Mathematisches Forschungsinstitut Oberwolfach

Report No. 37/2017

DOI: 10.4171/OWR/2017/37

Proof Complexity and Beyond

Organised by
Albert Atserias, Barcelona
Jakob Nordström, Stockholm
Toniann Pitassi, Toronto
Alexander Razborov, Chicago/Moscow

13 August – 19 August 2017

Abstract. Proof complexity is a multi-disciplinary intellectual endeavor that addresses questions of the general form "how difficult is it to prove certain mathematical facts?" The current workshop focused on recent advances in our understanding of logic-based proof systems and on connections to algorithms, geometry and combinatorics research, such as the analysis of approximation algorithms, or the size of linear or semidefinite programming formulations of combinatorial optimization problems, to name just two important examples.

Mathematics Subject Classification (2010): Primary 03F20; Secondary 68Q17, 68W25, 90C22.

Introduction by the Organisers

The workshop *Proof Complexity and Beyond* was organised by Albert Atserias (Barcelona), Jakob Nordström (Stockholm), Toniann Pitassi (Toronto) and Alexander Razborov (Chicago/Moscow). The workshop was held on August 13th-19th and was attended by approximately 50 participants. The program featured a total of 32 talks: 4 long lectures, 7 one-hour talks and 21 short talks. In addition, there was an open problem session and during breaks intensive interaction took place in smaller groups.

As originally conceived by Stephen Cook and Robert Reckhow in their seminal article [4], propositional proof complexity is "the study of the length of the shortest proof of a propositional tautology in various proof systems as a function of the length of the tautology." The original motivation for what came to be known as Cook's program was to shed light on the celebrated P vs. NP problem, today one

of the Clay Mathematical Institute Millenium Problems. A significant portion of the workshop was devoted to Cook's program proper, i.e. attempts to further advance our understanding of logic-based proof systems.

A major theme of the workshop stems from the following simple observation. Two of the most fundamental mathematical results underlying algebraic and real geometry, Hilbert's Nullstellensatz and Stengle's Positivestellensatz, are essentially proof systems for proving unsatisfiability of a system of polynomial equations and inequalities, respectively. In turn, the grading of "proofs" in such proof systems by their "complexity" underlies several of the successful applications of these results of classical mathematics to theoretical computer science and affine areas. A key observation underlying this connection is that when the degree of the proof is bounded, it can be found efficiently by a Gröbner basis algorithm or a semidefinite program, which leads to a myriad of practical and theoretical applications in areas that include optimization theory [7], probability theory [5], quantum information theory [1], extremal combinatorics [6, 8], algorithms for machine learning [2], and computational complexity [3].

We now proceed to describing concrete talks delivered at the workshop, and we attempt to classify them into groups according to the above lines.

Semialgebraic proofs, combinatorial optimization and inapproximability Semialgebraic proof systems are based on the duality theorem of linear programming and the vastly more general duality theory for semialgebraic sets known as Stengle's Positivstellensatz. One interesting consequence of this duality is that very similar questions are worked on by researchers in (at least) two different areas: proof complexity and combinatorial optimization/inapproximability. One of our main intentions was to bring these two communities together, and here we report on how this goal was achieved during the workshop.

Two long lectures by O'Donnell and Atserias gave an extensive overview of this area from the two perspectives. Another long lecture by Lee was devoted to the extension complexity in convex optimization that makes one of the most striking applications of semi-algebraic proof systems today.

Two talks were devoted to Cutting Planes, which is one of the most prominent proof systems used in Operation Research. Fleming presented a recent breakthrough result making major progress on the long-standing open problem of proving lower bounds on the size of cutting planes refutations for random k-CNF formulas. Vinyals in his talk gave the first true size-space trade-offs for Cutting Planes.

The Sum-of-Squares proof system (SoS) is the one directly based on the Positivestellensatz, and it is arguably the most important one in the family, partly due to its connections with the Unique Games Conjecture (see, e.g., [3]). Not surprisingly, quite a number of talks at the workshop were devoted to this system, and its close cousins like Sherali-Adams, from several different perspectives.

Tulsiani and Kothari spoke of the complexity of the constraint satisfaction problem (CSP) in this context, which is one of the most fundamental core problems in the area. Ochremiak discussed a general theory of reductions between CSPs

of various types based on classical algebraic constructions such as algebras of polymorphisms. Schramm spoke of a recent result on the equivalence between SoS and spectral algortihms in a somewhat broader context, and Dawar connected SoS to fixed-point logic with counting.

Finally, a number of talks gave applications of SoS beyond *discrete* optimization. Guruswami focussed on the fundamental problem of optimizing homogeneous polynomials over the sphere. Steurer and Potechin discussed very interesting applications to machine learning, of which the famuous tensor completion problem makes an important example. Raymond spoke of intriguing and unexpected connections between SoS and the theory of flag algebras [8] successfully employed in Extremal Combinatorics.

Algebraic proof systems Algebraic proof systems have been extensively studied in the last twenty years. Proofs in these systems are witnesses realizing Hilbert's Nullstellensatz: a proof of unsatisfiability for a system of polynomial equations (representing a CNF formula, say) is an algebraic circuit witnessing that 1 is in the ideal generated by the given polynomials.

A survey talk by Shpilka was devoted to the recent Ideal Proof Systems significantly deviating from the Cook-Reckhow paradigm. Tzameret spoke of prominent proof systems naturally combining logic-based and algebraic reasoning; this area has quite a number of concrete interesting open problems. Finally, Lauria presented lower bounds for Graph Coloring for the Polynomial Calculus proof system, which formalizes Gröbner basis computations and is strong enough to capture successful algorithms used in practice.

Logic-based proof systems As we mentioned above, these are proof systems in the proper sense, i.e., those in which lines encode normal mathematical statements in a recognizable form.

Håstad spoke of his recent breakthrough result on improved lower bounds for bounded-depth Frege proof systems. It required significant enhancements to the classical restriction method, and it is widely expected that new methods will find many further applications. Pudlák addressed in his talk the theory of disjoint NP-pairs from the perspective of proof complexity.

Most other talks in this category pertained to even weaker proof systems centered around the celebrated Resolution proof systems. Concrete lower bounds were represented in the talks by Berkholz (very strong trade-offs for resolution, with spectacular applications to finite variable logic) and by de Rezende (size lower bounds for regular resolution proofs of a prominent combinatorial principle). The theme of regular resolution was taken up by Urquhart who gave a lovely introduction to the area. Itsykson spoke of an important proof system, closely related to resolution, that reasons about OBDD-representations of Boolean functions. Beame's talk was of even more practical flavor—it was devoted to the task of verifying arithmetic circuits based on the resolution proof system.

Finally, the talks by Dantchev and Thapen explored another fascinating concept in proof complexity closely connected to interactive proofs: what does it mean for a propositional proof to be *approximately* correct?

Beyond proof complexity Several interesting talks given at the workshop belong to adjacent areas and can hardly be classified according to the above scheme.

The two areas where ties to proof complexity have been traditionally extremely strong are circuit complexity and communication complexity. In the second part of her long lecture, Pitassi gave an overview of spectacular recent developments in those areas exploiting the method of hardness escalation. She concluded with applications to proof complexity proper. This theme was continued in the talk by Robere in which the first strongly exponential lower bound for the monotone circuit size was discussed.

Sudan's survey talk was devoted to the captivating framework of communication amid uncertainty attempting to capture real-life practice when communicating agents are even unsure about the rules of the game itself or even about the language used for communication. Williams spoke of the task of multipoint arithmetic evaluation from the perspective of the so-called Strong Exponential Time Hypothesis. Beyersdorff gave an overview talk about various proof systems used for refuting *quantified* Boolean formulas.

Open problem session On Tuesday evening an "Open Problem Session" was held. The main goal of the activity was to give the participants an opportunity to address the audience in somewhat informal terms about a research problem or direction for which progress could constitute an important advance in the area. A call for five minute informal presentations was announced on Monday morning with the promise of holding the first twelve proposals in order of arrival. At the beginning of the session on Tuesday evening we had received seven proposals. At the end of the session, a new call for last minute proposals was made, and three additional research problems were presented. The diversity of the audience backgrounds was reflected in the variety of problems presented. These ranged areas from the relative complexity of Frege systems as compared to resolution-modulo-theories systems (contributed by Kolokolova), through the complexity of proof systems that model the operation of state-of-the-art SAT-solvers (contributed by Johannsen), to an important but not so well-known problem that asks for the complexity of the parity principle in dag-like Lovász-Schrijver proof system (contributed by Beame). As mentioned by Beame in his presentation, this last problem can be tracked back, in slightly different language, to a lecture delivered by Laszlo Lovász himself at an Oberwolfach Workshop in Complexity Theory in 1996 (see `http://oda.mfo.de/view/bsz/325094934/DEFAULT/5/` for the abstract of Lovász's lecture).

References

[1] 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, 2012.

[2] Boaz Barak, Jonathan A. Kelner, and David Steurer. Dictionary learning and tensor decomposition via the sum-of-squares method. In *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing*, STOC 2015, pages 143–151. ACM, 2015.

[3] Boaz Barak and David Steurer. Sum-of-squares proofs and the quest toward optimal algorithms. In *Proceedings of International Congress of Mathematicians (ICM)*, 2014.
[4] Stephen A. Cook and Robert Reckhow. The relative efficiency of propositional proof systems. *Journal of Symbolic Logic*, 44(1):36–50, March 1979.
[5] Jean B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM Journal on Optimization*, 11:796–817, 2001.
[6] Laszlo Lovász. *Large Networks and Graph Limits*. American Mathematical Society, 2012.
[7] Pablo A. Parrilo. *Structured Semidefinite Programs and Semialgebraic Geometry Methods in Robustness and Optimization*. PhD thesis, California Institute of Technology, 2000.
[8] Alexander Razborov. What is a flag algebra? *Notices of the AMS*, 60(1):1324–1327, 2013.

Acknowledgement: The MFO and the workshop organizers would like to thank the National Science Foundation for supporting the participation of junior researchers in the workshop by the grant DMS-1049268, "US Junior Oberwolfach Fellows".

Workshop: Proof Complexity and Beyond

Table of Contents

Abstracts

Selected Topics on Semialgebraic Proof Complexity

Albert Atserias

Semi-algebraic proof systems are designed to reason with polynomial inequalities over the reals. Their significance for proof and algorithmic complexity is two-fold. On one hand, the expressive power of polynomial inequalities is particularly well suited for stating and reasoning about combinatorial optimization problems; this includes elementary pigeonhole-based arguments, as well as more complex counting arguments such as those arising in the theory of hypercontractivity in discrete Fourier analysis. On the other hand, by elementary reductions to linear or semi-definite programs, semi-algebraic proof systems tend to have relatively tractable proof-search problems. This survey-like talk started by introducing the family of semi-algebraic proof systems that I called "Lovász-Schrijver proof systems" in recognition of their highly influential article [5]. Then I discussed the following aspects of it: (1) their most important proof complexity measures, including degree, rank, length and size, in the most traditional style of proof complexity, (2) their relationship to the linear and semi-definite programming hierarchies of Sherali-Adams [10] and Lasserre/Sums-of-Squares [4, 7, 1], (3) their ability to efficiently formalize some interesting counting arguments, including the pigeonhole principle [5, 3] and the small-set expansion property of the noisy hypercube as an application of hypercontractivity [1, 6], (4) the degree-size tradeoffs that apply to them [8], and, last but not least, (5) the strong limitation result of Grigoriev [2] and Schoenebeck [9] showing that, for certifying the unsatisfiability of sparse random systems of parity equations, linear rank or degree is required.

References

[1] 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, 2012.

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

[3] Dima Grigoriev, Edward A. Hirsch, Dmitrii V. Pasechnik. Complexity of semi-algebraic proofs. *Moscow Mathematical Journal*, 4(2):647–679, 2002.

[4] Jean B. Lasserre. Global optimization with polynomials and the problems of moments. *SIAM Journal on Optimization*, 11(3):296–317, 2001.

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

[6] Ryan O'Donnell and Yuan Zhou. Approximability and proof complexity. In *Proceedings of the Twenty-Fourth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1537–1556, 2013.

[7] Pablo A. Parrilo. *Structured Semidefinite Programs and Semialgebraic Geometry Methods in Robustness and Optimization*. PhD thesis.

[8] Toniann Pitassi and Nathan Segerlind. Exponential Lower Bounds and Integrality Gaps for Tree-like Lovász-Schirjver Procedures. *SIAM Journal on Computing*, 41(1):128–159, 2012.

[9] Grant Schoenebeck. Linear Level Lasserre Lower Bounds for Certain k-CSPs. In *49th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 593–602, 2008.
[10] 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(3):411–430, 1990.

Verifying Multipliers in Resolution

Paul Beame
(joint work with Vincent Liew)

Recent decades have seen remarkable advances in our ability to verify hardware and software, beginning in the 1980s using OBDDs and more recently using CDCL SAT solvers. Nonetheless, there is an important area of formal verification where roadblocks that were identified in the 1980s still remain: any verification problem in hardware or software that involves the detailed properties of nonlinear arithmetic. Natural examples of such verification problems in software include computations involving hashing or cryptographic constructions. At the highest level of abstraction, nonlinear arithmetic over the integers is undecidable, but the focus of these verification problems is on the decidable case of integers of bounded size.

In particular, a notorious open problem is that of verifying properties of integer multipliers in a way that both is general purpose and avoids exponential scaling in the bit-width. Bryant [8] showed that this is impossible using OBDDs since they require exponential size in the bit-width just to represent the middle bit of the output of a multiplier. With the flexibility of CNF formulas, efficient representation of multipliers is not a problem but, even with the advent of greatly improved SAT solvers, there has been no advance in verifying multipliers beyond exponential scaling. The problem of verifying nonlinear arithmetic, and multipliers in particular, has recently been identified as one of the key gaps in our current verification methods [4, 5, 7, 10].

Integer multipliers must satisfy natural ring identities of commutativity, distributivity, and associativity which ensure their correctness. Biere, in the text accompanying benchmarks on these ring identities submitted to the 2016 SAT Competition [6], writes that when given as CNF formulas, no known technique is capable of handling bit-width larger than 16 for commutativity or associativity of multiplication or bit-width 12 for distributivity of multiplication over addition. Since efficient verifications by CDCL SAT solvers requires the existence of short resolution proofs [1], Biere conjectured [7] that there is a fundamental proof-theoretic obstacle to succeeding on such problems; namely, verifying ring identities for multiplication circuits, such as commutativity, requires resolution proofs that are exponential in the bit-width n.

We show that such a roadblock to efficient verification of nonlinear arithmetic does not exist by giving a general method for finding short resolution proofs for verifying *any* degree 2 identity for Boolean circuits consisting of bit-vector adders

and multipliers. This method is based on reducing the multiplier verification to finding a resolution refutation of one of a number of narrow *critical strips*. We apply this method to a number of the most widely used multiplier circuits, yielding $n^{O(1)}$ size proofs for array, diagonal, and Booth multipliers, and $n^{O(\log n)}$ size proofs for Wallace tree multipliers.

These resolution proofs are of a special simple form: they are *regular* resolution proofs, which have been identified in theoretical models of CDCL SAT solvers as one of the simplest kinds of proof that those solvers naturally express [9].

(Based on a paper presented at the 2017 Computer-Aided Verification conference [2], with full version in [3].)

References

[1] Paul Beame, Henry Kautz, and Ashish Sabharwal. Towards understanding and harnessing the potential of clause learning. *Journal of Artificial Intelligence Research*, 22:319–351, 2004.

[2] Paul Beame and Vincent Liew. Towards verifying nonlinear integer arithmetic. In *Computer Aided Verification - 29th International Conference, CAV 2017, Heidelberg, Germany, July 24-28, 2017, Proceedings, Part II*, pages 238–258, 2017.

[3] Paul Beame and Vincent Liew. Towards verifying nonlinear integer arithmetic. *CoRR*, abs/1705.04302, 2017.

[4] Armin Biere. Challenges in bit-precise reasoning. In *Formal Methods in Computer-Aided Design, FMCAD 2014*, page 3, Lausanne, Switzerland, October 2014.

[5] Armin Biere. Where does SAT not work? In *BIRS Workshop on Theory and Applications of Applied SAT Solving*, January 2014. http://www.birs.ca/events/2014/5-day-workshops/14w5101/videos/watch/201401201634-Biere.html.

[6] Armin Biere. Collection of Combinational Arithmetic Miters Submitted to the SAT Competition 2016. In Tomáš Balyo, Marijn Heule, and Matti Järvisalo, editors, *Proc. of SAT Competition 2016 – Solver and Benchmark Descriptions*, volume B-2016-1 of *Department of Computer Science Series of Publications B*, pages 65–66. University of Helsinki, 2016.

[7] Armin Biere. Weaknesses of CDCL solvers. In *Fields Institute Workshop on Theoretical Foundations of SAT Solving*, August 2016. http://www.fields.utoronto.ca/talks/weaknesses-cdcl-solvers.

[8] Randal E. Bryant. On the complexity of vlsi implementations and graph representations of boolean functions with application to integer multiplication. *IEEE Trans. Comput.*, 40(2):205–213, 1991.

[9] Samuel R. Buss, Jan Hoffmann, and Jan Johannsen. Resolution trees with lemmas: Resolution refinements that characterize DLL algorithms with clause learning. *Logical Methods in Computer Science*, 4(4:13):1–28, 2008.

[10] Priyank Kalla. Formal verification of arithmetic datapaths using algebraic geometry and symbolic computation. In *Proceedings, Formal Methods in Computer-Aided Design, FMCAD*, page 2, Austin, TX, September 2015.

Resolution Trade-Offs for XOR-Formulas with Applications to Finite Variable Logics and the Weisfeiler-Leman Algorithm

Christoph Berkholz
(joint work with Jakob Nordström)

We establish strong trade-offs between the width and the depth of resolution refutations of CNF formulas that encode unsatisfiable XOR-formulas. The main motivation for this are applications in finite model theory and the proofs combine techniques from both worlds. The trade-offs in the resolution calculus help us to establish near-optimal lower bounds on the quantifier depth in finite variable logics, which in turn imply strong lower bounds on the number of refinement steps in the k-dimensional Weisfeiler-Leman algorithm.

