Report from Dagstuhl Seminar 14421

Optimal Algorithms and Proofs

Edited by

Olaf Beyersdorff[1], Edward A. Hirsch[2], Jan Krajíček[3], and Rahul Santhanam[4]

1 **University of Leeds, GB,** o.beyersdorff@leeds.ac.uk
2 **Steklov Institute of Mathematics, St. Petersburg, RU,** edward.a.hirsch@gmail.com
3 **Charles University in Prague, CZ,** krajicek@karlin.mff.cuni.cz
4 **University of Edinburgh, GB,** rsanthan@inf.ed.ac.uk

Abstract

This report documents the programme and the outcomes of the Dagstuhl Seminar 14421 "Optimal algorithms and proofs". The seminar brought together researchers working in computational and proof complexity, logic, and the theory of approximations. Each of these areas has its own, but connected notion of optimality; and the main aim of the seminar was to bring together researchers from these different areas, for an exchange of ideas, techniques, and open questions, thereby triggering new research collaborations across established research boundaries.

Seminar October 12–17, 2014 – http://www.dagstuhl.de/14421
1998 ACM Subject Classification F.1.3 Complexity Measures and Classes, F.2.2 Nonnumerical Algorithms and Problems: Complexity of proof procedures, G.1.2 Approximation
Keywords and phrases computational complexity, proof complexity, approximation algorithms, optimal algorithms, optimal proof systems, speedup theorems
Digital Object Identifier 10.4230/DagRep.4.10.51
Edited in cooperation with Alexander Smal

1 Executive Summary

Olaf Beyersdorff
Edward A. Hirsch
Jan Krajíček
Rahul Santhanam

General Introduction to the Topic

The notion of optimality plays a major role in theoretical computer science. Given a computational problem, does there exist a "fastest" algorithm for it? Which proof system yields the shortest proofs of propositional tautologies? Is there a single distribution which can be used to inductively infer any computable sequence? Given a class of optimization problems, is there a single algorithm which always gives the best efficient approximation to the solution? Each of these questions is a foundational one in its area – the first in computational complexity, the second in proof complexity, the third in computational learning theory, and the last in the theory of approximation.

Consider, as an example, the Boolean Satisfiability (SAT) search problem, which asks, given a Boolean formula, for a satisfying assignment to the formula. Since SAT is NP-complete, being able to tell whether the fastest algorithm for SAT runs in polynomial time would imply a solution to the notoriously hard NP vs P problem, which is far beyond the state of our current knowledge. However, the possibility remains that we can define an *optimal* algorithm which we can guarantee to be essentially the fastest on every instance, even if we cannot rigorously analyze the algorithm. In a seminal paper, Leonid Levin (1973) proved that every NP search problem, and in particular SAT, has an optimal algorithm. It is still unknown whether every decision problem in NP has an optimal algorithm.

In general, given a class of computational artefacts (algorithms/proof systems/distributions) and performance measures for each artefact in the class, we say that an artefact is optimal if it matches the performance of every other artefact in every case. The main questions about optimality is: for which classes of artefacts and under which assumptions do they exist? In case they do exist, how well do they match the performance of other artefacts in the class? How is the existence of optimal artefacts related to other fundamental theoretical questions, such as complexity lower bounds, efficient learnability or approximability?

There have been a number of important recent results about optimality in various computational settings. Prime examples include optimal proof systems and acceptors under advice or in heuristic settings, surprising relations of optimal proof systems to descriptive complexity and parameterized complexity, hierarchy results in various computational settings, and optimal approximation algorithms for constraint satisfaction problems.

Organisation of the Seminar and Activities

The seminar brought together 41 researchers from different areas of computer science and mathematics such as computational complexity, proof complexity, logic, and approximations with complementary expertise, but common interest in different notions of optimality. The participants consisted of both senior and junior researchers, including a number of postdocs and a few advanced graduate students.

Participants were invited to present their work and to communicate state-of-the-art advances. Twenty-two talks of various lengths were given over the five-day workshop. Survey talks of 60 minutes were scheduled prior to workshop, covering the three main areas of computational complexity, proof complexity, and approximations. Most of the remaining slots were filled as the workshop commenced. In addition, during two spontaneously organised open problem sessions – one at the very start and the second, longer one near the end of the workshop – the participants posed a number of open problems across the different disciplines covered by the seminar. The organisers considered it important to leave ample free time for discussion.

Three tutorial talks were scheduled during the first two days in order to establish a common background for the different communities from computational complexity, proof complexity, logic, and approximation that came together for the workshop. The presenters and topics were:

- David Steurer: Survey on Approximations and Optimality
- Olaf Beyersdorff: Optimal Proof Systems – a Survey
- Rahul Santhanam: Hierarchies and Lower Bounds via Optimality – a Survey

The other 19 talks covered a broad range of topics from logic, computational complexity and proof complexity.

