem 14.** *In boolean case can we prove lower bound for three players in NOF model for $Search_{\varphi(x,y,z)}$ relation (vertex is valid iff $A(h, x, y) = B(h, y, z) = C(h, x, z) = 1$)?*

4.10 Game Characterization of Resolution Space

Jacobo Torán (University of Ulm, DE, jacobo.toran@uni-ulm.de)

4.10.1 Preliminaries

Game characterizations of complexity measures in resolution have helped to better understand these measures and the relations among them. Such game characterizations exist for width [1], space in tree-like resolution [2], depth [3] and variable space [4].

4.10.2 Problem

Is there a characterization of resolution clause space in terms of a combinatorial game?

References

1 Albert Atserias, Víctor Dalmau: *A Combinatorial Characterization of Resolution Width.* CCC 2003: 239–247
2 Juan Luis Esteban, Jacobo Torán: *A combinatorial characterization of treelike resolution space.* Inf. Process. Lett. 87(6): 295–300 (2003)
3 Alasdair Urquhart: *The Depth of Resolution Proofs.* Studia Logica 99(1-3): 349–364 (2011)
4 Nicola Galesi, Navid Talebanfard and Jacobo Torán: *Cops-Robber games and the resolution of Tseitin formulas.* SAT 2018

4.11 Miters

Alasdair Urquhart (University of Toronto – Toronto, CA, urquhart@cs.toronto.edu)

4.11.1 Preliminaries

A "miter" is a type of problem considered by hardware designers. Given a circuit C, with inputs $x_1, \ldots, x_n$, and gates $g_1, \ldots, g_m$, construct an isomorphic circuit C' with gates $g'_1, \ldots, g'_m$. The miter $M(C)$ is the CNF formula formalizing the statement "C and C' give different outputs for the inputs $x_1, \ldots, x_n$."

Obviously, this statement is unsatisfiable, and what is more, it has a short, narrow resolution refutation. However, CDCL solvers have a hard time with such statements. Donald Knuth [1] describes this situation as "somewhat scandalous."

4.11.2 Problem

The problem is simply to give a good theoretical explanation of what is going on here.

References

1 Donald Knuth *The Art of Computer Programming, Volume 4, Fascicle 6, "Satisfiability", p. 121*

5 Examples of Outcomes of the Workshop

It still a bit too early for any concrete publications to have resulted from the workshop, but participants have reported that the the following papers, in different stages of preparation, were significantly influenced by discussions during the workshop:

References

1 Olaf Beyersdorff, Leroy Chew, Judith Clymo and Meena Mahajan: *Short Proofs in QBF Expansion.* Submitted
2 Stefan Dantchev, Nicola Galesi and Barnaby Martin: *Resolution and the binary encoding of combinatorial principles.* Manuscript in preparation
3 Jan Elffers, Jesús Giráldez-Cru, Jakob Nordström, and Marc Vinyals: *Using Combinatorial Benchmarks to Probe the Reasoning Power of Pseudo-Boolean Solvers.* SAT 2018
4 Nicola Galesi, Navid Talebanfard and Jacobo Torán: *Cops-Robber games and the resolution of Tseitin formulas.* SAT 2018

5 Alasdair Urquhart: *Switching lemmas and bounded depth Frege proofs.* Manuscript in preparation

Participants of the workshop have reported about other concrete research projects that resulted to a large part from contacts during the week at Dagstuhl. Since many of these projects are still in a start-up phase it would seem slightly premature to list concrete participants, but it can be mentioned that these projects involve researchers from the Academy of Sciences of the Czech Republic, KTH Royal Institute of Technology, Ludwig Maximilians Universität München, Tata Institute of Fundamental Research, University of Toronto, and University of Warsaw, in various constellations.

6 Evaluation by Participants

In addition to the traditional Dagstuhl evaluation after the workshop, the organizing committee also arranged for a separate evaluation which specific questions about different aspects of the workshop. Below follows a summary of the answers.

The participants unanimously praise three elements of the workshop. One was good talks, both in the selection of topics and in length–in particular, the survey talks were highly appreciated. 78% of the respondents found the balance between longer and shorter talks mostly right, and 61% approved of the choice to have 55-minutes survey talks rather than 80-minutes tutorials. Another good aspect was the focused topic of the workshop, which made it easy to keep discussions relevant. Finally, the choice of participants was rated as balanced and conducive to a good atmosphere.