Using systems of linear equations over $\mathbb{Z}_2$ (also called XOR-formulas) as a source of hardness has a long tradition in proof complexity (e. g. Tseitin Tautologies, random 3-XOR) as well as in finite model theory (e. g. the Cai-Fürer-Immerman construction and its variants). The first contribution of our work is to make a precise connection between complexity measures on XOR-formulas from both worlds: We show that the *width* and the *depth* needed to proof the unsatisfiability of the CNF-encoding of an XOR-formula in resolution corresponds to the *number of variables* and the *quantifier rank* need to distinguish a pair of relational structures based on the same XOR-formula in first-order logic and its extension with counting quantifiers.

Our main goal is to prove trade-offs between these two measures. In terms of resolution our main result states that there is an n-variable XOR-formula that can be refuted in width k, but where every width-k refutation requires depth $n^{\Omega(k/\log k)}$. This nearly matches the trivial $O(n^k)$ upper bound. By the above correspondence our result implies an $n^{\Omega(k/\log k)}$ lower bound on the quantifier rank needed to distinguish two n-element relational structures in k-variable fragments of first order logic—before the best lower bound was only linear in n [3].

To obtain these results we make use of two unrelated techniques from proof complexity and finite model theory. One key component in our proof is the hardness condensation technique introduced by Razborov [5], who established similar width/depth trade-offs for CNF formulas that do not encode XOR formulas. This technique can be applied to prove a certain type of *supercritical* trade-off results that have the property that the restriction of one parameter (the width) causes the other parameter (the depth) to grow beyond its worst-case. Our width/depth trade-off is also of that shape, as there is always a resolution refutation of depth at most n, but restricting the width to k causes the depth to be at least $n^{\Omega(k/\log k)}$.

We apply this condensation technique to a modified version of a construction by Immerman [4], which was used to prove a $\Omega(2^{\sqrt{\log n}})$ lower bound on the quantifier depth of first-order counting logic.

After introducing the problem at hand from the proof complexity and the finite model theory side, the talk focuses on how the combination of both worlds lead to

the new trade-off result. The talk is based on a joint work with Jakob Nordström [1] (full version [2]), which appeared at LICS 2016.

References

[1] Christoph Berkholz and Jakob Nordström. Near-optimal lower bounds on quantifier depth and Weisfeiler-Leman refinement steps. In *Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science (LICS '16)*, pages 267–276, July 2016.

[2] Christoph Berkholz and Jakob Nordström. Near-optimal lower bounds on quantifier depth and Weisfeiler-Leman refinement steps. Technical Report TR16-135, Electronic Colloquium on Computational Complexity (ECCC), August 2016. Preliminary version in *LICS '16*.

[3] Martin Fürer. Weisfeiler–Lehman refinement requires at least a linear number of iterations. In *Proceedings of the 28th International Colloquium on Automata, Languages, and Programming (ICALP '01)*, volume 2076 of *Lecture Notes in Computer Science*, pages 322–333. Springer, July 2001.

[4] Neil Immerman. Number of quantifiers is better than number of tape cells. *Journal of Computer and System Sciences*, 22(3):384–406, June 1981.

[5] Alexander A. Razborov. A new kind of tradeoffs in propositional proof complexity. *Journal of the ACM*, 63:16:1–16:14, April 2016.

Proof Complexity of Quantified Boolean Formulas

Olaf Beyersdorff

(joint work with Joshua Blinkhorn and Luke Hinde)

Quantified Boolean formulas (QBF) are a natural extension of SAT problems, in which variables can be quantified by either universal or existential Boolean quantifiers, as opposed to the solely existential quantifiers implicit in a SAT problem. Determining whether such QBFs are true is the canonical PSPACE-complete problem, and is the subject of much practical and theoretical study.

Many different proof systems for QBFs have been proposed, in most cases building on a base propositional proof system, but with additional rules for dealing with universal quantifiers. One common such method is to add a $\forall$-reduction rule, which can be applied to any $\mathcal{C}$-Frege system [2], such as Resolution (resulting in QU-Res [12, 14]), as well as to systems such as Cutting Planes (CP) [4, 10] and Polynomial Calculus (PCR) [1, 9].

On propositional formulas, any QBF proof system reduces to a propositional proof system, with the corresponding lower bounds. Strategy extraction [2, 13] allows us to lift circuit lower bounds to QBF proof complexity lower bounds by computing witnessing functions, or winning strategies, for the universal variables from a refutation. For strong systems such as Frege+$\forall$red, propositional hardness and strategy extraction suffice to prove all superpolynomial lower bounds [6], however this is not the case for weaker systems such as QBF Resolution systems [5]. For these weaker systems, some additional lower bound techniques do exist for formulas with a particular structure (e.g. feasible interpolation [3, 15]), but there are relatively few general techniques.

We present such a technique for any proof system P+$\forall$red, which can be applied to any QBF. This lower bound relies on two semantic properties: the *cost* of a

QBF, which can be interpreted as the minimum number of different responses a winning strategy for the universal variables may produce, and the *capacity* of a proof, interpreted as the maximum number of different universal assignments which are obtained in strategy extraction from a line of the proof. Defining these formally, we obtain the *Size-Cost-Capacity Theorem*, that $|\pi| \geq \frac{\text{cost}(\Phi)}{\text{capacity}(\pi)}$ for any proof π of a QBF Φ.

Given a QBF proof system $\mathsf{P}+\forall\mathsf{red}$, we therefore seek upper bounds on the capacity of proofs in $\mathsf{P}+\forall\mathsf{red}$. In the case of $\mathsf{QU\text{-}Res}$ and $\mathsf{CP}+\forall\mathsf{red}$, we prove that in fact the capacity is equal to 1 for all proofs. For $\mathsf{PCR}+\forall\mathsf{red}$, capacity is not constant, but nevertheless, it holds that $\text{capacity}(\pi) \leq |\pi|$, and so in all three systems, Size-Cost-Capacity implies that QBFs with superpolynomial cost require proofs of superpolynomial size.

To exemplify this technique, we define the *equality formulas*. These natural QBFs are simple to construct, but there is a unique response for the universal player to any assignment, so it is clear the formulas have exponential cost. As a result of the capacity bounds, we therefore immediately obtain exponential proof size lower bounds for the equality formulas in $\mathsf{QU\text{-}Res}$, $\mathsf{CP}+\forall\mathsf{red}$ and $\mathsf{PCR}+\forall\mathsf{red}$.

As the major application of this new technique, we prove exponential lower bounds with high probability for a class $Q(n, m, c)$ of randomly generated QBFs, the first such lower bound on random QBFs. These random QBFs are essentially a disjunction of randomly generated (1,2)-QCNFs [8], regularly used as a model for random QBFs [7], but with a rearranged quantifier prefix. By choosing the number of clauses and variables carefully, we can apply results on the truth of random (1,2)-QCNFs [11], and the unsatisfiability of random 2-SAT problems [16]. By combining these results, we are able to obtain an exponential cost lower bound on $Q(n, m, c)$ with high probability.

References

[1] M. Alekhnovich, E. Ben-Sasson, A.A. Razborov, and A. Wigderson. Space complexity in propositional calculus. SIAM Journal on Computing 31(4), 1184–1211 (2002)

[2] O. Beyersdorff, I. Bonacina, and L. Chew. Lower bounds. From circuits to QBF proof systems. In: ACM Conference on Innovations in Theoretical Computer Science (ITCS). pp. 249–260 (2016)

[3] O. Beyersdorff, L. Chew, M. Mahajan, and A. Shukla. Feasible interpolation for QBF resolution calculi. In: International Colloquium on Automata, Languages, and Programming (ICALP). pp. 180–192 (2015)

[4] O. Beyersdorff, L. Chew, M. Mahajan, and A. Shukla. Understanding Cutting Planes for QBFs. In: 36th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2016). Leibniz International Proceedings in Informatics (LIPIcs), vol. 65, pp. 40:1–40:15 (2016)

[5] O. Beyersdorff, L. Hinde, and J. Pich. Reasons for hardness in QBF proof systems. Electronic Colloquium on Computational Complexity (ECCC) 24, 44 (2017)

[6] O. Beyersdorff and J. Pich. Understanding gentzen and frege systems for QBF. In: Symposium on Logic in Computer Science (LICS). pp. 146–155 (2016)

[7] R. Brummayer, F. Lonsing, and A. Biere. Automated testing and debugging of SAT and QBF solvers. In: Theory and Applications of Satisfiability Testing - (SAT) 2010. pp. 44–57 (2010)

[8] H. Chen and Y. Interian. A model for generating random quantified boolean formulas. In: International Joint Conference on Artificial Intelligence. pp. 66–71 (2005)
[9] M. Clegg, J. Edmonds, and R. Impagliazzo. Using the Groebner basis algorithm to find proofs of unsatisfiability. In: Proc. 28th ACM Symposium on Theory of Computing. pp. 174–183 (1996)
[10] W. Cook, C.R. Coullard, and G. Turán. On the complexity of cutting-plane proofs. Discrete Applied Mathematics 18(1), 25–38 (1987)
[11] N. Creignou, H. Daudé, U. Egly, and R. Rossignol. Exact location of the phase transition for random (1, 2)-QSAT. RAIRO - Theor. Inf. and Applic. 49(1), 23–45 (2015)
[12] A.V. Gelder. Contributions to the theory of practical quantified boolean formula solving. In: International Conference on Principles and Practice of Constraint Programming (CP). pp. 647–663 (2012)
[13] A. Goultiaeva, A.V. Gelder, and F. Bacchus. A uniform approach for generating proofs and strategies for both true and false QBF formulas. In: International Joint Conference on Artificial Intelligence IJCAI. pp. 546–553 (2011)
[14] H. Kleine Büning, M. Karpinski, and A. Flögel. Resolution for quantified boolean formulas. Information and Computation 117(1), 12–18 (1995)
[15] J. Krajícek. Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic. Journal of Symbolic Logic 62(2), 457–486 (1997)
[16] W.F. de la Vega. Random 2-SAT: results and problems. Theoretical Computer Science 265(1-2), 131–146 (2001)

Randomised Approximate Proofs

Stefan Dantchev
(joint work with Joshua Blinkhorn and Luke Hinde)

Recently, the notion of random resolution distributions has been proposed by Pudlák and Thapen in [3] (see also [1] for motivation), and some basic results have been proven. This has been the first attempt to introduce randomness to propositional proofs in the context of proof complexity. We suggest an alternative definition of **randomised approximate resolution** (ra-resolution) **refutations**, which is less restrictive, and, in our opinion, looks more natural. In particular, there is straightforward translation of a randomised algorithm that solves the search problem for an unsatisfiable set of clauses into a ra-resolution refutation. (The search problem is: given an assignment of the variables, find a clause falsified by it.)

As a matter of fact, our motivation comes entirely from the question if a randomised algorithm for the search problem can be turned into any kind of meaningful refutation, while Pudlák and Thapen's main motivation comes from questions concerning various separations of theories within Bounded Arithmetic. It turns out that both systems suffer from a nasty drawback, namely neither is a propositional proof system in the sense of Cook and Reckhow [2].

Our definition of a ra-resolution refutation is as follows.

Given a propositional contradiction F in cnf and a probability $0 \leq \varepsilon < 1$, an **ε-approximate resolution** (ε-ra resolution) **refutation** of F is a probability distribution $\mathcal{D}$ over pairs (R, Π), where R is a cnf over the variables of F and Π

is a resolution refutation of $F \wedge R$, and such that for every assignment x of the variables of F

$$\mathrm{Prob}_{(\mathrm{R},\Pi)\sim\mathcal{D}}\,[\text{the cannonical path of x ends in a clause of R in } \Pi] \leq \varepsilon$$

holds.

We prove some very general basic properties of these refutations. We also provide a number of of upper and lower bounds that give various separations between ra-resolution and resolution.

References

[1] Samuel R. Buss, Leszek Aleksander Kolodziejczyk, and Neil Thapen. Fragments of approximate counting. *J. Symb. Log.*, 79(2):496–525, 2014.

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

[3] Pavel Pudlák and Neil Thapen. Random resolution refutations. *Electronic Colloquium on Computational Complexity (ECCC)*, 23:175, 2016.

The Symmetry Gap in Combinatorial Optimization

Anuj Dawar

(joint work with Matthew Anderson, Bjarki Holm and Pengming Wang)

Fixed-point Logic with Counting (FPC), is a natural and powerful fragment of the class of polynomial-time decidable properties that is much studied in the context of finite model theory. See [3] for a short introduction. Though originally defined in logical terms, it has a circuit characterization as the class of properties decided by families of polynomial-time uniform *symmetric circuits* [1]. It is capable of expressing many polynomial-time algorithms but we can prove that some problems such as XOR-Sat are not in FPC. The method of proof is based on showing that every property in FPC is closed under $\equiv^k$, the k-dimensional Weisfeiler-Leman equivalence for some k. A direct proof of this, based on the circuit characterization, can be found in [4]. For any class of finite structures $\mathcal{C}$, we define its *counting width* $\nu_{\mathcal{C}} : \mathbb{N} \to \mathbb{N}$ to be the function that takes n to the least value of k such that the collection of structures in $\mathcal{C}$ with at most n elements is closed under $\equiv^k$. Then, any class in FPC has counting width bounded by a constant, while XOR-Sat has counting width $\Omega(n)$.

We proved in [2] that the ellipsoid method can be implemented in FPC. To be precise, we show that the problem of determining the feasibility of an explicitly given linear program (suitably represented as a class of structures) is in FPC. More generally, we show that the optimization problem for linear programs can be reduced to the separation problem: if the separation problem is in FPC, then so is the optimization problem. By constructing a suitable FPC separation oracle for the Edmonds matching polytope in graphs, we are able to show that the problem of determining the size of the maximum matching in a graph is FPC. More recently, we have extended the technique to weak optimization and weak separation in semidefinite programs and obtained a dichotomy in the context of finite valued

constraint satisfaction problems (a class of problems that generalizes the class of Max-CSP problems). We show that for any such problem, its counting width is either bounded by a constant or is $\Omega(n)$. By showing that a degree-d Lasserre sums-of-squares relaxation of such a problem is definable in FPC, we obtain another dichotomy: any finite valued CSP is either solvable by its basic linear programming relaxation or cannot be solved exactly by a sub-linear degree Lasserre lift of that relaxation [5, 6].

References

[1] Matthew Anderson and Anuj Dawar On symmetric circuits and fixed-point logics. *Theory Comput. Syst. 60* (2017), 521–551.

[2] Matthew Anderson, Anuj Dawar, and Bjarki Holm Solving linear programs without breaking abstractions. *J. ACM 62* (2015), 48:1–48:26.

[3] Anuj Dawar The nature and power of fixed-point logic with counting. *ACM SIGLOG News* (2015), 8–21.

[4] Anuj Dawar On symmetric and choiceless computation. In *Topics in Theoretical Computer Science* (2015), pp. 23–29.

[5] Anuj Dawar and Pengming Wang A definability dichotomy for finite valued CSPs. In *24th EACSL Annual Conference on Computer Science Logic, CSL 2015* (2015), pp. 60–77.

[6] Anuj Dawar and Pengming Wang Definability of semidefinite programming and Lasserre lower bounds for CSPs. In *Proc. of the 32nd IEEE Symp. on Logic in Computer Science (LICS).* (2017).

k-Clique is Hard on Average for Regular Resolution

Susanna F. de Rezende

(joint work with Albert Atserias, Ilario Bonacina, Massimo Lauria, Jakob Nordström and Alexander Razborov)

The problem of deciding whether a graph on n vertices has a k-clique is a fundamental problem in graph theory. A trivial enumeration algorithm can determine this in time $O(n^k)$ and unless the Exponential Time Hypothesis (ETH) is false there is no $f(k) \cdot n^{o(k)}$-time algorithm for solving this problem[5].

A natural question is whether we can prove an unconditional lower bounds for a restricted class of algorithms. For example, can we show that resolution requires size $n^{\Omega(k)}$, or even $n^{\Omega(g(k))}$ for some increasing function g, to prove the absence of k-cliques in a graph? This question was mentioned in [4] and remains open.

We make progress in this direction and show that, to certify the absence of k-cliques, regular resolution almost surely requires size $n^{\Omega(k)}$ for graphs sampled at random from the appropriate Erdős–Rényi model.

The first result in this direction was by Beame, Impagliazzo and Sabharwal [1]. They show that resolution requires size $2^{\Omega(k)}$ to establish that a graph does not contain a k-clique. Their proof uses the width method of Ben-Sasson and Wigderson [2], which cannot yield an $n^{\Omega(k)}$ lower bound since there are resolution proofs of width $O(k)$.

Beyersdorff, Galesi and Lauria [3] show that tree-like resolution requires size $n^{\Omega(k)}$ to prove the absence of k-cliques in complete $(k-1)$-partite graphs and in Erdős–Rényi graphs. They also show that in order to extend this result to regular resolution we cannot use $(k-1)$-colorable graphs since for these graphs there are regular proofs of size $O(2^k k^2 n^2)$.

The results mentioned so far all use the more natural unary encoding of the statement that a graph contains a k-clique. For the binary encoding, a lower bounds of $n^{\Omega(k)}$ for k up to $\log n$ can be obtained by careful reading of [6].

References

[1] Paul Beame, Russell Impagliazzo, and Ashish Sabharwal. The resolution complexity of independent sets and vertex covers in random graphs. *Computational Complexity*, 16(3):245–297, October 2007. Preliminary version in *CCC '01*.

[2] 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*.

[3] Olaf Beyersdorff, Nicola Galesi, and Massimo Lauria. Parameterized complexity of dpll search procedures. *ACM Transactions on Computational Logic (TOCL)*, 14(3):20, 2013. Preliminary version in *SAT '11*.

[4] Olaf Beyersdorff, Nicola Galesi, Massimo Lauria, and Alexander A. Razborov. Parameterized bounded-depth Frege is not optimal. *ACM Transactions on Computation Theory*, 4:7:1–7:16, September 2012. Preliminary version in *ICALP '11*.

[5] Jianer Chen, Xiuzhen Huang, Iyad A. Kanj, and Ge Xia. Linear FPT reductions and computational lower bounds. In *Proc. 36th STOC*, pages 212–221, New York, 2004.