The organisers think that the seminar fulfilled their original high goals: most talks were a great success and many participants reported about the inspiring seminar atmosphere, fruitful interactions, and a generally positive experience. The organisers and participants wish to thank the staff and the management of Schloss Dagstuhl for their assistance and excellent support in the arrangement of a very successful and productive event.

2 Table of Contents

3 Overview of Talks

3.1 Optimal Proof Systems – a Survey

Olaf Beyersdorff (University of Leeds, GB)

This talk is a survey on optimal proof system. I will not cover any results in detail, but try to present the general picture of what is known and what to expect. The question whether optimal proof systems exist was first raised by Krajíček and Pudlák [9] and has been open since. In the talk I survey

1. Characterizations for the existence of optimal proof systems [1, 3, 4, 9, 10];
2. Sufficient and necessary conditions for their existence [6, 9];
3. Positive results in different models [2, 5, 11];
4. Connections to first-order logic [7, 8].

A longer exposition of the content of the talk is available as a guest post to Hunter Monroe's blog 'Speedup in Computational Complexity'.

References

1 Olaf Beyersdorff, Johannes Köbler, and Jochen Messner. Nondeterministic functions and the existence of optimal proof systems. *Theoretical Computer Science*, 410(38–40):3839–3855, 2009.
2 Olaf Beyersdorff, Johannes Köbler, and Sebastian Müller. Proof systems that take advice. *Information and Computation*, 209(3):320–332, 2011.
3 Olaf Beyersdorff and Zenon Sadowski. Do there exist complete sets for promise classes? *Mathematical Logic Quarterly*, 57(6):535–550, 2011.
4 Yijia Chen and Jörg Flum. From almost optimal algorithms to logics for complexity classes via listings and a halting problem. *J. ACM*, 59(4):17, 2012.
5 Edward A. Hirsch and Dmitry Itsykson. On optimal heuristic randomized semidecision procedures, with application to proof complexity. In *Proc. STACS'10*, pages 453–464, 2010.
6 Johannes Köbler, Jochen Messner, and Jacobo Torán. Optimal proof systems imply complete sets for promise classes. *Information and Computation*, 184(1):71–92, 2003.
7 Jan Krajíček. *Bounded Arithmetic, Propositional Logic, and Complexity Theory*, volume 60 of *Encyclopedia of Mathematics and Its Applications*. Cambridge University Press, 1995.
8 Jan Krajíček. *Forcing with random variables and proof complexity*, volume 382 of *Lecture Note Series*. London Mathematical Society, 2011.
9 Jan Krajíček and Pavel Pudlák. Propositional proof systems, the consistency of first order theories and the complexity of computations. *The Journal of Symbolic Logic*, 54(3):1063–1079, 1989.
10 Jochen Messner. On optimal algorithms and optimal proof systems. In *Proc. STACS'99*, pages 541–550, 1999.
11 Toniann Pitassi and Rahul Santhanam. Effectively polynomial simulations. In *Proc. 1st Innovations in Computer Science*, 2010.

3.2 Total Space in Resolution

Ilario Bonacina (University of Rome "La Sapienza", IT)

Joint work of Bonacina, Ilario; Galesi, Nicola; Thapen, Neil

Consider a resolution refutation of some unsatisfiable formula F. Such refutation could be presented on a blackboard with limited space. Initially the blackboard is empty and at each step of the presentation we can either: write on the blackboard some clause from F; apply the resolution rule to clauses already on the blackboard and write down the clause we get; erase some clause from the blackboard (in order to save space). The refutation ends when we can write the empty clause on the blackboard. The Total Space of F is the minimal size of a blackboard needed to present a refutation of F, where the size of a blackboard is intended to be the number of literals (counted with repetitions) it can contain.

We will show that some constant width formulas in n variables the blackboard must contain at least cn clauses each of width cn, for some constant $c > 0$. Hence require Total Space $\Omega(n^2)$. This result is optimal (up to a constant factor).

3.3 Are There Hard Examples for Frege Systems? – Nearly Twenty Years Later

Samuel R. Buss (University of California – San Diego, US)

We discuss the lack of combinatorial examples of candidate tautologies for exponentially separating Frege and extended Frege systems. Recently, different groups have given quasipolynomial size Frege proofs for determinental identities, Frankl's theorem, and the Kneser-Lovasz tautologies. This talk presents a new proof of the pigeonhole principle which formalizes the Cook Reckhow proofs as quasipolynomial size Frege proofs.

3.4 Majority is Incompressible by $\mathsf{AC}^0[p]$ Circuits

Igor Carboni Oliveira (Columbia University, New York, US)

Joint work of Carboni Oliveira, Igor; Santhanam, Rahul

Razborov/Smolensky (1987) obtained lower bounds on the size of depth-d Boolean circuits extended with modulo p gates computing the Majority function. This result remains one of the strongest lower bounds for an explicit Boolean function. In this work, we obtain information about the structure of polynomial-size Boolean circuits with modulo p gates computing Majority. For instance, we show that for any d, at least $n/((\log n)^{O(d)})$ wires must enter the d-th layer of the circuit, which is essentially optimal. This result follows from the investigation of a more general framework called interactive compression games (Chattopadhyay and Santhanam, 2012), which combines computational complexity and communication complexity, and has applications in cryptography, parametrized complexity and circuit complexity. In this talk, we will discuss new results in this model, and mention a few open problems.