There was a general feeling, however, that the workshop program was perhaps a bit on the dense side, especially during the first one or two days.

When asked about topics that were felt to be missing, participants mostly cited neighbouring areas such as SAT solving, switching lemmas, and computational complexity theory in general, but some participants were also missing specific topics within proof complexity such as upper bounds for the Frege proof system and lower bounds for space complexity. It should be said, though, that the choice of topics for survey talks were based on an opinion poll before the workshop, and all topics with strong support in this opinion poll were given a survey talk slot (except when the organizing committee was unable to find a suitable speaker willing to give a survey talk).

As for the opposite question, whether some topics were superfluous, there was no clear consensus among the respondents, and the conclusion seems to be that for each topic a clear majority of participants felt that this topic was an essential one for the workshop. We had a combined panel discussion and open problems session, which 65% of the participants rated positively.

Regarding the social aspects of the seminar, participants were disappointed that there was not a hike, but felt it was a good decision to drop it because of bad weather. 89% of respondents enjoyed the music evening that was organized on Thursday.

To sum up, feedback was overwhelmingly positive. 83% of participants said they would definitely come again to a similar workshop, and 17% would probably come again.

Participants

- Amirhossein Akbar Tabatabei
The Czech Academy of Sciences – Prague, CZ
- Albert Atserias
UPC – Barcelona, ES
- Paul Beame
University of Washington – Seattle, US
- Arnold Beckmann
Swansea University, GB
- Olaf Beyersdorff
University of Leeds, GB
- Ilario Bonacina
UPC – Barcelona, ES
- Igor Carboni Oliveira
University of Oxford, GB
- Marco Carmosino
University of California – San Diego, US
- Leroy Chew
University of Leeds, GB
- Stefan Dantchev
Durham University, GB
- Yuval Filmus
Technion – Haifa, IL
- Noah Fleming
University of Toronto, CA
- Michael A. Forbes
University of Illinois – Urbana-Champaign, US
- Nicola Galesi
Sapienza University of Rome, IT
- Michal Garlik
UPC – Barcelona, ES
- Joshua A. Grochow
University of Colorado – Boulder, US
- Tuomas Hakoniemi
UPC – Barcelona, ES
- Johan Hastad
KTH Royal Institute of Technology – Stockholm, SE
- Edward A. Hirsch
Steklov Institute – St. Petersburg, RU
- Pavel Hrubes
The Czech Academy of Sciences – Prague, CZ
- Dmitry Itsykson
Steklov Institute – St. Petersburg, RU
- Emil Jerabek
The Czech Academy of Sciences – Prague, CZ
- Jan Johannsen
LMU München, DE
- Raheleh Jalali Keshavarz
Czech Academy of Sciences – Brno, CZ
- Leszek Kolodziejczyk
University of Warsaw, PL
- Antonina Kolokolova
Memorial University of Newfoundland – St. John's, CA
- Oliver Kullmann
Swansea University, GB
- Massimo Lauria
Sapienza University of Rome, IT
- Meena Mahajan
Institute of Mathematical Sciences – Chennai, IN
- Barnaby Martin
Durham University, GB
- Moritz Müller
Universität Wien, AT
- Jakob Nordström
KTH Royal Institute of Technology – Stockholm, SE
- Joanna Ochremiak
University Paris-Diderot, FR
- Jan Pich
Universität Wien, AT
- Aaron Potechin
KTH Royal Institute of Technology – Stockholm, SE
- Pavel Pudlák
The Czech Academy of Sciences – Prague, CZ
- Ninad Rajgopal
University of Oxford, GB
- Kilian Risse
KTH Royal Institute of Technology – Stockholm, SE
- Robert Robere
University of Toronto, CA
- Rahul Santhanam
University of Oxford, GB
- Dmitry Sokolov
KTH Royal Institute of Technology – Stockholm, SE
- Neil Thapen
The Czech Academy of Sciences – Prague, CZ
- Jacobo Torán
Universität Ulm, DE
- Iddo Tzameret
Royal Holloway, University of London, GB
- Alasdair Urquhart
University of Toronto, CA
- Marc Vinyals
TIFR Mumbai, IN