[6] Massimo Lauria, Pavel Pudlák, Vojtěch Rödl, and Neil Thapen. The complexity of proving that a graph is Ramsey. In *Proceedings of the 40th International Colloquium on Automata, Languages and Programming (ICALP '13)*, volume 7965 of *Lecture Notes in Computer Science*, pages 684–695. Springer, July 2013.

Random $O(\log n)$-CNF formulas Are Hard for Cutting Planes

Noah Fleming

(joint work with Denis Pankratov, Toniann Pitassi and Robert Robere)

Random k-SAT formulas form one of the most important testbeds of hard examples for algorithms in the AI and SAT communities. Furthermore, the conjectured hardness of certifying the unsatisfiability of random k-SAT instances has been connected to many areas in TCS. In 1988, Chvaátal and Szeméredi [1] proved that for any $k \geq 3$, random k-CNF formulas require an exponential number of lines to refute in Resolution. This result was further improved by several authors, and extended to k-DNF Resolution and Polynomial Calculus. Since then, it has been an open problem to prove similar results for other proof systems.

In this work [2], we make progress towards resolving this question for Cutting Planes. We show that Cutting Planes refutations of random $O(\log n)$-CNF formulas require exponentially many lines. This was proved independently by Pudlák and Hrubeš [3].

In 1997, Pudlák [6] obtained the first exponential lower bounds on the length of Cutting Planes refutations of split formulas (formulas of a very specific type

which are essentially the conjunction of two contradictory statements). This was achieved by showing that any Cutting Planes refutation of a split formula implies a real monotone circuit of the same size for separating an associated set of minterms and maxterms. Lower bounds were then obtained by proving lower bounds on the size of monotone real circuits for this separating set of minterms and maxterms. To obtain our lower bound, we generalize this, showing that a Cutting Planes refutation of *any* unsatisfiable formula implies a real monotone circuit of the same size for separating a set of minterms and maxterms. Furthermore, we characterize exactly when this technique can be applied by proving an if and only if direction for a stronger proof system, one that simulates Cutting Planes. That is, there exists a small real monotone circuit for separating this set of minterms and maxterms if and only if there exists a short refutation in this proof system. In order to prove this equivalence, we show that refutations in this proof system are equivalent to PLS games (a DAG-like model of communication introduced by Razborov [7]) and then make use of an equivalence between PLS games and real monotone circuits proved by Pudlák and Hrubeš [4]. The final task is to obtain a lower bound on the set of minterms and maxterms obtained via this equivalence for random $O(\log n)$-CNF formulas. To do this, we appeal to the method of symmetric approximations [5].

The aim of this talk is to give a high-level exposition of how this lower bound can be obtained, with a particular focus on proving the the equivalence between real monotone circuits and refutations. Furthermore, I will outline why this method cannot be used to solve certain other long-standing open problems for Cutting Planes, such as obtaining lower bounds on the Tseitin formulas, and the difficulties of using this approach to prove Cutting Planes lower bounds on random constant-width CNF formulas.

References

[1] Vasek Chvátal and Endre Szemerédi. Many hard examples for resolution. *J. ACM*, 35(4):759–768, 1988.

[2] Noah Fleming, Denis Pankratov, Toniann Pitassi, and Robert Robere. Random cnfs are hard for cutting planes. *Electronic Colloquium on Computational Complexity (ECCC)*, 24:45, 2017.

[3] Pavel Hrubes and Pavel Pudlák. A note on monotone real circuits. *Electronic Colloquium on Computational Complexity (ECCC)*, 24:48, 2017.

[4] Pavel Hrubeš and Pavel Pudlák. A note on monotone real circuits. *ECCC TR17-048*, 2017.

[5] Stasys Jukna. *Boolean Function Complexity - Advances and Frontiers*, volume 27 of *Algorithms and combinatorics*. Springer, 2012.

[6] Pavel Pudlák. Lower bounds for resolution and cutting plane proofs and monotone computations. *J. Symb. Log.*, 62(3):981–998, 1997.

[7] Alexander A. Razborov. Unprovability of lower bounds on circuit size in certain fragments of bounded arithmetic.

Sum-of-Squares Certificates of Maxima of Polynomials over the Sphere

Venkatesan Guruswami
(joint work with Vijay Bhattiprolu, Mrinalkanti Ghosh, Euiwoong Lee, and Madhur Tulsiani)

We consider the following basic problem: given an n-variate degree-d homogeneous polynomial f with real coefficients, compute a unit vector $x \in \mathbb{R}^n$ that maximizes $|f(x)|$. Besides its fundamental nature, this problem arises in diverse contexts ranging from tensor and operator norms to graph expansion to quantum information theory. The homogeneous degree 2 case is efficiently solvable as it corresponds to computing the spectral norm of an associated matrix, but the higher degree case is NP-hard.

In this work, we give approximation algorithms for this problem. Our algorithms leverage the tractability of the degree-2 case, and output the best solution among a carefully constructed set of quadratic polynomials. They offer a trade-off between the approximation ratio and running time: in $n^{O(q)}$ time, we get an approximation within factor $O_d((n/q)^{d/2-1})$ for arbitrary polynomials, $O_d((n/q)^{d/4-1/2})$ for polynomials with non-negative coefficients, and $O_d(\sqrt{m/q})$ for sparse polynomials with m monomials. The approximation guarantees are with respect to the optimum of the level-q sum-of-squares (SoS) SDP relaxation of the problem (though our algorithms do not rely on actually solving the SDP). We give approximation algorithms for this problem that offer a trade-off between the approximation ratio and running time: in $n^{O(q)}$ time, we get an approximation within factor $O_d((n/q)^{d/2-1})$ for arbitrary polynomials, $O_d((n/q)^{d/4-1/2})$ for polynomials with non-negative coefficients, and $O_d(\sqrt{m/q})$ for sparse polynomials with m monomials. The approximation guarantees are with respect to the optimum of the level-q sum-of-squares (SoS) SDP relaxation of the problem (though our algorithms do not rely on actually solving the SDP). Known polynomial time algorithms for this problem rely on "decoupling lemmas." Such tools are not capable of offering a trade-off like our results as they blow up the number of variables by a factor equal to the degree. We develop new decoupling tools that are more efficient in the number of variables at the expense of less structure in the output polynomials. This enables us to harness the benefits of higher level SoS relaxations. Our decoupling methods also work with "folded polynomials," which are polynomials with polynomials as coefficients. This allows us to exploit easy substructures (such as quadratics) by considering them as coefficients in our algorithms.

We complement our algorithmic results with some polynomially large integrality gaps for d-levels of the SoS relaxation. For general polynomials this follows from known results for *random* polynomials, which yield a gap of $\Omega_d(n^{d/4-1/2})$ [2] (this was extended to higher levels in [3]). For polynomials with non-negative coefficients, we prove an $\tilde{\Omega}(n^{1/12})$ gap for the degree 4 case, based on a novel distribution of 4-uniform hypergraphs. We establish an $n^{\Omega(d)}$ gap for general degree d, albeit for a slightly weaker (but still very natural) relaxation. Toward this, we

give a method to lift a level-4 solution matrix M to a higher level solution, under a mild technical condition on M.

References

[1] Vijay V. S. P. Bhattiprolu, Mrinal Kanti Ghosh, Venkatesan Guruswami, Euiwoong Lee, and Madhur Tulsiani. Weak Decoupling, Polynomial Folds, and Approximate Optimization over the Sphere. *Proceedings of the IEEE Symposium on Foundations of Computer Science (FOCS)*, 2017. Also ECCC Technical Report TR16-185, `https://eccc.weizmann.ac.il/report/2016/185/`.

[2] Vijay V. S. P. Bhattiprolu, Venkatesan Guruswami, Euiwoong Lee. Sum-of-Squares Certificates for Maxima of Random Tensors on the Sphere. *APPROX-RANDOM 2017*: 31:1-31:20, 2017.

[3] Samuel B. Hopkins, Pravesh K. Kothari, Aaron Potechin, Prasad Raghavendra, Tselil Schramm and David Steurer. The Power of Sum-of-Squares for Detecting Hidden Structures. *Proceedings of the IEEE Symposium on Foundations of Computer Science (FOCS)*, 2017.

On Small-Depth Frege Proofs for Tseitin for Grids

Johan Håstad

We study Frege proofs where each formula appearing in the proof is of depth at most d where this crucial parameter ranges from constant to almost $\log n$ where n is the number of variables in our formula. We are interested in refutations of any contradictory formula but the Pigeon-Hole-Principle (PHP) and the Tseitin formulas [9] for graphs play a central role. The latter says[1] that in a graph with an odd number of vertices we cannot have a labeling of the edges by bits such that each vertex is adjacent to an odd number of edges labeled one.

The first strong result for general depth d was obtained by Ajtai [1] showing that PHP cannot be proved in constant depth and polynomial size. Ajtai did not work out an explicit lower bound for the depth of polynomial size proofs but in a later reformulation by Bellantoni et al. [2], a lower bound of $\Omega(\log^* n)$ was given. This was later strengthened [5, 6] to obtain $\Omega(\log\log n)$ lower bounds for PHP. Similar bounds were later proved by Urquhart and Fu [10] and Ben-Sasson [3] for Tseitin formulas for the complete graph and for constant-degree expander graphs, respectively.

On the positive side Buss [4] proved that there are polynomial size $O(\log n)$-depth proofs for the PHP and this can be modified to handle the Tseitin formulas.

The exponential gap between the depth bounds $\log\log n$ and $\log n$ was recently partly closed by Pitassi et al. [7] obtaining a $\Omega(\sqrt{\log n})$ lower bound for Tseitin formulas on a certain 3-regular expander graph. It is curious to note the the size lower bounds of [7] when considering depth d is exponential in $\Omega((\log n)^2/d^2)$ and thus only weakly superpolynomial. For small values of d, this bound is weaker then the bounds of the form $exp(n^{c^{-d}})$ obtained in previous papers but extended the range of d for which it is superpolynomial.

[1] This is the special case where all charges are one.

In the current work we study the Tseitin formulas for the 2-dimensional grid and almost close the gap obtaining size lower bounds $exp(\Omega(n^{1/58(d+1)}))$ for depth d proofs and hence the depth lower bound $\Omega(\log n/\log\log n)$ for polynomial size proofs. Our proofs follow the same paradigm as earlier proofs and in particular the key component is defining a set of restrictions that give values to most variables. To be more precis we study projections (first formalized in [8]) that either assign constants to variables or identifies a variable with either a new variable or the negation of such a variable. A key property not used in restrictions from the 1980'ies is that many old variables are identified with the same new variable.

These restrictions are probabilistic and quite involved but manage to fulfill the two main properties needed. Firstly, with high probability they reduce a Tseitin formula of the grid to a Tseitin formula on a smaller grid. Secondly, it is possible to prove a switching lemma which essentially says that, with high probability, it is possible to reduce the depth of any occurring formula by one. Applying d consecutive restrictions to a supposed small formula consisting of formulas of depth d gives the desired contradiction.

References

[1] Miklos Ajtai. The complexity of the pigeonhole principle. *Combinatorica*, 14(4):417–433, 1994.

[2] Stephen Bellantoni, Toniann Pitassi, and Alasdair Urquhart Approximation and small-depth frege proofs. *SIAM J. Comput.*, 21(6):1161–1179, 1992.

[3] Eli Ben-Sasson. Hard examples for the bounded depth frege proof system. *Computational Complexity*, 11(3-4):109–136, 2002.

[4] Samuel R. Buss. Polynomial size proofs of the propositional pigeonhole principle. *Journal of Symbolic Logic*, 52:916–927, 1987.

[5] Jan Krajícek, Pavel Pudlák, and Alan R. Woods. An exponential lower bound to the size of bounded depth frege proofs of the pigeonhole principle. *Random Struct. Algorithms*, 7(1):15–40, 1995.

[6] Toniann Pitassi, Paul Beame, and Russell Impagliazzo. Exponential lower bounds for the pigeonhole principle. *Computational Complexity*, 3:97–140, 1993.

[7] Toniann Pitassi, Benjamin Rossman, Rocco A. Servedio, and Li-Yang Tan Poly-logarithmic frege depth lower bounds via an expander switching lemma. In *Proceedings of the Forty-eighth Annual ACM Symposium on Theory of Computing*, STOC '16, pages 644–657, New York, NY, USA, 2016. ACM.

[8] Benjamin Rossman, Rocco A. Servedio, and Li-Yang Tan An average-case depth hierarchy theorem for boolean circuits. In *IEEE 56th Annual Symposium on Foundations of Computer Science, FOCS 2015, Berkeley, CA, USA, 17-20 October, 2015*, pages 1030–1048, 2015.

[9] Grigorii S. Tseitin. On the complexity of derivation in the proposistional calculus. In A. O. Slisenko, editor, *Studies in constructive mathematics and mathematical logic, Part II*, 1968.

[10] Alasdair Urquhart and Xudong Fu. Simplified lower bounds for propositional proofs. *Notre Dame Journal of Formal Logic*, 37(4):523–544, 1996.

Some Separations for OBDD-Based Proof Systems

Dmitry Itsykson
(joint work with Sam Buss, Alexander Knop and Dmitry Sokolov)

We consider proof systems that operate with branching programs (BP): such proof systems represent clauses of the formula as branching programs and derive constant false BP by means of inference rules. We mainly consider very restrictive kind of branching programs — k-OBDDs that on every path from the source to a sink read variables in the fixed order for at most k passes. We consider three inference rules:

(1) join rule that allows to derive the conjunction of two k-OBDDs in the same order;
(2) weakening rule that allows to derive any k-OBDD that is semantically implied by the original one, and
(3) reordering rule that allows to derive a representation of k-OBDD in the another order.

We give an example of CNF formulas that have superpolynomial Resolution complexity but have 1-OBDD(join) proofs of polynomial size. An example of formulas that are hard for k-OBDD(join) but easy for Resolution was presented in [2, 6], hence k-OBDD(join) is incomparable with Resolution. We prove that Tseitin formulas and PHP are hard for k-OBDD(join, reordering) and also show that k-OBDD(join, reordering) is strictly stronger than k-OBDD(join) [3].

The proof system 1-OBDD(join, weakening) was introduced by Atserias, Kolaitis and Vardi in 2004 [1]. They noticed that 1-OBDD(join, weakening) simulates Cutting Plane with unary coefficients (CP*). In 2008 Krajicek proved an exponential lower bound for the size of k-OBDD(join, weakening) proofs of transformed Clique-Coloring tautologies using the combination of the monotone interpolation and a transformation that maps formulas hard for one order to formulas hard for all orders [4]. In contrast we show that Clique-Coloring tautologies have short 1-OBDD(join, weakening)-proof, thus 1-OBDD(join, weakening) is strictly stronger than CP*. Using the existence of a short proof of Clique-Coloring and the transformation proposed by Sigerlind [5] we show that k-OBDD(join, weakening, reordering) is strictly stronger than k-OBDD(join, weakening).

References

[1] Albert Atserias, Phokion G. Pg. Kolaitis, and Moshe Y. Vardi. Constraint propagation as a proof system. In Mark Wallace, editor, *Principles and Practice of Constraint Programming - CP 2004*, volume 3258 of *Lecture Notes in Computer Science*, pages 77–91. Springer, 2004.
[2] Jan Friso Groote and Hans Zantema. Resolution and binary decision diagrams cannot simulate each other polynomially. *Discrete Applied Mathematics*, 130(2):157–171, 2003.
[3] Dmitry Itsykson, Alexander Knop, Andrei Romashchenko, and Dmitry Sokolov. On OBDD-Based Algorithms and Proof Systems That Dynamically Change Order of Variables. In Heribert Vollmer and Brigitte Vallée, editors, *34th Symposium on Theoretical Aspects of Computer Science, STACS 2017, March 8-11, 2017, Hannover, Germany*, volume 66 of *LIPIcs*, pages 43:1–43:14. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2017.

[4] Jan Krajiček. An exponential lower bound for a constraint propagation proof system based on ordered binary decision diagrams. *Journal of Symbolic Logic*, 73(1):227–237, 2008.
[5] Nathan Segerlind. On the Relative Efficiency of Resolution-Like Proofs and Ordered Binary Decision Diagram Proofs. In *Proceedings of the 23rd Annual IEEE Conference on Computational Complexity, CCC 2008, 23-26 June 2008, College Park, Maryland, USA*, pages 100–111. IEEE Computer Society, 2008.
[6] Olga Tveretina, Carsten Sinz, and Hans Zantema. An Exponential Lower Bound on OBDD Refutations for Pigeonhole Formulas. *Proceedings Fourth Athens Colloquium on Algorithms and Complexity*, 4(Acac):13–21, 2009.

Optimal Sum-of-Squares Thresholds for Refuting Random CSPs

Pravesh Kothari
(joint work with Ryuhei Mori, Ryan O'Donnell and David Witmer)

Let $P : \{0,1\}^k \to \{0,1\}$ be a nontrivial k-ary predicate. Consider a random instance of the constraint satisfaction problem CSP(P) on n variables with Δn constraints, each being P applied to k randomly chosen literals. Provided the constraint density satisfies $\Delta \gg 1$, such an instance is unsatisfiable with high probability. The *refutation* problem is to efficiently find a proof of unsatisfiability.

We show that whenever the predicate P supports a *t-wise uniform* probability distribution on its satisfying assignments, the sum of squares (SOS) algorithm of degree $d = \Theta(\frac{n}{\Delta^{2/(t-1)} \log \Delta})$ (which runs in time $n^{O(d)}$) *cannot* refute a random instance of CSP(P). In particular, the polynomial-time SOS algorithm requires $\widetilde{\Omega}(n^{(t+1)/2})$ constraints to refute random instances of CSP(P) when P supports a t-wise uniform distribution on its satisfying assignments. Together with recent work of Lee et al. [2], our result also implies that *any* polynomial-size semidefinite programming relaxation for refutation requires at least $\widetilde{\Omega}(n^{(t+1)/2})$ constraints.

More generally, we consider the δ-refutation problem, in which the goal is to certify that at most a $(1-\delta)$-fraction of constraints can be simultaneously satisfied. We show that if P is δ-close to supporting a t-wise uniform distribution on satisfying assignments, then the degree-$\Theta(\frac{n}{\Delta^{2/(t-1)} \log \Delta})$ SOS algorithm cannot $(\delta + o(1))$-refute a random instance of CSP(P). This is the first result to show a distinction between the degree SOS needs to solve the refutation problem and the degree it needs to solve the harder δ-refutation problem.