3.5 A Parameterized Halting Problem

Yijia Chen (Shanghai Jiao Tong University, CN)

Joint work of Chen, Yijia; Flum, Jörg
Main reference Y. Chen, J. Flum, "A parameterized halting problem," in H. L. Bodlaender, R. Downey, F. V. Fomin, D. Marx (eds.), "The Multivariate Algorithmic Revolution and Beyond – Essays Dedicated to Michael R. Fellows on the Occasion of His 60th Birthday," LNCS, Vol. 7370, pp. 364–397, Springer, 2012.
URL http://dx.doi.org/10.1007/978-3-642-30891-8_17

The parameterized problem $p{-}Halt$ takes as input a nondeterministic Turing machine M and a natural number n, the size of M being the parameter. It asks whether every accepting run of M on empty input tape takes more than n steps. This problem is in the class XP_{uni}, the class "uniform XP," if there is an algorithm deciding it, which for fixed machine M runs in time polynomial in n. It turns out that various open problems of different areas of theoretical computer science are related or even equivalent to $p{-}Halt \in XP_{uni}$. Thus this statement forms a bridge which allows to derive equivalences between statements of different areas (proof theory, complexity theory, descriptive complexity, ...) which at first glance seem to be unrelated. As our presentation shows, various of these equivalences may be obtained by the same method.

3.6 Proof Complexity for Quantified Boolean Formulas

Leroy Chew (University of Leeds, GB)

Joint work of Beyersdorff, Olaf; Chew, Leroy; Janota, Mikoláš
Main reference O. Beyersdorff, L. Chew, M. Janota, "Proof complexity of resolution-based QBF calculi," to appear.

Proof systems for quantified Boolean formulas (QBFs) provide a theoretical underpinning for the performance of important QBF solvers. In particular, the calculi Q-resolution and long- distance Q-resolution serve as underlying formalisms for DPLL solvers for QBFs. More recently, calculi based on universal expansion were introduced in order to enable reasoning about expansion-based QBF solvers. These are ∀Exp+Res [3] and its generalisations IR and IRM [1]. However, the proof complexity of these proof systems is currently not well understood and in particular lower bound techniques are missing.

In this talk we exhibit a new and elegant proof technique for showing lower bounds in QBF proof systems based on strategy extraction [2]. This technique provides a direct transfer of circuit lower bounds to lengths of proofs lower bounds. We use our method to show the hardness of a natural class of parity formulas for Q-resolution. Variants of the formulas are hard for even stronger systems as long-distance and universal Q-resolution. With a completely different lower bound argument we show the hardness of the prominent formulas of Kleine Büning et al. for the strong expansion-based calculus IR, thus also confirming the hardness of the formulas for Q-resolution. Our lower bounds imply new exponential separations between two different types of resolution-based QBF calculi: proof systems for DPLL-based solvers (Q-resolution, long- distance Q-resolution) and proof systems for expansion-based solvers (∀Exp+Res and its generalisations IR and IRM). The relations between proof systems from the two different classes were not known before.

References

1 Olaf Beyersdorff, Leroy Chew, and Mikoláš Janota. On unification of QBF resolution-based calculi. In *MFCS*, pages 81–93, 2014.
2 Olaf Beyersdorff, Leroy Chew, and Mikoláš Janota. Proof complexity of resolution-based QBF calculi. In *STACS*. LIPIcs series, 2015.
3 Mikolás Janota and João Marques-Silva. On propositional QBF expansions and Q-resolution. In *SAT*, pages 67–82, 2013.

3.7 On the Success Probability of Polynomial-Time SAT Solvers

Andrew Drucker (University of Edinburgh, GB)

Main reference A. Drucker, "Nondeterministic Direct Product Reductions and the Success Probability of SAT Solvers," in Proc. of the 2013 IEEE 54th Annual Symp. on Foundations of Computer Science (FOCS'13), pp. 736–745, IEEE, 2013.
URL http://dx.doi.org/10.1109/FOCS.2013.84

In one approach to solving NP-complete problems like SAT, we try to design an efficient randomized algorithm that attempts to guess a solution, and that is guaranteed to have success probability better than truly-random guessing (if a solution exists). Such "intelligent random guessing" is at the core of a number of improved exponential-time algorithms for these problems. This was observed by Paturi and Pudlák [1], who found evidence for the limitations of such algorithms.

