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-1641185, "US Junior Oberwolfach Fellows".

Workshop: Proof Complexity and Beyond

Table of Contents

Albert Atserias
Selected Topics on Semialgebraic Proof Complexity 2309

Paul Beame (joint with Vincent Liew)
Verifying Multipliers in Resolution 2310

Christoph Berkholz (joint with Jakob Nordström)
Resolution Trade-Offs for XOR-Formulas with Applications to Finite Variable Logics and the Weisfeiler-Leman Algorithm 2312

Olaf Beyersdorff (joint with Joshua Blinkhorn and Luke Hinde)
Proof Complexity of Quantified Boolean Formulas 2313

Stefan Dantchev (joint with Joshua Blinkhorn and Luke Hinde)
Randomised Approximate Proofs 2315

Anuj Dawar (joint with Matthew Anderson, Bjarki Holm and Pengming Wang)
The Symmetry Gap in Combinatorial Optimization 2316

Susanna F. de Rezende (joint with Albert Atserias, Ilario Bonacina, Massimo Lauria, Jakob Nordström and Alexander Razborov)
k-Clique is Hard on Average for Regular Resolution 2317

Noah Fleming (joint with Denis Pankratov, Toniann Pitassi and Robert Robere)
Random $O(\log n)$-CNF formulas Are Hard for Cutting Planes 2318

Venkatesan Guruswami (joint with Vijay Bhattiprolu, Mrinalkanti Ghosh, Euiwoong Lee, and Madhur Tulsiani)
Sum-of-Squares Certificates of Maxima of Polynomials over the Sphere . 2320

Johan Håstad
On Small-Depth Frege Proofs for Tseitin for Grids 2321

Dmitry Itsykson (joint with Sam Buss, Alexander Knop and Dmitry Sokolov)
Some Separations for OBDD-Based Proof Systems 2323

Pravesh Kothari (joint with Ryuhei Mori, Ryan O'Donnell and David Witmer)
Optimal Sum-of-Squares Thresholds for Refuting Random CSPs 2324

Massimo Lauria (joint with Jakob Nordström)
Graph Colouring is Hard for Algorithms Based on Hilbert's Nullstellensatz and Gröbner Bases 2325

James Lee
Do You Even Lift? 2327

Ryan O'Donnell
When SOS Fails (Maybe It's Because Everything Fails) 2329

Joanna Ochremiak (joint with Albert Atserias)
Proof Complexity Meets Algebra 2331

Pablo A. Parrilo
Sum of Squares Methods: Beyond 0/1 2333

Toniann Pitassi
Part I: Proof Complexity Primer
Part II: Lifting in Communication Complexity and Proof Complexity . . 2335

Aaron Potechin (joint with David Steurer)
Exact Tensor Completion with Sum-of-Squares 2336

Pavel Pudlak
The Canonical NP-Pairs of Bounded Depth Frege Systems 2337

Annie Raymond (joint with James Saunderson, Mohit Singh, and Rekha Thomas)
Symmetric Sums of Squares over k-Subset Hypercubes 2338

Robert Robere (joint with Toniann Pitassi)
Unified and Optimal Lower Bounds for Monotone Computation 2340

Tselil Schramm (joint with Sam Hopkins, Pravesh Kothari, Aaron Potechin, Prasad Raghavendra and David Steurer)
Duality of Low-Degree SoS Refutations and Efficient Spectral Algorithms in the Average Case 2342

Amir Shpilka (joint with Grochow-Pitassi and Forbes-Shpilka-Tzameret-Wigderson)
The Ideal Proof System and Proof Complexity Lower Bounds from Algebraic Circuit Complexity 2343

David Steurer (joint with Boaz Barak, Sam Hopkins, Jon Kelner, Pravesh Kothari, Tengyu Ma, Aaron Potechin, Tselil Schramm and Jonathan Shi)
From Proofs to Algorithms in Machine Learning 2345

Madhu Sudan
Communication Amid Uncertainty 2346

Neil Thapen (joint with Pavel Pudlák)
Random Resolution 2348

Madhur Tulsiani (joint with Mrinalkanti Ghosh)
Hardness Escalation in the Sherali-Adams Hierarchy (From Weak to Strong LP Gaps for all CSPs) 2349

Iddo Tzameret
Resolution over Linear Equations: Survey and Open Problems 2350

Alasdair Urquhart
Regular and General Resolution Width 2352

Marc Vinyals (joint with Susanna F. de Rezende and Jakob Nordström)
How Limited Interaction Hinders Real Communication 2353

Ryan Williams
Probabilistic Non-Interactive Proof Systems for Batch Computation, #SAT, and more 2356