Our results (which also extend with no change to CSPs over larger alphabets) subsume all previously known lower bounds for semialgebraic refutation of random CSPs. For every constraint predicate P, they give a three-way hardness tradeoff between the density of constraints, the SOS degree (hence running time), and the strength of the refutation. By recent algorithmic results of Allen et al. [1] and Raghavendra et al. [3], this full three-way tradeoff is *tight*, up to lower-order factors.

References

[1] Sarah R. Allen, Ryan O'Donnell, and David Witmer. How to refute a random CSP. In *Proceedings of the 56th Annual IEEE Symposium on Foundations of Computer Science*, pages 689–708, 2015.

[2] James R. Lee, Prasad Raghavendra, and David Steurer. Lower bounds on the size of semidefinite programming relaxations. In *Proceedings of the 47th Annual ACM Symposium on Theory of Computing*, pages 567–576, 2015.

[3] Prasad Raghavendra, Satish Rao, and Tselil Schramm. Strongly refuting random csps below the spectral threshold. *CoRR*, abs/1605.00058, 2016.

Graph Colouring is Hard for Algorithms Based on Hilbert's Nullstellensatz and Gröbner Bases

Massimo Lauria

(joint work with Jakob Nordström)

Given an undirected graph $G = (V, E)$ and a positive integer k, the k-colouring problem asks whether the vertices $v \in V$ be coloured with at most k colours so that no two vertices connected by an edge have the same colour. This *graph colouring problem* is among the most studied NP-complete problems, and a survey on algorithms for this problems is [8].

In this work we focus on algebraic algorithms as the one discussed in the sequence of papers [4, 6, 5, 7], and in general on algorithms that try to decide the k-colouring problem by producing *Nullstellensatz certificates* or performing *Gröbner basis* computations. The common theme of these algorithms is to encode the k-colouring problem as a set of polynomial equations which is satisfiable if and only if G is indeed k-colourable, and then to infer a formal contradiction to show that G does not have such colouring. In the latter case such proofs of non-k-colourability can be formalized as proof in the language of *polynomial calculus (PC)* [1, 3]. Here we study the encoding:

$$\sum_{j=1}^{k} x_{v,j} = 1 \qquad v \in V(G), \tag{1}$$

$$x_{v,j}x_{v,j'} = 0 \qquad v \in V(G),\ j \neq j' \in [k], \tag{2}$$

$$x_{u,j}x_{v,j} = 0 \qquad (u,v) \in E(G),\ j \in [k]. \tag{3}$$

A PC proof of non-k-colourability is a sequence of polynomial equations over field $\mathbb{F}$ so that each line is either one of the equations in the encoding, or it is derived from previous lines using one of two inference rules, where $\alpha, \beta \in \mathbb{F}$:

$$\frac{p = 0 \quad q = 0}{\alpha p + \beta q = 0}\ \text{(linear combination)} \qquad \frac{p = 0}{x_{v,j}p = 0}\ \text{(multiplication)}$$

The main complexity measures about a PC proof are the *degree*, namely the largest degree among the polynomials occurring in the proof; and *monomial size*, which is the cumulative numbers of monomials among all polynomials in the proof.

The idea is that an algebraic algorithm will implicitly produce PC proofs of non-k-colourability, so that the complexity of these proofs are connected to the running time of the algorithm. By heavily capitalizing on results by [9] and [11] prove the following.

Theorem 1. *For any constant $k \geq 3$ there are explicit families of graphs $\{G_n\}_{n\in\mathbb{N}}$ of size $O(n)$ and constant vertex degree, which are not k-colourable but for which the polynomial calculus proof system requires linear degree, and hence exponential size, to prove this fact, regardless of the underlying field.*

Our theorem allows us to answer an open question raised in, for example, [4, 5, 6, 10], namely to find hard graphs for their algorithms.

Corollary 2. *There are explicit families of non-3-colourable graphs such that the algorithms based on Hilbert's Nullstellensatz over* $\mathsf{GF}(2)$ *in* [4, 5] *need to find certificates of linear degree, and hence must solve systems of linear equations of exponential size, in order to certify non-3-colourability.*

This is the extended abstract of the paper presented at the *32nd Annual Computational Complexity Conference (CCC '17).*

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] Richard Beigel and David Eppstein. 3-coloring in time $O(n^{1.3289})$. *Journal of Algorithms*, 54(2):168–204, February 2005.

[3] 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.

[4] 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.

[5] 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.

[6] 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*, 18:551–582, July 2009.

[7] Jesús A. De Loera, Susan Margulies, Michael Pernpeintner, Eric Riedl, David Rolnick, Gwen Spencer, Despina Stasi, and Jon Swenson. Graph-coloring ideals: Nullstellensatz certificates, Gröbner bases for chordal graphs, and hardness of Gröbner bases. In *Proceedings of the 40th International Symposium on Symbolic and Algebraic Computation (ISSAC '15)*, pages 133–140, July 2015.

[8] Thore Husfeldt. Graph colouring algorithms. In Lowell W. Beineke and Robin J. Wilson, editors, *Topics in Chromatic Graph Theory*, Encyclopedia of Mathematics and its Applications, chapter 13, pages 277–303. Cambridge University Press, May 2015.

[9] 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.

[10] Bo Li, Benjamin Lowenstein, and Mohamed Omar. Low degree Nullstellensatz certificates for 3-colorability. *The Electronic Journal of Combinatorics*, 23(1), January 2016.

[11] 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.

Do You Even Lift?

James Lee

1. Lifts of polytopes

A polytope Q is called a *lift* of polytope $P \subseteq \mathbb{R}^d$ if P is the image of Q under an affine projection, i.e. $P = \pi(Q)$, where $\pi : \mathbb{R}^D \to \mathbb{R}^n$ is the composition of a linear map and possibly a translation and $D \geq d$. By applying an affine map first, one can assume that the projection is merely coordinate projection to the first d coordinates. The *extension complexity* $\mathrm{xc}_+(P)$ *of* P is the minimal number of facets in any lift of P.

Let us write P in two different ways: As a convex hull of vertices

$$P = \mathrm{conv}\left(x_1, x_2, \ldots, x_n\right) ,$$

and as an intersection of half-spaces: For some $A \in \mathbb{R}^{m \times d}$,

$$P = \left\{x \in \mathbb{R}^d : Ax \leq b\right\} .$$

Given this pair of representations, we can define the corresponding *slack matrix* of P by

$$S_{ij} = b_i - \langle A_i, x_j \rangle \qquad i \in \{1, 2, \ldots, m\}, j \in \{1, 2, \ldots, n\} .$$

Here, $A_1, \ldots, A_m$ denote the rows of A.

If $M \in \mathbb{R}_+^{m \times n}$ is a non-negative matrix, then a *rank-r non-negative factorization of* M is a factorization $M = AB$ where $A \in \mathbb{R}_+^{m \times r}$ and $B \in \mathbb{R}_+^{r \times n}$. One defines the *non-negative rank of* M, written $\mathrm{rank}_+(M)$, to be the smallest r such that M admits a rank-r non-negative factorization.

Theorem 1 (Yannakakis Factorization Theorem)**.** *For every polytope P, it holds that $\mathrm{xc}_+(P) = \mathrm{rank}_+(S)$ for any slack matrix S of P.*

2. Non-negative rank and lifting theorems

In many models, one can prove a general relationship between the *communication complexity* of a given problem and the *query complexity* of a related problem. This goes by the name of "lifting" of query lower bounds to communication lower bounds, and this was the topic of Toni Pitassi's talk at the workshop.

Consider two finite domains $\mathcal{A}, \mathcal{B}$ and a "gadget" $g : \mathcal{A} \times \mathcal{B} \to \{0, 1\}$. Given $f : \{0,1\}^n \to \mathbb{R}_+$, define the *lifting of f using gadget g* as the matrix $M_f^g : \mathcal{A}^n \times \mathcal{B}^n \to \{0, 1\}$ defined by

$$M_f^g(x, y) = f\left(g(x_1, y_1), \ldots, g(x_n, y_n)\right) .$$

We want to prove lower bounds on $\mathrm{rank}_+(M_f^g)$ (which corresponds to the amount of communication in the "communication in expectation" model) using lower bounds on the complexity of f in some simpler "query" model.

We will consider the two gadgets

$$\mathrm{IP}_m : \{0,1\}^m \times \{0,1\}^m \to \{0,1\}$$
$$\mathrm{SEL}_m : [m] \times \{0,1\}^m \to \{0,1\}\,.$$

The first gadget is the inner product mod 2. The second gadget is defined by $\mathrm{SEL}_m(i,x) := x_i$.

Here is the query model: A *k-junta* is a function $q : \{0,1\}^n \to \mathbb{R}$ that depends on at most k of its inputs. Let $\mathcal{C}_{k,n}$ denote the cone of *non-negative* k-juntas $q : \{0,1\}^n \to \mathbb{R}_+$. Define

$$\deg_+(f) := \min\{k : f \in \mathcal{C}_{k,n}\}\,.$$

Theorem 2 ([1])**.** *For any $f : \{0,1\}^n \to \mathbb{R}_+$ with $\mathbf{E}\, f = 1$, it holds that*

$$\mathrm{rank}_+\left(M_f^{\mathrm{SEL}_m}\right) \geq n^{\Omega\left(\deg_+(f+2^{-n})\right)}\,,$$

where $m \leq c^n$ for some $c > 1$.

The major drawback of this theorem is that its application could require m to be exponential in n. This was remedied in a recent breakthrough of Kothari, Meka, and Raghavendra.

Theorem 3 ([3])**.** *For any $f : \{0,1\}^n \to \mathbb{R}_+$ with $\mathbf{E}\, f = 1$, it holds that*

$$\mathrm{rank}_+\left(M_f^{\mathrm{SEL}_m}\right) \geq \mathrm{rank}_+\left(M_f^{\mathrm{IP}_m}\right) \geq n^{\Omega\left(\deg_+(f+n^{-2})\right)}$$

with $m \leq n^{O(1)}$.

Applications of this theorem include the fact that no linear program of size $2^{n^{o(1)}}$ can approximate MAX-CUT within a factor better than $1/2$ or MAX-3-SAT within a factor better than $7/8$. The proof of [3] is quite technical, but using the methods introduced in the recent BPP lifting work of [2], proving this lifting theorem for the selector gadget becomes relatively simple.

3. Semidefinite extension complexity

Define the *positive semidefinite rank* of a matrix $M \in \mathbb{R}_+^{m \times n}$, written $\mathrm{rank}_{\mathsf{psd}}(M)$, as the smallest value r such that there exist symmetric positive semidefinite matrices $\{A_u, B_v \in \mathbb{R}^{r \times r} : u \in [m], v \in [n]\}$ satisfying

$$M_{u,v} = \mathrm{Tr}(A_u B_v) \qquad \forall u, v\,.$$

Let sos_k denote the cone generated by all squares of degree-k multilinear polynomials $q : \{0,1\}^n \to \mathbb{R}$, and define

$$\deg_{\mathsf{sos}}(f) := \min\{k : f \in \mathsf{sos}_k\}\,.$$

One can prove the following.

Theorem 4 ([4]). *For any $f : \{0,1\}^n \to \mathbb{R}_+$ with $\mathbf{E}\, f = 1$, it holds that*

$$\operatorname{rank}_{\mathsf{psd}}\left(M_f^{\mathrm{SEL}_m}\right) \geq n^{\Omega\left(\deg_+(f+o(1))\right)},$$

where $m \leq c^n$ for some $c > 1$.

It is a fascinating open question whether one can show that this holds assuming only $m \leq n^{O(1)}$, and this would have strong consequences. For instance, it implies that no SDP of size less than $2^{n^{o(1)}}$ can approximate MAX-3-SAT wthin a factor better than 7/8.

References

[1] Siu On Chan, James R. Lee, Prasad Raghavendra, and David Steurer. Approximate constraint satisfaction requires large LP relaxations. *J. ACM*, 63(4):Art. 34, 22, 2016.

[2] Mika Göös, Toniann Pitassi, and Thomas Watson. Query-to-communication lifting for BPP. *CoRR*, abs/1703.07666, 2017.

[3] Pravesh K. Kothari, Raghu Meka, and Prasad Raghavendra. Approximating rectangles by juntas and weakly-exponential lower bounds for LP relaxations of csps. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017*, pages 590–603, 2017.

[4] 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.

When SOS Fails (Maybe It's Because Everything Fails)

Ryan O'Donnell

I discussed the SOS (Sum Of Squares) proof system, and lower bounds for it, in the context of random CSPs (constraint satisfaction problems). The SOS proof system (also known as Lasserre, Static LS+, or Positivstellensatz), was introduced in works of Grigoriev–Vorobjov [7], Lasserre [9], and Parrilo [11]. It is a very powerful proof system, able to capture both "local" refutation methods and also "spectral" refutation methods. Furthermore, it is "automatizable" in the sense that when n-variable degree-d refutations exist, they can be found in $\mathrm{poly}(n^d)$ time (subject to certain technical caveats; see [10, 13]). Proving lower bounds for SOS refutations is therefore both desirable and plausible. However, due to the power of SOS, we might need to seek unsatisfiable formulas that are not hard to refute due to some limitation of SOS, but rather are hard to refute due to a (suspected) lack of *any* kind of succinct proof. The main candidates for such problems come from random instances of CSPs. SOS lower bounds for random CSPs also give evidence for Feige's Hypothesis [3], candidate cryptographic primitives proposed by Goldreich [5], and hardness of learning [2].

A classic example of a random CSP is random 3SAT, with n variables, m clauses/constraints, and "constraint density" $\Delta = m/n$. Once $\Delta > 4.2667$, random 3SAT formulas will with high probability (whp) be unsatisfiable; this statement is trivial to prove once $\Delta > 10$, say. On the other hand, once such a random

formula is fixed, refuting it might be very difficult; indeed, there might not even exist any kind of succinct refutation. When $\Delta \ll \sqrt{n}$, no known algorithm for finding refutations (whp) exists. On the other hand, for $\Delta \gg \sqrt{n}$, Friedman and Goerdt [4] gave a "spectral" algorithm that finds refutations whp. It is folklore these refutations can be made in "constant-degree SOS". A natural question is to show that succinct ("constant-degree") SOS refutations do not exist for random 3SAT when $\Delta \ll \sqrt{n}$. This was done by Grigoriev [6] and Schoenebeck [14].

In the talk, I described how SOS lower bound bounds can be proved by means of giving an appropriate *satisfying (degree-d) pseudoexpectation*; i.e., a linear map $\widetilde{E}[\cdot]$ on polynomials of degree at most d which satisfies $\widetilde{\mathbf{E}}[1] = 1$, $\widetilde{\mathbf{E}}[\text{“}C\text{”}] = 1$ for the arithmetization "C" of every 3SAT clause C, and $\widetilde{\mathbf{E}}[p(x)^2] \geq 0$ for every polynomial of degree at most $d/2$. The intuition is that such pseudoexpectations "look like" they come from probability distributions over satisfying assignments, as long as only one looks at expressions of degree at most d. Grigoriev and Schoenebeck's lower bounds show that for $\Delta \ll \sqrt{n}$, satisfying $O(1)$-degree pseudoexpectations exist whp for random 3SAT formulas. Conversely, Friedmand and Goerdt's work can be seen as showing that when $\Delta \gg \sqrt{n}$, satisfying $O(1)$-degree pseudoexpectations do not exist whp for random 3SAT formulas.

Finally, I discussed recent work in extending such results to general CSPs, and considering tradeoffs between constraint density, SOS degree, and quality of refutation (meaning refuting even that a $1 - \delta$ fraction of constraints can be satisfied). Such work includes positive results for SOS by Allen et al. [1] and Raghavendra et al. [12], and matching negative results by Kothari et al. [8].

References

[1] Sarah Allen, Ryan O'Donnell, and David Witmer. How to refute a random CSP. In *Proceedings of the 56th Annual IEEE Symposium on Foundations of Computer Science*, pages 689–708, 2015.

[2] Amit Daniely, Nati Linial, and Shai Shalev-Shwartz. From average case complexity to improper learning complexity. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, pages 441–448, 2014.

[3] Uriel Feige. Relations between average case complexity and approximation complexity. In *Proceedings of the 34th Annual ACM Symposium on Theory of Computing*, pages 543–543, 2002.

[4] Joel Friedman and Andreas Goerdt. Recognizing more unsatisfiable random 3-SAT instances efficiently. In *Proceedings of the 28th Annual International Colloquium on Automata, Languages and Programming*, pages 310–321, 2001.

[5] Oded Goldreich. Candidate one-way functions based on expander graphs. Technical Report 90, Electronic Colloquium on Computational Complexity, 2000.

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

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

[8] Pravesh Kothari, Ryuhei Mori, Ryan O'Donnell, and David Witmer. Sum of squares lower bounds for refuting any CSP. In *stoc17*, pages 132–145, 2017. Manuscript available at `http://www.cs.cmu.edu/~odonnell`.

[9] Jean Lasserre. Optimisation globale et théorie des moments. *Comptes Rendus de l'Académie des Sciences*, 331(11):929–934, 2000.

[10] Ryan O'Donnell. SOS is not obviously automatizable, even approximately. In *Proceedings of the 8th Annual Innovations in Theoretical Computer Science conference*, 2017.
[11] Pablo A. Parrilo. *Structured Semidefinite Programs and Semialgebraic Geometry Methods in Robustness and Optimization*. PhD thesis, California Institute of Technology, 2000.
[12] Prasad Raghavendra, Satish Rao, and Tselil Schramm. Strongly refuting random csps below the spectral threshold. In *Proceedings of the 49th Annual ACM Symposium on Theory of Computing*, pages 121–131, 2017.
[13] Prasad Raghavendra and Benjamin Weitz. On the bit complexity of sum-of-squares proofs. Technical Report 1702.05139, arXiv, 2017.
[14] Grant Schoenebeck. Linear level Lasserre lower bounds for certain k-CSPs. In *Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science*, pages 593–602, 2008.

Proof Complexity Meets Algebra

Joanna Ochremiak
(joint work with Albert Atserias)

In my talk I discussed a way to develop the standard theory of reductions between constraint satisfaction problems so that it applies to the most studied propositional and semi-algebraic proof systems.