We further this project. We show that a standard hardness assumption ($NP \notin coNP/poly$) implies the following: For every polynomial-time randomized algorithm attempting to produce satisfying assignments to Boolean formulas, there are infinitely many satisfiable instances on which the algorithm's success probability is nearly-exponentially small. Our proof involves new ideas for the study of average-case complexity in the circuit model.

References

1 R. Paturi, P. Pudlák. *On the Complexity of Circuit Satisfiability.* Proceedings of the forty-second ACM symposium on Theory of computing, pp. 241–250, 2010.

3.8 The Space Complexity of Cutting Planes Refutations

Nicola Galesi (University of Rome "La Sapienza", IT)

Joint work of Galesi, Nicola; Pavel Pudlák; Neil Thapen

We study the space complexity of the cutting planes proof system, in which the lines in a proof are integral linear inequalities. We measure the space used by a refutation as the number of inequalities that need to be kept on a blackboard while verifying it. We show that any unsatisfiable set of inequalities has a cutting planes refutation in space five. This is in contrast to the weaker resolution proof system, for which the analogous space measure has been well-studied and many optimal lower bounds are known.

Motivated by this result we consider a natural restriction of cutting planes, in which all coefficients have size bounded by a constant. We show that there is a CNF which requires super-constant space to refute in this system. The system nevertheless already has an exponential speed-up over resolution with respect to size, and we additionally show that it is stronger than resolution with respect to space, by constructing constant-space cutting planes proofs of the pigeonhole principle with coefficients bounded by two.

We also consider variable space for cutting planes, where we count the number of instances of variables on the blackboard, and total space, where we count the total number of symbols.

3.9 On the Correlation of Parity and Small-Depth Circuits

Johan Håstad (KTH Royal Institute of Technology, SE)

Main reference J. Håstad, "On the Correlation of Parity and Small-Depth Circuits," SIAM J. Computing, 43(5):1699–1708, 2014.
URL http://dx.doi.org/10.1137/120897432

We prove that the correlation of a depth-d unbounded fan-in circuit of size S with parity of n variables is at most $\exp(-\Omega(n/(\log S)^{d-1}))$.

3.10 On Optimal Heuristic Computations and Heuristic Proofs

Dmitry Itsykson (Steklov Institute of Mathematics, St. Petersburg, RU)

Joint work of Itsykson, Dmitry; Hirsch, Edward; Monakhov, Ivan; Nikolaenko, Valeria; Smal, Alexander; Sokolov, Dmitry

An acceptor for a language L is an algorithm that accepts elements of L and does not stop on other inputs. Messner proved that for all good enough (paddable) languages the existence of an optimal acceptor is equivalent to the existence of a p-optimal proof system. We consider a notion of randomized heuristic acceptors that may accept with noticeable probability a small fraction of inputs according to some distribution concentrated on the complement of the language. We show that for every recursively enumerable langauge L and polynomial-time samplable distribution concentrated on the complement of L there exists an optimal randomized heuristic acceptor. Sometimes it is possible to make a construction deterministic. For example for a language of the images of an injective function $f_n : \{0,1\}^n \to \{0,1\}^{n+1}$ there exists an optimal deterministic heuristic algorithm. Sometimes it is also possible to eliminate errors: there exists an average-case optimal randomized acceptor for graph non-isomorphism.

In the heuristic setting the proof of the equivalence between optimal acceptor and p-optimal proof systems fails. However a heuristic proof system is an interesting concept. We give some examples of short heuristic proofs that have no known short classical counterparts.

3.11 QBF Solving and Proof Systems

Mikoláš Janota (INESC-ID, Lisbon, PT)

Joint work of Janota, Mikoláš; Klieber, William; Marques-Silva, Joao; Clarke, Edmund
Main reference M. Janota, W. Klieber, J. Marques-Silva, E. Clarke, "Solving QBF with Counterexample Guided Refinement," in Proc. of the 15th Int'l Conf. on Theory and Applications of Satisfiability Testing (SAT'12), LNCS, Vol. 7317, pp. 114–128, Springer, 2012.
URL http://dx.doi.org/10.1007/978-3-642-31612-8_10

Deciding Quantified Boolean Formulas (QBFs) is interesting both theoretically and practically. QBFs are amenable to solving and theoretical analysis due to its canonic structure . At the same time, they enable expressing a wide range of problems as the decision problem is PSPACE complete. In this talk we will look at a recent method for solving QBF, which gradually expands the given formula and invokes a SAT solver in a blackbox fashion. This approach has proven to be highly competitive compared to existing ones. We will briefly discuss a proof system that corresponds to this solving algorithm.

3.12 New Lower and Upper Bounds on Circuit Complexity

Alexander S. Kulikov (Steklov Institute of Mathematics, St. Petersburg, RU)

In the first part of the talk, we will show how SAT-solvers can help to prove stronger upper bounds on the Boolean circuit complexity. Roughly, the main idea is that circuits for some functions are naturally built from blocks of constant size. E.g., the well-known circuit that computes the binary representation of the sum of n input bits is built from n full adders and has size $5n$. One can then state the question "whether there exist a block of smaller size computing the same function" in terms of CNF- SAT and then ask SAT-solvers to verify this. Using this simple approach we managed to improve the upper bound for the above mentioned function to $4.5n$. This, in particular, implies that any symmetric function has circuit size at most $4.5n + o(n)$. We will also present improved upper bounds for some other symmetric functions.

In the second part we will present much simpler proofs of currently best known lower bounds on Boolean circuit complexity. These are $3n - o(n)$ for the full binary basis [Blum, 1984] and $5n - o(n)$ for the binary basis where parity and its complement are excluded [Iwama, Morizumi, 2002]. The properties of the functions under consideration allow us to prove the stated lower bounds with almost no case analysis.

3.13 Narrow Proofs May Be Maximally Long

Massimo Lauria (KTH Royal Institute of Technology, SE)

Joint work of Atserias, Albert; Lauria, Massimo; Nordström, Jakob
Main reference A. Atserias, M. Lauria, J. Nordström, "Narrow Proofs May Be Maximally Long," in Proc. of the 2014 IEEE 29th Conf. on Computational Complexity (CCC'14), pp. 286–297, IEEE, 2014.
URL http://dx.doi.org/10.1109/CCC.2014.36

We prove that there are 3-CNF formulas over n variables refutable in resolution in width w that require resolution proofs of size n^w. This shows that the simple counting argument that any formula refutable in width w must have a proof in size n^w is essentially tight. Moreover, our lower bound extends even to polynomial calculus resolution (PCR) and Sherali-Adams, implying that the corresponding size upper bounds in terms of degree and rank are tight as well. In contrast, the formulas have Lasserre proofs of constant rank and size polynomial in both n and w.

3.14 An Observation on Levin's Algorithm and a New (?) Application to Matrix Multiplication

Jochen Messner (Ulm, DE)

We present a simple observation on Levin's algorithm which allows an efficient implementation for example on Turing machines. Then we use Freyvald's randomized matrix multiplication test together with Levin's method to obtain an optimal probabilistic matrix multiplication algorithm.

3.15 Speedup and Noncomputability

Hunter Monroe (IMF, Washington, US)

Speedup broadly is the nonexistence of an optimal algorithm under some partial order. The presentation will consider whether speedup exists for "natural" computational problems such as multiplying integers or matrices and not only for Blum's artificially constructed languages. The goal will be to direct attention toward nonexistence rather than existence of optimal algorithms. The talk will: (1) consider worst case speedup for integer and matrix multiplication; (2) note a connection with monotone-nonmonotone gap for Boolean circuits; (3) examine possible infinitely often speedup for the complement of bounded halting (and for coNP-complete languages and for proof systems) and whether better algorithms be easily produced; and (4) discuss a possible relationship between the properties "has no best algorithm" and "has no algorithm at all".

3.16 On Some Problems in Proof Complexity

Pavel Pudlák (Academy of Sciences, Prague, CZ)

We are interested in open problems about the relation of complexity and provability. For most of these statements, it seems that one answer is more plausible than the other. Therefore we rather talk about conjectures. A prototype of such a conjecture is the one that says that there is no finitely axiomatized consistent theory S such that for every finitely axiomatized consistent theory one can construct proofs of $Con_S(n)$ in polynomial time. Here $Con_S(n)$ denotes the consistency of S restricted to proofs of length at most n. The conjectures $P \neq NP$ and $NP \neq coNP$ can also be viewed as such conjectures, because they can be stated in terms of propositional proof systems.

The conjecture that we studied so far can be classified in two ways: (1) deterministic/nondeterministic, (2) universal/existential. The main universal conjectures are comparable and so are the main existential conjectures. Thus the conjectures form two branches. We introduce two new conjecture. One is the Σ_1^b finite reflection principle, which is a natural strengthening of finite consistency mentioned above. The second one is *Herbrand consistency search*. The reason for introducing Herbrand consistency search is to get a conjecture related to consistency also in the existential branch of conjectures.

The strongest conjecture in the universal branch is the conjecture saying that there is no complete disjoint NP pair. Similarly, the strongest conjecture in the existential branch is the conjecture saying that there is no complete disjoint $coNP$ pair. We have not been able to find a natural conjecture that would imply both conjectures.

3.17 On the AC^0 Complexity of Subgraph Isomorphism

Benjamin Rossman (National Institute of Informatics, Tokyo, JP)

Joint work of Rossman, Benjamin; Li, Yuan; Razborov, Alexander

Let P be a fixed graph (hereafter called a "pattern"), and let Subgraph(P) denote the problem of deciding whether a given graph G contains a subgraph isomorphic to P. We are interested in AC^0-complexity of this problem, determined by the smallest possible exponent $C(P)$ for which Subgraph(P) possesses bounded-depth circuits of size $n^{C(P)+o(1)}$. Motivated by the previous research in the area, we also consider its "colorful" version $\text{Subgraph}_{col}(P)$ in which the target graph G is $V(P)$-colored, and the average-case version $\text{Subgraph}_{ave}(P)$. Defining $C_{col}(P)$ and $C_{ave}(P)$ analogously to $C(P)$, our main contributions can be summarized as follows.