The literature on CSPs has focussed on three different types of conditions that, if met by two constraint languages, give a reduction from the CSP of one language to the CSP of the other. These conditions are a) *pp-interpretability*, b) *homomorphic equivalence*, and c) *addition of constants to the core* (see [4, 8]). Those three types of reductions correspond to classical algebraic constructions at the level of the *algebras of polymorphisms* of the constraint languages. Thus, for any fixed algorithm, heuristic, or method $\mathcal{M}$ for deciding the satisfiability of CSPs, if the class of constraint languages that are solvable by $\mathcal{M}$ is closed under these notions of reducibility, then this class admits a purely algebraic characterization.

Our first result is that, for most proof systems P in the literature, each of these methods of reduction preserves the proof complexity of the problem with respect to proofs in P. We show this for DNF-resolution with terms of bounded size, bounded-depth Frege, and Frege, Sherali-Adams, SOS, and Lovász-Schrijver of bounded and unbounded degree.

Our second main result is an application: we obtain unconditional gap theorems for the proof complexity of CSPs. Building on the bounded-width theorem for CSPs [3, 7], the known correspondance between local consistency algorithms, existential pebble games and bounded width resolution [2, 12], the lower bounds for propositional and semi-algebraic proof systems [1, 5, 6, 9, 10, 13], and a modest amount of additional work to fill in the gaps, we prove a strong gap theorem which says that for any finite constraint language B exactly one of the following holds: either B has resolution refutations of bounded width and hence polynomial size, or B has neither Frege refutations of bounded depth and subexponential size, nor SOS refutations of sublinear degree. Moreover, the first case happens precisely if B has bounded width. The collapse of SOS to bounded width was already known [14]; we give a different proof.

Our third main result is about proof systems that operate with polynomial inequalities beyond SOS. The above theorem raises a question: is there a natural proof system for which the class of languages that have efficient unsatisfiability proofs is closed under the standard reducibility methods for CSPs, and that at the same time has efficient unsatisfiability proofs beyond bounded width? We give an example of such a proof system by showing that bounded-degree Lovász-Schrijver satisfies both requirements: unsatisfiable systems of linear equations over the 2-element group have LS refutations of bounded degree and polynomial size. Proving this amounts to showing that Gaussian elimination over $\mathbb{Z}_2$ can be simulated by reasoning with low-degree polynomial inequalities over $\mathbb{R}$. The proof of this counter-intuitive fact relies on earlier work in proof complexity for reasoning about gaps of the type $(-\infty, c] \cup [c+1, +\infty)$, for $c \in \mathbb{Z}$, through quadratic polynomial inequalities [11].

References

[1] M. Ajtai. The complexity of the pigeonhole principle. In *29th Annual IEEE Symposium on Foundations of Computer Science*, pages 346–355, 1988.

[2] A. Atserias and V. Dalmau. A combinatorial characterization of resolution width. *J. Comput. Syst. Sci.*, 74(3):323–334, May 2008. A preliminary version appeared in CCC 2003.

[3] L. Barto and M. Kozik. Constraint satisfaction problems solvable by local consistency methods. *J. ACM*, 61(1):3:1–3:19, January 2014.

[4] L. Barto, J. Opršal, and M. Pinsker. The wonderland of reflections. *CoRR*, abs/1510.04521, 2015.

[5] P. Beame, R. Impagliazzo, J. Krajícek, T. Pitassi, P. Pudlák, and A. Woods. Exponential lower bounds for the pigeonhole principle. In *24th Annual ACM Symposium on the Theory of Computing*, pages 200–220, 1992.

[6] E. Ben-Sasson. Hard examples for bounded depth frege. In *34th Annual ACM Symposium on the Theory of Computing*, pages 563–572, 2002.

[7] A. Bulatov. Bounded relational width. Manuscript, 2009.

[8] A. Bulatov, P. Jeavons, and A. Krokhin. Classifying the complexity of constraints using finite algebras. *SIAM Journal on Computing*, 34(3):720–742, 2005.

[9] Siu On Chan. Approximation resistance from pairwise-independent subgroups. *J. ACM*, 63(3):27:1–27:32, August 2016.

[10] D. Grigoriev. Linear lower bound on degrees of positivstellensatz calculus proofs for the parity. *Theoretical Computer Science*, 259(1–2):613–622, 2001.

[11] D. Grigoriev, E. A. Hirsch, and D. V. Pasechnik. Complexity of semi-algebraic proofs. *Moscow Mathematical Journal*, 4(2):647–679, 2002.

[12] Ph. G. Kolaitis and M. Y. Vardi. A game-theoretic approach to constraint satisfaction. In *Proceedings of the Seventeenth National Conference on Artificial Intelligence and Twelfth Conference on Innovative Applications of Artificial Intelligence*, pages 175–181. AAAI Press, 2000.

[13] J. Krajícek, P. Pudlák, and A. Woods. Exponential lower bound to the size of bounded depth Frege proofs of the pigeon hole principle. *Random Structures and Algorithms*, 7(1):15–39, 1995.

[14] J. Thapper and S. Živný. The limits of SDP relaxations for general-valued csps. *CoRR*, abs/1612.01147, 2016.

Sum of Squares Methods: Beyond 0/1

Pablo A. Parrilo

Summary: We present a short survey of sum of squares methods, beyond purely combinatorial situations. We discuss applications to dynamical systems, approximation of the joint spectral radius, as well as outline different methodologies for exploiting structure (e.g., symmetries).

Sum of squares and SDP. Semidefinite programming (SDP) is a natural class of convex optimization problems, that generalize linear programming to symmetric matrices. The condition that a multivariate polynomial is a sum of squares (SOS) can be rewritten as a semidefinite program. The reason is the following theorem:

Theorem 1. [8] *A polynomial $p(x)$ is SOS if and only if $p(x) = z^T Q z$, where z is a vector of monomials in the x_i variables, $Q \in \mathcal{S}^N$ and $Q \succeq 0$.*

The vector of monomials z (and therefore N) in general depends on the degree and sparsity pattern of $p(x)$. If $p(x)$ has n variables and total degree $2d$, then z can always be chosen as a subset of the set of monomials of degree less than or equal to d, of cardinality $N = \binom{n+d}{d}$.

Sum of squares appear naturally in the construction of infeasibility certificates for systems of polynomial equations/inequalities over the reals, via the Positivstellensatz (or Real Nullstellensatz, see e.g. [4]). Table 1 summarizes different classes of infeasibility certificates, according to the nature of the equations and the underlying field.

Degree \ Field	Complex	Real
Linear	*Range/Kernel* Linear Algebra	*Farkas Lemma* Linear Programming
Polynomial	*Nullstellensatz* Bounded degree: Linear Algebra Gröbner bases	*Positivstellensatz* Bounded degree: SDP

Table 1. Infeasibility certificates and associated computational techniques.

Dynamical systems and Lyapunov stability. Consider a dynamical system given by differential equations of the form

$$\dot{x}(t) = f(x(t))$$

where f is a polynomial map and $f(0) = 0$. The system is *globally asymptotically stable* if all solutions satisfy $x(t) \to 0$, as $t \to \infty$, for all possible initial conditions $x(0)$ (plus a technical condition, omitted here for simplicity).

For a system to be globally asymptotically stable, it is sufficient to show the existence of a Lyapunov function that satisfies

$$V(x) > 0, \qquad \dot{V}(x) = \left(\frac{\partial V}{\partial x}\right)^T f(x) < 0$$

for all $x \in \mathbb{R}^n \setminus \{0\}$ (see e.g., [5]). The SOS approach makes possible to search over affinely parametrized polynomial (or rational) Lyapunov functions:

$$V(x) \text{ is sos}, \qquad -\dot{V}(x) = -\left(\frac{\partial V}{\partial x}\right)^T f(x) \text{ is sos}.$$

These conditions can be expressed as sum of squares constraints in terms of the coefficients of the Lyapunov function. Since both conditions are affine in the coefficients of $V(x)$, they can be transformed into a standard SDP formulation. Similar approaches have been developed for more complicated problems in systems and control theory, including non-polynomial, time-delayed, stochastic, uncertain, or hybrid systems; see e.g. [6, 10, 1] and the references therein.

Joint spectral radius. The *joint spectral radius* [11] of a finite set of matrices is defined as

$$\rho(A_1, \dots, A_m) := \limsup_{k \to +\infty} \max_{\sigma \in \{1,\dots,m\}^k} ||A_{\sigma_k} \cdots A_{\sigma_2} A_{\sigma_1}||^{1/k}. \tag{4}$$

This quantifies the maximum growth (or decay) rate that can be obtained by taking arbitrary products of the matrices A_i. It is well known that computing ρ is hard from a computational viewpoint, and even approximating it is difficult [3, 12]. Nevertheless, it is possible to give SOS-based algorithms with provable approximation properties.

Theorem 2 ([9])**.** *Let $p(x)$ be a strictly positive homogeneous polynomial of degree $2d$ that satisfies*

$$p(A_i x) \leq \gamma\, p(x), \qquad \forall x \in \mathbb{R}^n \quad i = 1, \dots, m.$$

Then, $\rho(A_1, \dots, A_m) \leq \gamma^{\frac{1}{2d}}$.

Consider the following SOS relaxation of the conditions in Theorem 2:

$$\rho_{SOS,2d} := \inf_{p(x),\gamma} \gamma \qquad \text{s.t.} \begin{cases} p(x) & \text{is SOS} \\ \gamma^{2d} p(x) - p(A_i x) & \text{is SOS} \end{cases}$$

where $p(x)$ is a homogeneous polynomial of degree $2d$.

Theorem 3 ([9])**.** *The SOS-based approximation $\rho_{SOS,2d}$ satisfies*

$$\eta^{-\frac{1}{2d}} \cdot \rho_{SOS,2d}(\mathcal{M}) \leq \rho(\mathcal{M}) \leq \rho_{SOS,2d}(\mathcal{M}),$$

where $\eta := \min\{m, \binom{n+d-1}{d}\}$.

References

[1] A. A. Ahmadi, M. Krstic, and P. A. Parrilo. A globally asymptotically stable polynomial vector field with no polynomial Lyapunov function. In *IEEE Conference on Decision and Control and European Control Conference (CDC-ECC)*, pages 7579–7580. IEEE, 2011.

[2] G. Blekherman, P. A. Parrilo, and R. Thomas, editors. *Semidefinite optimization and convex algebraic geometry*, volume 13 of *MOS-SIAM Series on Optimization*. SIAM, 2012.

[3] V. D. Blondel and J. N. Tsitsiklis. The boundedness of all products of a pair of matrices is undecidable. *Systems & Control Letters*, 41:135–140, 2000.

[4] J. Bochnak, M. Coste, and M.-F. Roy. *Real Algebraic Geometry*. Springer, 1998.

[5] H. Khalil. *Nonlinear Systems*. Macmillan Publishing Company, 1992.

[6] A. Papachristodoulou and S. Prajna. On the construction of Lyapunov functions using the sum of squares decomposition. In *Proceedings of the 41^{th} IEEE Conference on Decision and Control*, 2002.
[7] P. A. Parrilo. *Structured semidefinite programs and semialgebraic geometry methods in robustness and optimization*. PhD thesis, California Institute of Technology, May 2000.
[8] P. A. Parrilo. Semidefinite programming relaxations for semialgebraic problems. *Math. Prog.*, 96(2, Ser. B):293–320, 2003.
[9] P. A. Parrilo and A. Jadbabaie. Approximation of the joint spectral radius using sum of squares. *Linear Algebra and its Applications*, 428(10):2385–2402, 2008.
[10] S. Prajna, A. Jadbabaie, and G. J. Pappas. Stochastic safety verification using barrier certificates. In *Proceedings of the 43^{th} IEEE Conference on Decision and Control*, 2004.
[11] G. C. Rota and W. G. Strang. A note on the joint spectral radius. *Indag. Math.*, 22:379–381, 1960.
[12] J. N. Tsitsiklis and V. Blondel. The Lyapunov exponent and joint spectral radius of pairs of matrices are hard- when not impossible- to compute and to approximate. *Mathematics of Control, Signals, and Systems*, 10:31–40, 1997.

Part I: Proof Complexity Primer
Part II: Lifting in Communication Complexity and Proof Complexity

Toniann Pitassi

In the first half of my talk, I will give a brief introduction to proof complexity. I will introduce all of the standard proof systems that will be discussed this week (including propositional proof systems, algebraic proof systems and semi-algebraic proof systems). I will give a brief survey of the known lower bound techniques and state of the art in proof complexity lower bounds.

In the second half of the talk, I will discuss the "lifting" in communication complexity. Communication complexity attempts to understand the limits and power of communication in solving computational problems through the joint efforts of multiple parties. Since its introduction in the 1970's, communication complexity has found an astounding variety of applications across computer science, including: networks, streaming algorithms, distributed computing, circuit complexity, computational geometry, data structures, and game theory.

In the second half of this talk we will discuss *hardness escalation*, or *lifting* in communication complexity, a growing research area whereby lower bounds and separations in communication complexity are obtained by developing "simulation theorems". The basic idea of a simulation theorem is to start with an *arbitrary* function and "lift it" via function composition in order to get a new function whose communication complexity is essentially the same as the query complexity of the original function. In query complexity, the objects of study are decision trees, perhaps the simplest, most basic model of computation. A simulation theorem thus shows that the optimal communication protocol for the composed function is essentially the trivial one which mimics the decision tree protocol.

The first hardness escalation theorem was [1] who proved a simulation theorem for deterministic decision trees and deterministic communication protocols. Since then, many other simulation theorems have been developed for other decision tree models and their corresponding communication complexity classes.

These simulation theorems have introduced new tools into complexity theory, and have led to the resolution of many open problems including: graph theory, combinatorial optimization, circuit complexity and cryptography, proof complexity and communication complexity. Moreover the field has led to a revival of query complexity, with new techniques leading to the resolution of some longstanding open problems.

In query complexity the objects of study are decision trees, one of the simplest and most basic models of computation. As with most complexity classes, decision trees come in many flavors: deterministic, nondeterministic, randomized, etc. Query complexity was intended to separate complexity classes relative to oracles.

Prove a general communication-to-query simulation theorem stating that for a large class of communication problems F any protocol for F can be efficiently simulated by a decision tree solving a related problem f. With a simulation theorem at hand, communication lower bounds can be obtained by just proving a decision tree lower bound, a much more tractable problem.

After reviewing the many lifting theorems that have been proven for various models of communication complexity, we will focus on their applications in proof complexity.

References

[1] Ran Raz and Pierre McKenzie. Separation of the monotone NC hierarchy. *Combinatorica*, 19(3):403–435, March 1999. Preliminary version in *FOCS '97*.

Exact Tensor Completion with Sum-of-Squares

Aaron Potechin
(joint work with David Steurer)

In the matrix completion problem, we are given some entries of a matrix and we are asked to fill in the remaining entries. A canonical example of this problem is the Netflix challenge where we are given the ratings of users on some movies and we are asked to predict their ratings on other movies. While the matrix completion problem is impossible to solve in general, it can be solved efficiently if the matrix has the additional structure of being low-rank.

The tensor completion problem is analogous to the matrix completion problem except that there is a third dimension. This makes the problem considerably more difficult, as even if we are given the entire tensor, it can be NP-hard to find the minimal rank decomposition [2]. Thus, we expect the tensor completion problem to be difficult in general but we can hope to solve special cases of the problem. In this paper, we show that degree 4 sum of squares solves the tensor completion problem exactly when the components are orthogonal.

This work was primarily inspired by two papers, "A Simpler Approach to Matrix Completion" by Benjamin Recht [3] and "Noisy Tensor Completion via Sum of Squares" by Boaz Barak and Ankur Moitra [1]. We asked whether Recht's

techniques could be generalized to tensor completion and whether the tensor completion result could be made exact or some error is necessary. With this work, we provide a partial affirmative answer to both questions.

To prove our results, we view the analysis of nuclear norm minimization for matrix completion in terms of a dual certificate which certifies that the true answer is optimal. We then adapt this certificate to the tensor completion problem. A key idea for both our analysis and Barak and Moitra's analysis is to use SOS-symmetry, this is what allows us to do better than flattening the tensor into an $n \times n^2$ matrix and using matrix completion.

One open problem is to generalize our results beyond the non-orthogonal case. We only prove it for the orthogonal case, but this is likely a flaw in our analysis rather than the algorithm itself. Indeed, Barak and Moitra obtained noisy completion in a somewhat more general setting. A second open question is whether the sum of squares algorithm for tensor completion can be modified to be faster and useable in practice.

References

[1] Boaz Barak and Ankur Moitra. Noisy tensor completion via the sum-of-squares hierarchy, COLT, JMLR Workshop and Conference Proceedings, vol. 49, JMLR.org,p. 417–445, 2016.

[2] Christopher Hillar and Lek-Heng Lim. Most Tensor Problems are NP-hard. JACM Volume 60, Issue 6, Article No. 45, 2013.

[3] Benjamin Recht. A simpler approach to matrix completion. Journal of Machine Learning Research 12 p.3413–3430, 2011

The Canonical NP-Pairs of Bounded Depth Frege Systems

Pavel Pudlak

Definition 1 ([2])**.** *Let P be a propositional proof system. The* canonical pair *of P is the pair of disjoint NP sets (A, B) where*

$A = \{(\phi, 1^m) : \phi \text{ is satisfiable}\}$
$B = \{(\phi, 1^m) : \phi \text{ has a } P\text{-refutation of size at most } m\}$.

We want to characterize the canonical pairs of bounded depth Frege systems, i.e., we want to find pairs defined by combinatorial conditions (rather than logical) that are equivalent to these canonical pairs with respect to polynomial time reductions. So far only the canonical pair for Resolution has been characterized [1].

We propose a characterization based on certain games defined as follows. The games are played on $k \times n$ square grids, where k is a constant, called the *depth of the game*, and n is a parameter. Two players alternate and fill in the squares with elements from an alphabet Σ. They start at the left upper corner and gradually fill the first row. Then they fill the second row in the *opposite* direction, i.e., the right-left direction. Next they fill the third row in the left-right direction, and so on.