1. $C_{col}(P)$ coincides with the tree-width of the pattern P within a logarithmic factor. This shows that the previously known upper bound by Alon, Yuster, Zwick is almost tight.
2. We give a characterization of $C_{ave}(P)$ in purely combinatorial terms within a multiplicative factor of 2. This shows that the lower bound technique of Rossman is essentially tight, for any pattern P whatsoever.
3. We prove that if Q is a minor of P then $\text{Subgraph}_{col}(Q)$ is reducible to $\text{Subgraph}_{col}(P)$ via a linear-size monotone projection. At the same time, we show that there is no monotone

projection whatsoever that reduces Subgraph(M_3) to Subgraph($P_3 + M_2$) (P_3 is a path on 3 vertices, M_k is a matching with k edges, and "+" stands for the disjoint union). This result strongly suggests that the colorful version of the subgraph isomorphism problem is much better structured and well-behaved than the standard (worst-case, uncolored) one.

3.18 Characterizing the Existence of Optimal Proof Systems and Complete Sets for Promise Classes

Zenon Sadowski (University of Białystok, PL)

Joint work of Sadowski, Zenon; Beyersdorff, Olaf
Main reference O. Beyersdorff, Z. Sadowski, "Do there exist complete sets for promise classes?" Mathematical Logic Quarterly, 57(6):535–550, 2011.
URL http://dx.doi.org/10.1002/malq.201010021

We investigate the following two questions:

Q1: Do there exist optimal proof systems for a given language L?
Q2: Do there exist complete problems for a given promise class C?

For concrete languages (such as TAUT or SAT) and concrete promise classes (such as UP, disjoint NP-pairs etc.) these questions have been intensively studied during last years, and a number of characterizations have been obtained. Here we provide new characterizations for Q1 and Q2 that apply to almost all promise classes C and languages L, thus creating a unifying framework for the study of these questions. More specifically, we introduce the notion of a promise complexity class representable in a proof system (captured by a proof system). We express the promise condition of a class in a language L and then use a proof system for L to verify that a given Turing machine satisfies the promise.

3.19 Hierachies and Lower Bounds via Optimality: A Survey

Rahul Santhanam (University of Edinburgh, GB)

I survey work on hierarchy theorems and circuit lower bounds, which uses ideas from optimal algorithms. This work includes hierarchy theorems for probabilistic time with advice due to Barak and Fortnow & myself, and my work on circuit lower bounds for MA with advice.

3.20 Disjoint NP-Pairs and Propositional Proof Systems

Alan Selman (SUNY – Buffalo, US)

Joint work of Glasser, Christian; Hughes, Andrew; Selman, Alan; Wisiol, Nils

This talk surveys results on disjoint NP-pairs, propositional proof systems, function classes, and promise classes – including results that demonstrate close connections that bind these topics together. We illustrate important links between the questions of whether these classes have complete objects and whether optimal proof systems may exist.

3.21 Examples of Heuristic Proofs

Dmitry Sokolov (Steklov Institute of Mathematics, St. Petersburg, RU)

Joint work of Sokolov, Dmitry; Itsykson, Dmitry

In this talk we consider heuristic proof systems and give non-trivial examples of proof systems of this kind. We give an example of a distributional problem (Y, D) that is in the complexity class $HeurNP$ but if NP is not equal to $coNP$ then Y is not in NP, and if $(NP, PSamp)$ is not contained in $HeurBPP$ then (Y, D) is not in $HeurBPP$.

For a language L and a polynomial q we define a language L_q composed of pairs (x, r) where x is an element of L and r is an arbitrary binary string of length $q(|x|)$. If $D = \{D_n\}$ is an ensemble of distributions on strings, let $[D, U]$ be a distribution on pairs (x, r), where x is distributed according to D_n and r is uniformly distributed on strings of length $q(n)$. We show that for every language L in AM there is a polynomial q such that for every distribution D concentrated on the complement of L the distributional problem $(L_q, [D, U]_q)$ has a polynomially bounded heuristic proof system. Since graph non-isomorphism (GNI) is in AM, the above result is applicable to GNI.