Let us denote by $A = \{a_{ij}\}$ the matrix they construct. An upper segment $(a_{1j}, a_{2j}, \ldots, a_{ij})^T$ of a column in A will be called a *position*. Legal moves are determined by positions. In more detail, for every pair (i, j), if i is odd and $j < n$, then legal moves $a_{i,j+1}$ are determined only by the position $(a_{1j}, a_{2j}, \ldots, a_{ij})^T$, and if i is even and $j > 1$, then legal moves $a_{i,j-1}$ are determined only by the position $(a_{1j}, a_{2j}, \ldots, a_{ij})^T$. If i is odd, then legal moves $a_{i+1,n}$ are determined by $(a_{1n}, \ldots, a_{in})^T$, and if i is even, then legal moves $a_{i+1,1}$ are determined by $(a_{11}, \ldots, a_{i1})^T$. The game ends when the players reach a winning/loosing position, or when there is no legal move for the player in turn.

Thus the game is determined by a set of winning/loosing positions, and for every position, a set of legal moves. If we assume that the size of the alphabet Σ is polynomial in n, then the size of the description of the game is also polynomial in n.

Positional strategies of the players are defined in the same way as legal moves the only difference being that strategies determine moves of only one player and for each position they give only one choice, or none in case of an end position. For $k > 1$, it is possible that neither player has a positional winning strategy.

Let a depth k be fixed. We define a pair of disjoint NP set by

$A_k := \{G \mid \text{Player 1 has a positional winning strategy in } G\}$,
$B_k := \{G \mid \text{Player 2 has a positional winning strategy in } G\}$,

where Gs are depth k games.

Our aim is to prove that these pairs characterize the canonical pairs of bounded depth Frege proof systems. A substantial amount of lemmas needed to prove this conjecture has been proven, however there is still an important part that has to be finished. Our proof borrows ideas from [3]. The depth k of the games does not correspond exactly to the depth of the Frege systems; more work will be needed to get a precise characterization.

References

[1] Arnold Beckmann, Pavel Pudlák, and Neil Thapen, *Parity Games and Propositional Proofs,* ACM Transaction on Computational Logic, Vol 15:2, article 17, (2014).
[2] Alexander A. Razborov, *On provably disjoint NP-pairs*, Tech. Rep. RS-94-36, Aarhus, (1994).
[3] Allan Skelley and Neil Thapen, *The Provably Total Search Problems of Bounded Arithmetic,* Proc. London Math. Soc. (3), 103, 106-138, (2011)

Symmetric Sums of Squares over k-Subset Hypercubes

Annie Raymond
(joint work with James Saunderson, Mohit Singh, and Rekha Thomas)

Polynomial optimization over discrete hypercubes plays a central role in many areas such as combinatorial optimization, decision problems and proof complexity. In many situations, it is natural to consider k-subset hypercubes by which we mean discrete hypercubes whose coordinates are indexed by the k-element subsets of a

ground set $[n]$. For instance, a major focus in extremal graph theory is to optimize the edge (hyperedge) density in families of graphs (hypergraphs) with specified structure which can be cast as optimization problems over k-subset hypercubes. In this scenario, as in many others, the polynomial to be optimized is often symmetric which allows representation-theoretic techniques to dramatically cut down on computations. Here, we consider the general problem of optimizing a symmetric polynomial over a k-subset hypercube $\mathcal{V}_{n,k} := \{0,1\}^{\binom{n}{k}}$ when $k \geq 2$; the case $k = 1$ was handled in [2]. See [1, 3, 4, 5, 6, 7, 8, 9, 10, 11, 14, 15, 16, 17, 18, 23, 24] for other uses of symmetry in semidefinite programming.

Phrased differently, our central problem is to certify the non-negativity of a symmetric polynomial p over $\mathcal{V}_{n,k}$ which can be done by finding a sum of squares (sos) expression that equals p as a function on $\mathcal{V}_{n,k}$. In [12], Gatermann and Parrilo showed how to use representation theory to simplify the computations involved in finding a sos representation of a polynomial p that is invariant under the action of a finite group. We propose a variant of their method that is adapted to the combinatorics in our setting, and hence, offers many simplifications and advantages. For every symmetric polynomial that has a sos expression of a fixed degree, our method finds a succinct sos expression whose size depends only on the degree and not on the number of variables. Our results relate naturally to Razborov's flag algebra calculus for solving problems in extremal combinatorics ([19, 20, 21, 22]). This connection exposes a family of non-negative polynomials first appearing in [13] that cannot be certified exactly with any fixed set of flags. Moreover, the polynomial setting allows flags to be used for finite problems as well as for sparse graph theoretical problems in a systematic way.

References

[1] Y. Bai, E. de Klerk, D.V. Pasechnik, and R. Sotirov. Exploiting group symmetry in truss topology optimization. *Optimization and Engineering*, 10:331–349, 2009.

[2] G. Blekherman, J. Gouveia, and J. Pfeiffer. Sums of squares on the hypercube. *Mathematische Zeitschrift*. to appear.

[3] C. Bachoc, D.C. Gijswijt, A. Schrijver, and F. Vallentin. Invariant semidefinite programs. In *Handbook on Semidefinite, Conic and Polynomial Optimization*, volume 166 of *Internat. Ser. Oper. Res. Management Sci.*, pages 219–269. Springer, New York, 2012.

[4] C. Bachoc and F. Vallentin. New upper bounds for kissing numbers from semidefinite programming. *Journal of the AMS*, 21:909–924, 2008.

[5] E. de Klerk, J. Maharry, D.V. Pasechnik, R.B. Richter, and G. Salazar. Improved bounds for crossing numbers of $k_{m,n}$ and k_n. *SIAM Journal of Discrete Mathematics*, 20:189–202, 2006.

[6] E. de Klerk and D.V. Pasechnik. Solving sdp's in non-commutative algebras part i: the dual-scaling algorithm. *Discussion paper from Tilburg University, Center for economic research*, 2005.

[7] E. de Klerk, D.V. Pasechnik, and A. Schrijver. Reduction of symmetric semidefinite programs using the regular $*$-representation. *Mathematical Programming Series B*, 109:613–624, 2007.

[8] E. de Klerk and R. Sotirov. Exploiting group symmetry in semidefinite programming relaxations of the quadratic assignment problem. *Mathematical Programming Series A*, 122:225–246, 2010.

[9] D. Gijswijt. Block diagonalization for algebra's associated with block codes. arXiv:0910.4515, 2014.
[10] N. Gvozdenović and M. Laurent. Computing semidefinite programming lower bounds for the (fractional) chromatic number via block-diagonalization. *SIAM Journal of Optimization*, 19:592–615, 2008.
[11] N. Gvozdenović, M. Laurent, and F. Vallentin. Block-diagonal semidefinite programming hierarchies for 0/1 programming. *Operations Research Letters*, 37:27–31, 2009.
[12] K. Gatermann and P.A. Parrilo. Symmetry groups, semidefinite programs, and sums of squares. *J. Pure Appl. Algebra*, 192(1-3):95–128, 2004.
[13] D. Grigoriev. Complexity of Positivstellensatz proofs for the knapsack. *Computational Complexity*, 10(2):139–154, 2001.
[14] D. Gijswijt, A. Schrijver, and H. Tanaka. New upper bounds fof nonbinary codes based on the terwilliger algebra and semidefinite programming. *Journal of Combinatorial Theory, Series A*, 113:1719–1731, 2006.
[15] L. Jansson, J.B. Lasserre, C. Riener, and T. Theobald. Exploiting symmetries in sdp-relaxations for polynomial optimization. *Optimization Online*, September 2006.
[16] Y. Kanno, M. Ohsaki, K. Murota, and N. Katoh. Group symmetry in interior-point methods for semidefinite program. *Optimization and Engineering*, 2:293–320, 2001.
[17] M. Laurent. Strengthened semidefinite bounds for codes. *Mathematical Programming*, 109(2-3):239–261, 2007.
[18] B. Litjens, S. Polak, and Schrijver A. Semidefinite bounds for nonbinary codes based on quadruples. *Designs, Codes and Cryptography*, pages 1–14, 2016.
[19] A.A. Razborov. Flag algebras. *J. Symbolic Logic*, 72(4):1239–1282, 2007.
[20] A.A. Razborov. On 3-hypergraphs with forbidden 4-vertex configurations. *SIAM Journal on Discrete Mathematics*, 24(3):946–963, 2010.
[21] A.A. Razborov. Flag algebras: an interim report. In *The Mathematics of Paul Erdős II*, pages 207–232. Springer, 2013.
[22] A.A. Razborov. On Turán's (3, 4)-problem with forbidden subgraphs. *Mathematical Notes*, 95(1-2):245–252, 2014.
[23] A. Schrijver. *Association schemes and the Shannon capacity: Eberlein polynomials and the Erdös-Ko-Rado theorem.* Number 25 in Algebraic methods in graph theory, Vol. I, II (Szeged, 1978), Colloq. Math. Soc. János Bolyai. North-Holland, Amsterdam-New York, 1981.
[24] A. Schrijver. New code upper bounds from the terwilliger algebra. *IEEE Transactions on Information Theory*, 51:2859–2866, 2005.

Unified and Optimal Lower Bounds for Monotone Computation

Robert Robere
(joint work with Toniann Pitassi)

A classic counting argument due to Shannon [8] shows that almost all boolean functions have high complexity — more formally, all but an exponentially small fraction of boolean functions with n input variables require strongly exponential (i.e. $2^{\Omega(n)}$) size circuits. On the other hand, the best lower bounds on circuit size (with, say, AND, OR, and NOT gates) for any *explicit* function is on the order of $5n - o(1)$, which is not even superlinear [4]! The state of affairs is not much better for boolean formulas, for which we merely have the cubic lower bounds $\Omega(n^{3-\varepsilon})$ for all $\varepsilon > 0$ [3]. Even for monotone circuits and formulas, which are relatively well understood, the best lower bounds for explicit functions are not strongly

exponential: for monotone circuits the strongest lower bound is $2^{\Omega((n/\log n)^{1/3})}$ by Harnik and Raz [2], and for monotone formulas the best lower bound is $2^{\Omega(n/\log n)}$ by Göös and Pitassi [1].

In this talk, we discuss some recent work (joint with Toniann Pitassi [5]) in which we prove the first strongly exponential lower bounds for computing an explicit function (i.e. one computable in NP) in a wide variety of monotone circuit models. More precisely, we prove the following theorem:

Theorem 1. *For all sufficiently large N, there is an explicit monotone boolean function $f : \{0,1\}^N \to \{0,1\}$ such that every monotone formula, switching network, real span program, or comparator circuit computing f requires size 2^{cn} for some universal constant $c > 0$.*

The lower bounds are proved via Razborov's rank measure [6], which is a complexity measure on boolean functions that is strong enough to bound all of these circuit models simultaneously. To prove a lower bound on this rank measure we use a framework introduced in [7] involving a *lifting theorem* that reduces the problem to bounding a new complexity measure on search problems called the *algebraic gap complexity*. We also discuss some recent extensions of this work, specifically: an extension of the lower bounds to monotone span programs over *all* fields, and an equivalence (for certain search problems) between algebraic gap complexity and Nullstellensatz degree (this second result, in particular, yields a *characterization* of the minimal monotone span program size by Nullstellensatz degree for certain structured boolean functions).

References

[1] Mika Göös and Toniann Pitassi. Communication lower bounds via critical block sensitivity. In *Symposium on Theory of Computing, STOC 2014, New York, NY, USA, May 31 - June 03, 2014*, pages 847–856, 2014.

[2] Danny Harnik and Ran Raz. Higher lower bounds on monotone size. In F. Frances Yao and Eugene M. Luks, editors, *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, May 21-23, 2000, Portland, OR, USA*, pages 378–387. ACM, 2000.

[3] Johan Håstad. The shrinkage exponent of de morgan formulas is 2. *SIAM J. Comput.*, 27(1):48–64, 1998.

[4] Kazuo Iwama and Hiroki Morizumi. An explicit lower bound of 5n - o(n) for boolean circuits. In *Mathematical Foundations of Computer Science 2002, 27th International Symposium, MFCS 2002, Warsaw, Poland, August 26-30, 2002, Proceedings*, pages 353–364, 2002.

[5] Toniann Pitassi and Robert Robere. Strongly exponential lower bounds for monotone computation. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017*, pages 1246–1255, 2017.

[6] Alexander A. Razborov. Applications of matrix methods to the theory of lower bounds in computational complexity. *Combinatorica*, 10(1):81–93, 1990.

[7] Robert Robere, Toniann Pitassi, Benjamin Rossman, and Stephen A. Cook. Exponential lower bounds for monotone span programs. *Electronic Colloquium on Computational Complexity (ECCC)*, 23:64, 2016.

[8] Claude Shannon et al. The synthesis of two-terminal switching circuits. *Bell System Technical Journal*, 28(1):59–98, 1949.

Duality of Low-Degree SoS Refutations and Efficient Spectral Algorithms in the Average Case

Tselil Schramm

(joint work with Sam Hopkins, Pravesh Kothari, Aaron Potechin, Prasad Raghavendra and David Steurer)

It is well-known that semidefinite programs (such as the Sum-of-Squares semidefinite programming relaxation) capture spectral arguments. In fact, for many NP-hard optimization problems such as Max-Cut, graph coloring, and more, the best known spectral algorithms obtain far weaker approximation guarantees than the best semidefinite programs (see for example [10] versus [4]).

However, in the average case, this gap between semidefinite programming and spectral algorithms seems to disappear. A recent line of work has shown that the reverse is also true for many average-case problems: spectral algorithms are just as powerful as Sum-of-Squares semidefinite programming relaxations for planted clique [2, 3], refuting random constraint satisfaction problems [1, 5, 7, 8, 9], finding maxima of polynomials with random coefficients [6], and more.

In this talk, I will discuss a recent result which shows the equivalence of SoS and spectral algorithms is not a coincidence, and can be shown in a black-box fashion for a broad class of average-case problems. By combining convex duality arguments with simple Fourier-analysis, we show that average-case problems with solutions that are robust to random restriction cannot be well-approximated by the Sum-of-Squares semidefinite program of size S unless there is a spectral algorithm with equal performance running in time $\mathrm{poly}(S)$.

References

[1] Sarah R. Allen, Ryan O'Donnell, and David Witmer. How to refute a random CSP. In *FOCS*, pages 689–708. IEEE Computer Society, 2015.

[2] Noga Alon, Michael Krivelevich, and Benny Sudakov. Finding a large hidden clique in a random graph. In *SODA*, pages 594–598. ACM/SIAM, 1998.

[3] Boaz Barak, Samuel B. Hopkins, Jonathan A. Kelner, Pravesh Kothari, Ankur Moitra, and Aaron Potechin. A nearly tight sum-of-squares lower bound for the planted clique problem. In *FOCS*, pages 428–437. IEEE Computer Society, 2016.

[4] Michel X. Goemans and David P. Williamson. .879-approximation algorithms for MAX CUT and MAX 2sat. In *STOC*, pages 422–431. ACM, 1994.

[5] Dima Grigoriev. Linear lower bound on degrees of positivstellensatz calculus proofs for the parity. *Theor. Comput. Sci.*, 259(1-2):613–622, 2001.

[6] Samuel B. Hopkins, Jonathan Shi, and David Steurer. Tensor principal component analysis via sum-of-square proofs. In *COLT*, volume 40 of *JMLR Workshop and Conference Proceedings*, pages 956–1006. JMLR.org, 2015.

[7] Pravesh K. Kothari, Ryuhei Mori, Ryan O'Donnell, and David Witmer. Sum of squares lower bounds for refuting any CSP. *CoRR*, abs/1701.04521, 2017.

[8] Prasad Raghavendra, Satish Rao, and Tselil Schramm. Strongly refuting random csps below the spectral threshold. *CoRR*, abs/1605.00058, 2016.

[9] Grant Schoenebeck. Linear level lasserre lower bounds for certain k-csps. In *FOCS*, pages 593–602. IEEE Computer Society, 2008.

[10] Luca Trevisan. Max cut and the smallest eigenvalue. *SIAM J. Comput.*, 41(6):1769–1786, 2012.

The Ideal Proof System and Proof Complexity Lower Bounds from Algebraic Circuit Complexity

Amir Shpilka
(joint work with Grochow-Pitassi and Forbes-Shpilka-Tzameret-Wigderson)

Propositional proof complexity aims to understand and analyze the computational resources required to prove propositional tautologies, in the same way that circuit complexity studies the resources required to compute boolean functions. A typical goal would be to establish, for a given proof system, super-polynomial lower bounds on the *size* of any proof of some propositional tautology. The seminal work of Cook and Reckhow [8] showed that this goal relates quite directly to fundamental hardness questions in computational complexity such as the NP vs. coNP question: establishing super-polynomial lower bounds for *every* propositional proof system would separate NP from coNP (and thus also P from NP). We refer the reader to Krajíček [13] for more on this subject.

Propositional proof systems come in a large variety, as different ones capture different forms of reasoning, either reasoning used to actually prove theorems, or reasoning used by algorithmic techniques for different types of search problems (as failure of the algorithm to find the desired object constitutes a proof of its nonexistence). Much of the research in proof complexity deals with propositional proof systems originating from logic or geometry. Logical proof systems include such systems as *resolution* (whose variants are related to popular algorithms for automated theory proving and SAT solving), as well as the *Frege* proof system (capturing the most common logic text-book systems) and its many subsystems. Geometric proof systems include *cutting-plane proofs*, capturing reasoning used in algorithms for integer programming, as well as proof systems arising from systematic strategies for rounding linear- or semidefinite-programming such as the *lift-and-project* or *sum-of-squares* hierarchies.

In this talk we focus on algebraic proof systems, in which propositional tautologies (or rather contradictions) are expressed as unsatisfiable systems of polynomial equations and algebraic tools are used to refute them. This study originates with the work of Beame, Impagliazzo, Krajíček, Pitassi and Pudlák [3], who introduced the Nullstellensatz refutation system (based on Hilbert's Nullstellensatz), followed by the Polynomial Calculus system of Clegg, Edmonds, and Impagliazzo [5], which is a "dynamic" version of Nullstellensatz. In both systems the main measures of proof size that have been studied are the *degree* and *sparsity* of the polynomials appearing in the proof. Substantial work has lead to a very good understanding of the power of these systems with respect to these measures (see for example [1, 2, 4, 11, 12, 14] and references therein).

However, the above measures of degree and sparsity are rather rough measures of a complexity of a proof. As such, Grochow and Pitassi [9] have recently advocated measuring the complexity of such proofs by their algebraic circuit size and shown that the resulting proof system can polynomially simulate strong proof systems such as the Frege system. This naturally leads to the question of establishing

lower bounds for this stronger proof system, even for restricted classes of algebraic circuits.

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 [9], 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. All of the subsystems considered in this talk can simulate the well-studied *Nullstellensatz* proof system, and prior to our 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.

Our first method is a *functional lower bound*, a notion of Grigoriev and Razborov [10], which is a function $\hat{f} : \{0,1\}^n \to \mathbb{F}$ such that any polynomial f agreeing with $\hat{f}$ on the boolean cube requires large algebraic circuit complexity. For our classes of interest, we develop functional lower bounds where $\hat{f}(\overline{x})$ equals $1/p(\overline{x})$ where p is a constant-degree polynomial, which in turn yield corresponding IPS lower bounds for proving that p is nonzero over the boolean cube. In particular, we show super-polynomial lower bounds for refuting variants of the subset-sum axiom in various IPS subsystems.

Our second method is to give *lower bounds for multiples*, that is, to give explicit polynomials whose all (nonzero) multiples require large algebraic circuit complexity. By extending known techniques, we are able to obtain such lower bounds for our classes of interest, which we then use to derive corresponding IPS lower bounds. Such lower bounds for multiples are of independent interest, as they have tight connections with the algebraic hardness versus randomness paradigm.

References

[1] Michael Alekhnovich and Alexander A. Razborov. Lower bounds for polynomial calculus: Non-binomial case. In *Proceedings of the 42nd Annual IEEE Symposium on Foundations of Computer Science (FOCS 2001)*, pages 190–199, 2001.

[2] Samuel R. Buss, Dima Grigoriev, Russell Impagliazzo, and Toniann Pitassi. Linear gaps between degrees for the polynomial calculus modulo distinct primes. *J. Comput. Syst. Sci.*,

62(2):267–289, 2001. Preliminary version in the *14th Annual IEEE Conference on Computational Complexity (CCC 1999)*.

[3] Paul Beame, Russell Impagliazzo, Jan Krajíček, Toniann Pitassi, and Pavel Pudlák. Lower bounds on Hilbert's Nullstellensatz and propositional proofs. *Proc. London Math. Soc. (3)*, 73(1):1–26, 1996. Preliminary version in the *35th Annual IEEE Symposium on Foundations of Computer Science (FOCS 1994)*.

[4] Samuel R. Buss, Russell Impagliazzo, Jan Krajíček, Pavel Pudlák, Alexander A. Razborov, and Jiří Sgall. Proof complexity in algebraic systems and bounded depth Frege systems with modular counting. *Computational Complexity*, 6(3):256–298, 1996.

[5] Matthew Clegg, Jeff 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 1996)*, pages 174–183, 1996.

[6] Stephen A. Cook and Robert A. Reckhow. On the lengths of proofs in the propositional calculus (preliminary version). In *Proceedings of the 6th Annual ACM Symposium on Theory of Computing (STOC 1974)*, pages 135–148, 1974. For corrections see Cook-Reckhow [7].

[7] Stephen A. Cook and Robert A. Reckhow. Corrections for "On the lengths of proofs in the propositional calculus (preliminary version)". *SIGACT News*, 6(3):15–22, July 1974.

[8] Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. *J. Symb. Log.*, 44(1):36–50, 1979. This is a journal-version of Cook-Reckhow [6] and Reckhow [15].

[9] Joshua A. Grochow and Toniann Pitassi. Circuit complexity, proof complexity, and polynomial identity testing. In *Proceedings of the 55th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2014)*, pages 110–119, 2014. Full version at `arXiv:abs/1404.3820`.

[10] Dima Grigoriev and Alexander A. Razborov. Exponential lower bounds for depth 3 arithmetic circuits in algebras of functions over finite fields. *Appl. Algebra Eng. Commun. Comput.*, 10(6):465–487, 2000. Preliminary version in the *39th Annual IEEE Symposium on Foundations of Computer Science (FOCS 1998)*.

[11] 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 1998)*, pages 648–652, 1998.

[12] 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. Preliminary version in the Electronic Colloquium on Computational Complexity (ECCC), Technical Report TR97-042.

[13] Jan Krajíček. *Bounded arithmetic, propositional logic, and complexity theory*, volume 60 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1995.

[14] Alexander A. Razborov. Lower bounds for the polynomial calculus. *Computational Complexity*, 7(4):291–324, 1998.

[15] Robert A. Reckhow. *On the lengths of proofs in the propositional calculus*. PhD thesis, University of Toronto, 1976.

From Proofs to Algorithms in Machine Learning

David Steurer

(joint work with Boaz Barak, Sam Hopkins, Jon Kelner, Pravesh Kothari, Tengyu Ma, Aaron Potechin, Tselil Schramm and Jonathan Shi)

A common theme in several recent works is that proofs in restricted proof systems like sum-of-squares, can inform the design of efficient algorithms, especially for the kind of estimation problems that arise in statistics and machine learning. To

illustrate this theme, we discuss the examples of tensor completion, dictionary learning, and community detection.

Based on joint works with Boaz Barak, Sam Hopkins, Jon Kelner, Tengyu Ma, Aaron Potechin, Tselil Schramm, and Jonathan Shi [1, 2, 3, 4, 5].

References

[1] Boaz Barak, Jonathan A. Kelner, and David Steurer. Dictionary learning and tensor decomposition via the sum-of-squares method. In *STOC*, pages 143–151. ACM, 2015.
[2] Samuel B. Hopkins and David Steurer. Bayesian estimation from few samples: community detection and related problems. Submitted, 2017.
[3] Tengyu Ma, Jonathan Shi, and David Steurer. Polynomial-time tensor decompositions with sum-of-squares. In *FOCS*, pages 438–446. IEEE Computer Society, 2016.
[4] Aaron Potechin and David Steurer. Exact tensor completion with sum-of-squares. In *COLT*, volume 65 of *Proceedings of Machine Learning Research*, pages 1619–1673. PMLR, 2017.
[5] Tselil Schramm and David Steurer. Fast and robust tensor decomposition with applications to dictionary learning. In *COLT*, volume 65 of *Proceedings of Machine Learning Research*, pages 1760–1793. PMLR, 2017.

Communication Amid Uncertainty

Madhu Sudan

The works of Boole [1], Turing [12] and Shannon [11] give us the amazing power to capture many intellectual processes mathematically! And among processes of interest is how human society aggregates knowledge. Individuals start by building on knowledge gained by others and add to it by their own observations and reason. The entire process is completely decentralized with many faulty ingredients, including individual entities, but perhaps the most dominant source of errors is the errors that occur while exchanging knowledge. Despite the abundance of such errors it is remarkable that much of this knowledge is essentially correct! This talk and the surrounding line of work is motivated by the question: "What are the features of our communication methods that lead to such robustness in the aggregation of information?" While the scope of this question is broad (and it is our hope that others will also investigate it in fuller breadth), our specific focus in this talk is on the role of shared context.

Much of the communication is made efficient by assuming that the parties involved share a large common context (be it language, mathematical tools, common knowledge etc.). But this context is shared only vaguely and no one piece of it seems crucial for the communication to succeed. In this talk I will focus on some of our efforts to abstract shared context in communication and ability to communicate effectively even when context is not perfectly shared using Yao's model of communication complexity [13] as a starting point. (See also [10].) In an attempt to connect to the theme of this workshop, I will also briefly introduce the concept of "contextual proofs"—where proofs are compressed by using (imperfectly) shared context ("we'll assume the reader is familiar with high school math") and the challenges that this seems to pose in communicating and verifying proofs—topics that we believe are ripe for further study using the tools of proof complexity.

This talk is based on a series of joint works. In the works with Juba [9], and Goldreich and Juba [6] we initiated this line of queries in the setting where the level of shared context was minimal and the emphasis was on the mere feasibility (rather than efficiency) of reliable communication. Subsequent works [2, 3, 4, 5, 7, 8] have attempted to isolate settings in the Yao model that emphasize the role of (perfectly) shared context in making communication short, and study the effect of weakening the sharing of context to some imperfect form.

References

[1] George Boole. *An Investigation of the Laws of Thought on Which are Founded the Mathematical Theories of Logic and Probabilities*. Macmillan. Reprinted by Dover Publications, NY, NY, 1958., 1854.

[2] Clément Louis Canonne, Venkatesan Guruswami, Raghu Meka, and Madhu Sudan. Communication with imperfectly shared randomness. In Tim Roughgarden, editor, *Proceedings of the 2015 Conference on Innovations in Theoretical Computer Science, ITCS 2015, Rehovot, Israel, January 11-13, 2015*, pages 257–262. ACM, 2015.

[3] Badih Ghazi, Elad Haramaty, Pritish Kamath, and Madhu Sudan. Compression in a distributed setting. In *Proceedings of* ITCS 2016, page (to appear), 2016.

[4] Badih Ghazi, Ilan Komargodski, Pravesh Kothari, and Madhu Sudan. Communication with contextual uncertainty. In Robert Krauthgamer, editor, *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2016, Arlington, VA, USA, January 10-12, 2016*, pages 2072–2085. SIAM, 2016.

[5] Badih Ghazi and Madhu Sudan. The power of shared randomness in uncertain communication. In Ioannis Chatzigiannakis, Piotr Indyk, Fabian Kuhn, and Anca Muscholl, editors, *44th International Colloquium on Automata, Languages, and Programming, ICALP 2017, July 10-14, 2017, Warsaw, Poland*, volume 80 of *LIPIcs*, pages 49:1–49:14. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2017.

[6] Oded Goldreich, Brendan Juba, and Madhu Sudan. A theory of goal-oriented communication. *Journal of the ACM*, 59(2):8, 2012.

[7] Elad Haramaty and Madhu Sudan. Deterministic compression with uncertain priors. *Algorithmica*, 76(3):630–653, 2016.

[8] Brendan Juba, Adam Tauman Kalai, Sanjeev Khanna, and Madhu Sudan. Compression without a common prior: an information-theoretic justification for ambiguity in language. In Bernard Chazelle, editor, *ICS*, pages 79–86. Tsinghua University Press, 2011.

[9] Brendan Juba and Madhu Sudan. Universal semantic communication I. In *Proceedings of the 2008 ACM International Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008*, pages 123–132. ACM, 2008.

[10] Eyal Kushilevitz and Noam Nisan. *Communication Complexity*. Cambridge University Press, 1997.

[11] Claude E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 623–656, 1948.

[12] Alan M. Turing. On computable numbers, with an application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society*, 2(42):230–265, 1936. A correction *ibid*, 43, 544-546.

[13] Andrew Chi-Chih Yao. Some complexity questions related to distributive computing (preliminary report). In Michael J. Fischer, Richard A. DeMillo, Nancy A. Lynch, Walter A. Burkhard, and Alfred V. Aho, editors, *Proceedings of the 11h Annual ACM Symposium on Theory of Computing, April 30 - May 2, 1979, Atlanta, Georgia, USA*, pages 209–213. ACM, 1979.

Random Resolution

Neil Thapen
(joint work with Pavel Pudlák)

The following system for refuting propositional CNFs was introduced in [2]. Let F be a CNF in variables $x_1, \dots, x_n$ and let $0 < \varepsilon < 1$.

Definition. An *ε-random resolution distribution*, or *ε-RR distribution*, of F is a probability distribution $\mathcal{D}$ on pairs $(B_i, \Pi_i)_{i \sim \mathcal{D}}$ such that

(1) for each $i \in \mathcal{D}$, B_i is a CNF in variables $x_1, \dots, x_n$ and Π_i is a resolution refutation of $F \wedge B_i$
(2) for every $\alpha \in \{0,1\}^n$, $\Pr_{i \sim \mathcal{D}}[B_i \text{ is satisfied by } \alpha] \geq 1 - \varepsilon$.

We will usually take $\varepsilon = 1/2$, although an amplification lemma means that the exact value ε is not important. The appearance of this definition in [2] is motivated by questions about formalizing approximate counting in bounded arithmetic, and is indirectly related to the problem of separating the levels of constant-depth Frege.

The system is sound and complete. On the other hand, it is not a propositional proof system in the sense of Cook and Reckhow [3], because it is defined by a semantic condition that cannot be tested in polynomial time, unless $\mathsf{P} = \mathsf{NP}$. Nevertheless it makes sense to compare the complexity of proofs in it with proofs in the standard proof systems, in particular with resolution and bounded depth Frege.

We show some simple upper bounds. Random 3-CNFs have constant size 1/2-RR refutations, and rWPHP, a version of the weakpigeonhole principle, has polynomial size, polylogarithmic width 1/2-RR refutations.

The main problem about the system posed in [2] is to find a CNF which has small refutations in constant depth Frege, but does not have polylogarithmic width 1/2-RR refutations. A partial version of this problem was solved in [1].

We solve the full problem by showing that the family CPLS_n of CNFs based on the *coloured polynomial local search* principle [4], which has polynomial size resolution refutations, requires large width in 1/2-RR. We also define a family CPLS^2_n which has polynomial size Res(2) refutations, and show that it requires exponential size in 1/2-RR.

The lower bounds follow from constructing suitable random restrictions and proving a lemma that looks like a simple version of the switching lemma: that every small-width CNF, with polynomially high probability, is either falsified or unfalsifiable (over a well-behaved set of partial assignments) after a random restriction.

References

[1] Albert Atserias and Neil Thapen. *The Ordering Principle in a Fragment of Approximate Counting.* ACM Transactions on Computational Logic 15:4, article 29, 2014.
[2] Samuel Buss, Leszek Aleksander Kołodziejczyk and Neil Thapen. *Fragments of approximate counting.* Journal of Symbolic Logic 79:2, pp. 496-525, 2014.

[3] Stephen Cook and Robert Reckhow. *The relative efficiency of propositional proof systems.* Journal of Symbolic Logic 44:1, pp. 36-50, 1979.
[4] Jan Krajíček, Alan Skelley and Neil Thapen. *NP search problems in low fragments of bounded arithmetic.* Journal of Symbolic Logic 72:2, pp. 649-672, 2007.

Hardness Escalation in the Sherali-Adams Hierarchy (From Weak to Strong LP Gaps for all CSPs)

Madhur Tulsiani
(joint work with Mrinalkanti Ghosh)

This work studies the approximability of constraint satisfaction problems (CSPs) by linear programming (LP) relaxations. We show that for every CSP, the approximation obtained by a basic LP relaxation, is no weaker than the approximation obtained using relaxations given by $\Omega\left(\frac{\log n}{\log\log n}\right)$ levels of the Sherali-Adams hierarchy on instances of size n. Equivalently, a lower bound for the basic LP (captured by the lowest level of the Sherali-Adams hierarchy) can be escalated to a lower bound for $\Omega\left(\frac{\log n}{\log\log n}\right)$ levels of the hierarchy.

It was proved by Chan et al.[1] (and recently strengthened by Kothari, Meka and Raghavendra [3]) that for CSPs, any polynomial size LP extended formulation is no stronger than relaxations obtained by a super-constant levels of the Sherali-Adams hierarchy. Combining this with our result also implies that any polynomial size LP extended formulation is no stronger than simply the *basic* LP, which can be thought of as the base level of the Sherali-Adams hierarchy. This essentially gives a dichotomy result for approximation of CSPs by polynomial size LP extended formulations.

Using our techniques, we also simplify and strengthen the result by Khot, Worah and the second author [2] on (strong) approximation resistance for LPs. They provided a necessary and sufficient condition under which $\Omega(\log\log n)$ levels of the Sherali-Adams hierarchy cannot achieve an approximation better than a random assignment. We simplify their proof and strengthen the bound to $\Omega\left(\frac{\log n}{\log\log n}\right)$ levels.

References

[1] Siu On Chan, James R. Lee, Prasad Raghavendra, and David Steurer. Approximate constraint satisfaction requires large LP relaxations. In *Proceedings of the 54th IEEE Symposium on Foundations of Computer Science*, pages 350–359, Washington, DC, USA, 2013. IEEE Computer Society.
[2] Subhash Khot, Madhur Tulsiani, and Pratik Worah. A characterization of strong approximation resistance. In *Proceedings of the 46th ACM Symposium on Theory of Computing*, pages 634–643, New York, NY, USA, 2014. ACM.
[3] Pravesh Kothari, Raghu Meka, and Prasad Raghavendra. Approximating rectangles by juntas and weakly-exponential lower bounds for LP relaxations of CSPs. In *Proceedings of the 49th ACM Symposium on Theory of Computing*, 2017.

Resolution over Linear Equations: Survey and Open Problems

Iddo Tzameret

Recently, extensions of resolution that operate with linear equations instead of literals gained quite a lot of attention in proof complexity research. This refutation system is interesting both on its own merit as a "minimal" extension of resolution with counting gates, as well as from the perspective of lower bounds questions, since it is the "weakest" subsystem of $\mathsf{AC}^0[q]$-Frege for which no lower bounds are known to date. Thus, establishing lower bounds on (dag-like, unrestricted) resolution over linear equations modulo q can be viewed as a step towards $\mathsf{AC}^0[q]$-Frege lower bounds, a problem that is open for decades.

This talk surveys briefly lower and upper bounds on (mostly restricted versions of) resolution over linear equations. We will focus on cases when the linear equations are over the two element field $\mathbb{F}_2$, and over the integers $\mathbb{Z}$. We then describe important open problems concerning this refutation system as well as possible approaches considered recently to solve these problems.