4 Open Problems

The seminar hosted two open problem sessions: the first immediately after the introduction on Monday morning, thus giving participants the opportunity to state problems they would like to discuss with others during the week, and the second one towards the end of the workshop on Thursday evening, reflecting on material presented during the week. The problems presented in these two sessions include:

1. **Andrew Drucker**
   - Let $PC(\varphi)$ denotes a proof length of φ in some propositional proof system Π. Is there a sequence of tautologies $\varphi_1(x_1, \ldots, x_n), \ldots, \varphi_t(x_1, \ldots, x_n)$, s.t. $PC(\varphi_1, \ldots, \varphi_t) = \omega(\max_i PC(\varphi_i))$?
2. **Nicola Galesi**
   - Can CP^* (cutting-plane proof system with polynomially bounded coefficients) refute every unsatisfiable CNF using constant space?
   - Is it possible to refute every unsatisfiable CNF in CP with linear total space?
   - Devise better lower bounds for CP^2 (cutting-plane proofs with coefficients bounded by 2).

   Background information on these problems can be found in [5].
3. **Andreas Goerdt**
   - Prove that linear resolution does not p-simulate regular resolution.
4. **Johan Håstad**
   - Devise relations between monotone threshold circuits with bounded and unbounded weights. Non-monotone question is described in [7].

5. **Alexander Kulikov**
   - A function $f : \{0,1\}^n \to \{0,1\}$ is called an affine disperser for dimension d, if for every affine subspace $S \subseteq \{0,1\}^n$ of dimension at least d, f is not constant on S. This means that $n-d$ linear substitutions of the form $x_i = \bigoplus_{j \neq i} x_j \cdot b_j \oplus b_0$, where $b_i \in \{0,1\}$ do not make the function constant.
     Ben-Sasson and Kopparty, Shaltiel showed that there are affine dispersers for dimension $o(n)$ in P.
     Let us consider the following extension of affine dispersers. Now we allow linear and 'quadratic' substitutions. We start with a function of n variables. Then we make a substitution of the form $x_i = \bigoplus_{j \neq i} x_j \cdot b_j \oplus b_0$ or $x_i = (x_j \oplus b_j) \cdot (x_k \oplus b_k) \oplus b$, s.t. the substitution makes it a function of $n-1$ variables (i.e., after substituting x_i, it will never appear in the subsequent substitutions). We make $n-k$ substitutions as above and require the resulting function of k variables to be non-constant. Using a probabilistic argument one can show that these functions exist for dimension $k = o(n)$.
     My main question is whether it is possible to find dispersers of this kind for dimension $o(n)$ in NP?
   - Let $C(AND, OR, XOR)$ denote the circuit complexity (over the full binary basis B_2) of a function $f : \{0,1\}^n \to \{0,1\}^3$, such that $f(x) = (AND(x), OR(x), XOR(x))$.
     It is known that $2n - 2 \leq C(AND, OR, XOR) \leq 2.5n$. Is it possible to improve the lower bound?
6. **Massimo Lauria**
   - There is a natural way to express in CNF form that a graph $G = ([n], E)$ contains a clique of size k (i.e., a set of k vertices pairwise connected by edges).
     If G has no k-clique then the corresponding CNF formula has a refutation. Furthermore, most algorithms to detect cliques in graphs would implicitly produce a resolution refutation of the k-clique formula, when they look for a k-clique in a graph that does not have any. The length of the refutation is proportional to the running time of the algorithm.
     For this reason it is interesting to determine how long is a refutation the k-clique formula: $n^{O(k)}$ is an obvious upper bound. Is this tight? Does the k-clique formula require a resolution refutation of size $n^{\Omega(k)}$ for some graph family?
     The CNF formulation of the clique formulas as well as further background can be found in [1,2].
7. **Jochen Messner**
   - Is there a $\leq_m^p$-complete set among all sets with an optimal acceptor?
   - Does every set with an optimal acceptor have a p-optimal proof system?
   - Is there a set outside P that has a p-optimal proof system?
     Some background information can be found in [4,6].
8. **Hunter Monroe**
   - Can hard instances be generated in various settings (hard tautologies to prove or to accept, hard inputs $< N, x, 1^t >$ to the complement of bounded halting) and given that such a construction would imply P$\neq$ NP, how could it circumvent the limits on diagonalization identified by Baker, Gill, and Solovay?
9. **Sebastian Müller**
   - In Parity Games you can easily construct gadgets that, when adjoined to any game graph, make the associated Parity Game trivial, but alteration of one specific edge, vertex or priority makes the gadget useless and therefore the game on the graph with the altered gadget is as hard to solve as the original one.

As these gadgets can be constructed for most classes of graphs (planar is a weak exception), it shows that most classes of game graphs over which Parity Games are feasible are not closed under the above alterations.

What happens if we are concerned with random edges, vertices or priorities? Can we construct a graph, where random alterations already lead to problems? Can we posibly add this to an exisiting graph and infer something in the light of what I said above? Also, what happens if we look at specific or random alterations on the random graph (perceived as a game graph)?

Background information on these problems can be found in [9].