Raz and Tzameret [8] introduced the *resolution over linear equation* refutation system, denoted $\mathrm{R}(\mathrm{lin}_{\mathfrak{R}})$, where the linear equations are over a ring $\mathfrak{R}$ ([8] considered only the case $\mathfrak{R} = \mathbb{Z}$). The system is defined as follows:

Definition 2 ($\mathrm{R}(\mathrm{lin}_{\mathfrak{R}})$)**.** *Let $K := \{K_1, \ldots, K_m\}$ be a collection of disjunctions of linear equations over the ring $\mathfrak{R}$ and variables $x_1, \ldots, x_n$. An* $\mathrm{R}(\mathrm{lin}_{\mathfrak{R}})$*-proof from K of a disjunction of linear equations D is a finite sequence $\pi = (D_1, \ldots, D_\ell)$ of disjunctions of linear equations, such that $D_\ell = D$ and for every $i \in [\ell]$, either $D_i = K_j$ for some $j \in [m]$, or D_i is the* Boolean axiom *$(x_h = 0) \vee (x_h = 1)$ for some $h \in [n]$, or D_i was derived by one of the following inference rules, using D_j, D_k for some $j, k < i$:*

- **Resolution:** *Let A, B be two, possibly empty, disjunctions of linear equations and let L_1, L_2 be two linear equations. From $A \vee L_1$ and $B \vee L_2$ derive $A \vee B \vee (L_1 - L_2)$.*
- **Weakening:** *From a, possibly empty, disjunction of linear equations A derive $A \vee L$, where L is an arbitrary linear equation over X.*
- **Simplification:** *From $A \vee (0 = k)$ derive A, where A is a, possibly empty, disjunction of linear equations and $k \neq 0$.*

An $\mathrm{R}(\mathrm{lin}_{\mathfrak{R}})$ *refutation of a collection of disjunctions of linear equations K is a proof of the empty disjunction from K.*

The *size* of an $\mathrm{R}(\mathrm{lin}_{\mathfrak{R}})$ proof π is the total size of all the disjunctions of linear equations in π, where coefficients are written in *unary* representation.

We state some known upper bounds, simulations and restricted lower bounds for $\mathrm{R}(\mathrm{lin}_{\mathbb{Z}})$ refutations. We write $\mathrm{R}(\mathrm{lin}_{\mathfrak{R}}) \vdash^* \tau$ to denote that τ has a polynomial-size refutation in $\mathrm{R}(\mathrm{lin}_{\mathfrak{R}})$.

(1) $\mathrm{R}(\mathrm{lin}_{\mathbb{Z}}) \vdash^* m$-to-$n$ Pigeonhole Principle, for any $m > n$ (written as a CNF) [8];
(2) $\mathrm{R}(\mathrm{lin}_{\mathbb{Z}}) \vdash^*$ Tseitin (mod q) (written as a CNF) [8];

(3) $\mathrm{R}(\mathrm{lin}_{\mathbb{Z}})$ simulates Cutting Planes with coefficients written in *unary*, as well as R(CP*) introduced by Krajíček [4]. The latter system extends Cutting Planes to operate with disjunctions of linear inequalities with coefficients written in unary.
(4) [8] also showed *exponential lower bounds* on restrictions of $\mathrm{R}(\mathrm{lin}_{\mathbb{Z}})$ where the disjunctions in each proof-line have only constant many distinct linear forms (excluding single variables, that can occur freely), and where coefficients of variables are bounded by some global constant.

Itsykson and Sokolov [3] studied the system $\mathrm{R}(\mathrm{lin}_{\mathbb{F}_2})$. They obtained lower bounds for tree-like $\mathrm{R}(\mathrm{lin}_{\mathbb{F}_2})$ refutations. Note that in the case of $\mathrm{R}(\mathrm{lin}_{\mathbb{F}_2})$ there is no need to have the Boolean axioms. We provide a partial list of what is known about $\mathrm{R}(\mathrm{lin}_{\mathbb{F}_2})$:

(1) $\mathrm{R}(\mathrm{lin}_{\mathbb{Z}})$ simulates $\mathrm{R}(\mathrm{lin}_{\mathbb{F}_2})$ [3];
(2) Let $A\mathbf{x} = \mathbf{b}$ be an unsatisfiable system of linear equations over $\mathbb{F}_2$. Then, tree-like $\mathrm{R}(\mathrm{lin}_{\mathbb{F}_2}) \vdash^* A\mathbf{x} = \mathbf{b}$ [3];
(3) Tree-like $\mathrm{R}(\mathrm{lin}_{\mathbb{F}_2}) \vdash^*$ Graph Matching Principle [3].

Loosely speaking, this means that tree-like $\mathrm{R}(\mathrm{lin}_{\mathbb{F}_2})$ captures basic modulo 2 arguments. Itsykson-Sokolov [3] characterized tree-like $\mathrm{R}(\mathrm{lin}_{\mathbb{F}_2})$ refutations as *linear decision trees*, which are decision trees that query linear equations modulo 2 in the nodes, and terminates at leaves determining which of the initial clauses of an unsatisfiable CNF falsifies the given truth-assignment.

(4) Exponential lower bounds on tree-like $\mathrm{R}(\mathrm{lin}_{\mathbb{F}_2})$ refutations of the $n+1$ to n Pigeonhole Principle [3].

This lower bound is obtained via a Prover-Delayer game approach (similar to Pudlák-Impagliazzo [7]).
The main problem left open: *Prove super-polynomial lower bounds on (dag-like, unrestricted)* $\mathrm{R}(\mathrm{lin}_{\mathbb{F}_2})$ refutations.

Several groups of researchers have been trying recently to approach such a lower bound:

(1) *Algebraic approach*: depth-3 IPS over $\mathbb{F}_2$ (where IPS is the Ideal Proof System from Grochow-Pitassi [2]) can be shown to simulate tree-like $\mathrm{R}(\mathrm{lin}_{\mathbb{F}_2})$; similarly, depth-4 IPS is expected to simulate dag-like $\mathrm{R}(\mathrm{lin}_{\mathbb{F}_2})$ (this is due to ongoing work by the speaker together with Fedor Part). This lends itself to the possibility to achieve lower bounds on $\mathrm{R}(\mathrm{lin}_{\mathbb{F}_2})$ refutations via low depth IPS over finite fields lower bounds (lower bounds on several fragments of IPS have already been shown in Forbes *et al.* [1]).
(2) *Feasible monotone interpolation approach*: Krajíček [5] and Krajíček-Oliveira [6] considered the possibility of reducing the lower bound task of $\mathrm{R}(\mathrm{lin}_{\mathbb{F}_2})$ to proving monotone circuits lower bounds. The monotone circuit class obtained, for which lower bounds would entail $\mathrm{R}(\mathrm{lin}_{\mathbb{F}_2})$ lower bounds, is the class of *monotone circuits with oracles*, which naturally is stronger than standard monotone circuits.

(3) *Communication complexity approach:* Sokolov [9] defined a dag-like communication protocol, on which lower bounds would imply lower bounds on $\mathrm{R}(\mathrm{lin}_{\mathbb{F}_2})$ refutations, in a similar way that standard (tree-like) communication protocols entail tree-like $\mathrm{R}(\mathrm{lin}_{\mathbb{F}_2})$ lower bounds.

References

[1] Michael A. Forbes, Amir Shpilka, Iddo Tzameret, and Avi Wigderson. Proof complexity lower bounds from algebraic circuit complexity. In *31st Conference on Computational Complexity, CCC 2016, May 29 to June 1, 2016, Tokyo, Japan*, pages 32:1–32:17, 2016.

[2] Joshua A. Grochow and Toniann Pitassi. Circuit complexity, proof complexity, and polynomial identity testing. In *55th Annual IEEE Symposium on Foundations of Computer Science, FOCS*, 2014. Also available as arXiv:1404.3820 [cs.CC].

[3] Dmitry Itsykson and Dmitry Sokolov. Lower bounds for splittings by linear combinations. In *Proc. of Math. Found. Comp. Sci. 2014–39th Intl. Symp., MFCS 2014, Proceedings*, pages 372–383, 2014.

[4] Jan Krajíček. Discretely ordered modules as a first-order extension of the cutting planes proof system. *The Journal of Symbolic Logic*, 63(4):1582–1596, 1998.

[5] Jan Krajícek. Randomized feasible interpolation and monotone circuits with a local oracle. *CoRR*, abs/1611.08680, 2016.

[6] Jan Krajícek and Igor Carboni Oliveira. On monotone circuits with local oracles and clique lower bounds. *CoRR*, abs/1704.06241, 2017.

[7] Pavel Pudlák and Russell Impagliazzo. A lower bound for DLL algorithms for k-sat (preliminary version). In *Proceedings of the Eleventh Annual ACM-SIAM Symposium on Discrete Algorithms, January 9-11, 2000, San Francisco, CA, USA.*, pages 128–136, 2000.

[8] Ran Raz and Iddo Tzameret. Resolution over linear equations and multilinear proofs. *Ann. Pure Appl. Logic*, 155(3):194–224, 2008.

[9] Dmitry Sokolov. Dag-like communication and its applications. In *Computer Science - Theory and Applications - 12th International Computer Science Symposium in Russia, CSR 2017, Kazan, Russia, June 8-12, 2017, Proceedings*, pages 294–307, 2017.

Regular and General Resolution Width

Alasdair Urquhart

It is known that the size of regular and general resolution refutations can differ widely. It can be shown [3] that there is a sequence of sets of clauses Π_1, $\Pi_2, \ldots, \Pi_i, \ldots$ for which the minimum regular resolution refutation of Π_i has size $2^{\Omega(R_i/(\log R_i)^7 \log\log R_i)}$, where R_i is the minimum size of an unrestricted resolution refutation of Π_i. However, for some well known examples, such as the graph-based clauses of Tseitin [2] or the pigeonhole principle [1], the shortest known resolution refutations are regular, and it is a plausible conjecture that in these cases, the minimal refutations are always regular.

This conjecture seems to remain open, but it is possible to prove a similar result for resolution width. This paper shows that the regular and general resolution width coincide for the two cases above, though in the general case [3], unrestricted and regular resolution width can diverge widely.

References

[1] Armin Haken. The intractability of resolution. *Theoretical Computer Science*, 39:297–308, 1985.

[2] Grigorii S. Tseitin. On the complexity of derivation in propositional calculus. In A. O. Slisenko, editor, *Studies in Constructive Mathematics and Mathematical Logic, Part 2*, pages 115–125. Consultants Bureau, New York, 1970.

[3] Alasdair Urquhart. A near-optimal separation of regular and general resolution. *SIAM Journal on Computing*, 40:107–121, 2011.

How Limited Interaction Hinders Real Communication

Marc Vinyals

(joint work with Susanna F. de Rezende and Jakob Nordström)

In resolution, which is arguably the most well-studied proof system in proof complexity, the input is an unsatisfiable formula in conjunctive normal form (CNF) and new disjunctive clauses are derived from this formula until an explicit contradiction is reached (in the form of the empty clause without literals). The question of time-space trade-offs for resolution was first raised by Ben-Sasson [4], who also obtained such trade-offs for the restricted subsystem of tree-like resolution. Size-space trade-offs for general, unrestricted resolution were later shown in [2, 3, 6, 18].

One can obtain exponential lower bounds on proof size (corresponding to running time) for proofs in sublinear but polynomial space [6, 18], and results in [2, 3] even exhibit trade-offs where size has to be superpolynomial and space has to be superlinear simultaneously. These results are true trade-offs in the sense that it is actually possible to refute the formulas both in small size and in small space, only not simultaneously. A third nice feature of the trade-offs are that the upper bounds are on proof size and total space, whereas the (sometimes tightly matching) lower bounds are on length and line space, meaning that one only charges one time unit for each derivation step regardless of its complexity, and only one space unit per "formula" (for resolution: per clause) regardless of how large it is. Thus, the upper bounds are algorithmically achievable, while the lower bounds hold in a significantly stronger model.

A stronger proof system than resolution is polynomial calculus [1, 8], where the clauses of a formula are translated to multilinear polynomials and calculations inside the ideal generated by these polynomials (basically corresponding to a Gröbner basis computation) establishes unsatisfiability. The first size-space trade-offs for polynomial calculus—which were not true trade-offs in the sense discussed above, however—were obtained in [16], and these results were further improved in [3] to true trade-offs essentially matching the results cited above for resolution except for a small loss in parameters.

Another proof system that is also stronger than resolution and that has been the focus of much research is cutting planes [9], which formalizes the integer linear programming algorithm in [7, 13]. In cutting planes the clauses of a CNF formula

are translated to linear inequalities, which are then manipulated to derive a contradiction. Thus, the question of Boolean satisfiability is reduced to the geometry of polytopes over the real numbers. Cutting planes is much more poorly understood than resolution and polynomial calculus, however, and size-space trade-offs have proven elusive. The results in [16] apply not only to resolution and polynomial calculus but also to cutting planes, and were improved further in [14] to hold for even stronger proof systems, but unfortunately are not true trade-offs in the sense discussed above.

The problem is that what is shown in [14, 16] is only that proofs in small space for certain formulas have to be very large, but it is not established that these formulas can be refuted space-efficiently. In fact, for resolution it can be shown using techniques from [5] that such small-space proofs provably do not exist, and for polynomial calculus there is circumstantial evidence for a similar claim. This turns out to be an inherent limitation of the technique used.

In a recent surprising paper [12], it was shown that cutting planes can refute any formula in *constant* space if we only count the number of lines or formulas. Plugging this result into [14, 16] yields a trade-off of sorts, since "small-space" proofs will always exist, but the catch is that such proofs will have exponentially large coefficients. This means that these trade-offs do not seem very "algorithmically relevant" in the sense that such proofs could hardly be found in practice, and saying that a proof with exponential-size coefficients has "constant space" somehow does not feel quite right.

We obtain the first true size-space trade-offs for the cutting planes proof system, where the upper bounds hold for size and total space for derivations with constant-size coefficients, and the lower bounds apply to length and line space (i.e., number of inequalities in memory) even for derivations with exponentially large coefficients. These are also the first trade-offs to hold uniformly for resolution, polynomial calculus and cutting planes, thus capturing the main methods of reasoning used in current state-of-the-art SAT solvers.

We prove our results by a reduction to communication lower bounds in a round-efficient version of the real communication model of Krajíček [17], drawing on and extending techniques by Raz and McKenzie [19] and Göös et al. [15]. The communication lower bounds are in turn established by a reduction to trade-offs between cost and number of rounds in the game of Dymond and Tompa [11] played on directed acyclic graphs.

As a by-product of the techniques developed to show these proof complexity trade-off results, we also obtain an exponential separation between $\mathsf{monotone\text{-}AC}^{i-1}$ and $\mathsf{monotone\text{-}AC}^{i}$, improving exponentially over the superpolynomial separation in [19]. That is, we give an explicit Boolean function that can be computed by monotone Boolean circuits of depth $\log^i n$ and polynomial size, but for which circuits of depth $\mathrm{O}(\log^{i-1} n)$ require exponential size.

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] Paul Beame, Chris Beck, and Russell Impagliazzo. Time-space tradeoffs in resolution: Superpolynomial lower bounds for superlinear space. *SIAM Journal on Computing*, 45(4):1612–1645, August 2016. Preliminary version in *STOC '12*.

[3] Chris Beck, Jakob Nordström, and Bangsheng Tang. Some trade-off results for polynomial calculus. In *Proceedings of the 45th Annual ACM Symposium on Theory of Computing (STOC '13)*, pages 813–822, May 2013.

[4] Eli Ben-Sasson. Size-space tradeoffs for resolution. *SIAM Journal on Computing*, 38(6):2511–2525, May 2009. Preliminary version in *STOC '02*.

[5] Eli Ben-Sasson and Jakob Nordström. Short proofs may be spacious: An optimal separation of space and length in resolution. In *Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science (FOCS '08)*, pages 709–718, October 2008.

[6] Eli Ben-Sasson and Jakob Nordström. Understanding space in proof complexity: Separations and trade-offs via substitutions. In *Proceedings of the 2nd Symposium on Innovations in Computer Science (ICS '11)*, pages 401–416, January 2011.

[7] Vašek Chvátal. Edmonds polytopes and a hierarchy of combinatorial problems. *Discrete Mathematics*, 4(1):305–337, 1973.

[8] 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.

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

[10] 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.

[11] Patrick W. Dymond and Martin Tompa. Speedups of deterministic machines by synchronous parallel machines. *Journal of Computer and System Sciences*, 30(2):149–161, April 1985. Preliminary version in *STOC '83*.

[12] Nicola Galesi, Pavel Pudlák, and Neil Thapen. The space complexity of cutting planes refutations. In *Proceedings of the 30th Annual Computational Complexity Conference (CCC '15)*, volume 33 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 433–447, June 2015.

[13] 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.

[14] 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.

[15] Mika Göös, Toniann Pitassi, and Thomas Watson. Deterministic communication vs. partition number. In *Proceedings of the 56th Annual IEEE Symposium on Foundations of Computer Science (FOCS '15)*, pages 1077–1088, October 2015.

[16] 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.

[17] Jan Krajíček. Interpolation by a game. *Mathematical Logic Quarterly*, 44:450–458, 1998.

[18] Jakob Nordström. A simplified way of proving trade-off results for resolution. *Information Processing Letters*, 109(18):1030–1035, August 2009. Preliminary version in ECCC report TR07-114, 2007.

[19] Ran Raz and Pierre McKenzie. Separation of the monotone NC hierarchy. *Combinatorica*, 19(3):403–435, March 1999. Preliminary version in *FOCS '97*.

Probabilistic Non-Interactive Proof Systems for Batch Computation, #SAT, and more

Ryan Williams

Let Multipoint Arithmetic Circuit Evaluation (MACE) be the task of evaluating an multivariate arithmetic circuit of size s (made of plus and times gates) on s arbitrary inputs. We present a non-interactive probabilistic proof system for MACE which saves roughly a quadratic factor over the obvious $O(s^2)$ time algorithm when the circuit has low degree. One corollary is that there is such a proof system for counting SAT assignments to arbitrary Boolean formulas of n variables and $2^{o(n)}$ size, where the proofs are of length about $2^{n/2+o(n)}$ and the proofs can be verified (using $O(n)$ random bits) in about $2^{n/2+o(n)}$ time with high confidence. In particular, UNSAT for arbitrary Boolean formulas can be verified by proofs of this length and with this running time. This result strongly refutes a "Merlin-Arthur Strong Exponential Time Hypothesis" which had been informally conjectured in the theory community. (Previously appeared in the 2016 Computational Complexity Conference [1].)

References

[1] Ryan Williams. Strong ETH Breaks With Merlin and Arthur: Short Non-Interactive Proofs of Batch Evaluation. In *31st Computational Complexity Conference*, 2:1–2:17, 2016.

Reporter: Susanna F. de Rezende