10. **Rahul Santhanam**
    - For a deterministic Turing machine M which halts on all inputs, let $T_M(n)$ be the worst-case time complexity of M on inputs of length n. Consider the following 'running time estimation' problem: given n in unary, compute $T_M(n)$. Is there an exponential time-bounded machine M such that a polynomial-time solution to the running time estimation problem for M has interesting complexity-theoretic consequences, eg., a collapse of complexity classes?

11. **Alexander Smal**
    - The following are equivalent
      a. There is an optimal propositional proof system.
      b. TAUT has an almost optimal nondeterministic algorithm.
      c. There is a nondeterministic algorithm that decides p-Halt$_>$ problem.
      (Input of p-Halt$_>$ is a pair of nondeterministic Turing machine M and natural number n in unary. The problem is "does every accepting run of M on the empty input take more than n steps?")

    What is a heuristic analogue of this statement?

    Some background information can be found in [3, 8].

References

1 Olaf Beyersdorff, Nicola Galesi, and Massimo Lauria. Parameterized complexity of DPLL search procedures. *ACM Transactions on Computational Logic*, 14(3), 2013.

2 Olaf Beyersdorff, Nicola Galesi, Massimo Lauria, and Alexander Razborov. Parameterized bounded-depth Frege is not optimal. *ACM Transactions on Computation Theory*, 4(3), 2012.

3 Yijia Chen, Jörg Flum. A parameterized halting problem. *Lecture Notes in Computer Science*, 7370, 2012.

4 Johannes Köbler, Jochen Messner, Jacobo Torán. Optimal proof systems imply complete sets for promise classes. *Information and Computation*, 184(1), 2003.

5 Nicola Galesi, Pavel Pudlák, and Neil Thapen. The space complexity of cutting planes refutations. *Electronic Colloquium on Computational Complexity (ECCC)*, 21:138, 2014.

6 Jochen Messner. On optimal algorithms and optimal proof systems. In *Proc. STACS'99*, pages 541–550, 1999.

7 Mikael Goldmann, Johan Håstad and Alexander Razborov. Majority Gates vs. General Weighted Threshold Gates. *Journal of Computation Complexity*, 1(4), 1992.

8 Edward A. Hirsch, Dmitry Itsykson, Ivan Monakhov, Alexander Smal. On Optimal Heuristic Randomized Semidecision Procedures, with Applications to Proof Complexity and Cryptography. *Theory of Computing Systems*, 51(2), 2012.

9 Sebastian Müller. Graph structure and parity games. *Electronic Colloquium on Computational Complexity (ECCC)*, 21:121, 2014.

Participants

- Per Austrin
KTH Royal Institute of Technology, SE
- Olaf Beyersdorff
University of Leeds, GB
- Ilario Bonacina
University of Rome "La Sapienza", IT
- Samuel R. Buss
University of California – San Diego, US
- Igor Carboni Oliveira
Columbia Univ. – New York, US
- Ruiwen Chen
University of Edinburgh, GB
- Yijia Chen
Shanghai Jiao Tong Univ., CN
- Leroy Chew
University of Leeds, GB
- Andrew Drucker
University of Edinburgh, GB
- Susanna Figueiredo de Rezende
KTH Royal Institute of Technology, SE
- Jörg Flum
Universität Freiburg, DE
- Nicola Galesi
University of Rome "La Sapienza", IT
- Michal Garlik
Charles University – Prague, CZ
- Christian Glasser
Universität Würzburg, DE
- Andreas Goerdt
TU Chemnitz, DE
- Johan Hastad
KTH Royal Institute of Technology, SE
- Edward A. Hirsch
Steklov Institute – St. Petersburg, RU
- Dmitry Itsykson
Steklov Institute – St. Petersburg, RU
- Mikoláš Janota
INESC-ID – Lisboa, PT
- Emil Jerabek
Acad. of Sciences – Prague, CZ
- Alexander Knop
St. Petersburg State Univ., RU
- Johannes Köbler
HU Berlin, DE
- Jan Krajíček
Charles University – Prague, CZ
- Alexander S. Kulikov
Steklov Institute – St. Petersburg, RU
- Massimo Lauria
KTH Royal Institute of Technology, SE
- Barnaby Martin
Middlesex University, GB
- Jochen Messner
Ulm, DE
- Hunter Monroe
IMF – Washington, US
- Moritz Müller
Universität Wien, AT
- Sebastian Mueller
University of Toronto, CA
- Jakob Nordström
KTH Royal Institute of Technology, SE
- Jan Pich
Charles University – Prague, CZ
- Pavel Pudlák
Acad. of Sciences – Prague, CZ
- Benjamin Rossman
National Institute of Informatics – Tokyo, JP
- Zenon Sadowski
University of Bialystok, PL
- Rahul Santhanam
University of Edinburgh, GB
- Alan Selman
SUNY – Buffalo, US
- Alexander Smal
Steklov Institute – St. Petersburg, RU
- Dmitry Sokolov
Steklov Institute – St. Petersburg, RU
- David Steurer
Cornell University, US
- Jacobo Torán
Universität Ulm, DE