Proof Complexity Workshop

St. Petersburg State University
May 15-20, 2016

Speakers, Titles and Abstracts

James Aisenberg
Proof complexity of the Kneser-Lovász theorem
Thursday, May 19. 15:45-16:15

Abstract: It is generally conjectured that there is an exponential separation in proof length between Frege and extended Frege systems; however, there are currently few candidate families of tautologies that could provide such a separation. One such candidate was based on Lovász's theorem about the chromatic number of Kneser graphs. We show that propositional translations of the Kneser-Lovász theorem have quasipolynomial size Frege proofs, and thus they can no longer be considered a candidate for providing the desired separation. Additionally, we discuss a related candidate family of tautologies based on Tucker's lemma that is known to have polynomial size extended Frege proofs but is not known to have sub-exponential size Frege proofs.

Joint work with Maria Luisa Bonet, Sam Buss, Adrian Crăciun, and Gabriel Istrate.

Albert Atserias
Two Applications of a Refined Analysis of Random Restrictions in Proof Complexity
Friday, May 20. 9:45-10:45

Abstract: Since its first use in propositional proof complexity in the seminal work of Ajtai, the method of random restrictions has shown quite useful for proving lower bounds for low-depth propositional proof systems. On the other hand, the feeling of many experts in the area was that, in their optimal incarnations, all such applications would produce exponential lower bounds of type 2^{n^γ} for natural formulas with n variables. In other words, it looked like proving matching lower bounds for natural formulas that have quasipolynomial upper bounds of type $n^{(\log n)^c}$, if possible at all, would seem to require quite different methods. In this talk I will discuss a very simple refined analysis of random restrictions that is able to achieve matching lower bounds of all ranges for specific yet natural formulas. The first application

of this method is a matching lower bound of type $n^{\log n}$ for depth-two proofs of a natural relativized version of the weak pigeonhole principle. The second application gives lower bounds of (essentially) all ranges for resolution proofs of parameterized versions of the same formulas. These results seem to indicate that the random restriction method for low-depth proof systems is less of an overkill than previously thought.

This is based on separate joint works with Moritz Müller and Sergi Oliva, and Massimo Lauria and Jakob Nordström.

Arnold Beckmann
Total NP Search Problems for Second-Order Bounded Arithmetic related to PSPACE Reasoning
Tuesday, May 17. 12:15-13:15

Abstract: Total NP search problems play an important role in analysing bounded arithmetic theories. We review known characterisations of the total NP search problems for second-order bounded arithmetic related to PSPACE reasoning, given by Koodziejczyk, Nguyen, and Thapen (2011) in terms of local improvement properties, and improved by Beckmann and Buss (2014). We present new characterisations based on extended local improvement properties, involving PSPACE machines with consistent restarts.

This is joint work with Jean-Jose Razafindrakoto.

Eli Ben-Sasson
The quest for scalable PCPs
Friday, May 20. 10:45-11:45

Abstract: Multiprover Interactive Proof (MIP) systems and Probabilistically Checkable Proofs (PCP) have many promising applications to decentralized systems like Bitcoin and Zerocash.

In this talk I will discuss our ongoing efforts to implement quasi-linear PCP systems for NEXP-complete languages, and focus on new theoretical models and research questions emerging from this pursuit.

Based on joint works with Iddo Ben-Tov, Alessandro Chiesa, Ariel Gabizon, Daniel Genkin, Matan Hamilis, Evgenya Pergament, Michael Riabzev, Mark Siberstein, Nicholas Spooner, Eran Tromer and Madars Virza.

Olaf Beyersdorff
Proof Complexity of Quantified Boolean Formulas
Tuesday, May 17. 14:45-15:45

Abstract: This talk will give an overview of the relatively young field of QBF proof complexity. We explain the main resolution-based proof systems for QBF, modelling CDCL and expansion-based solving. In the main part of the talk we will give an overview of current lower bound techniques (and their limitations) for QBF systems. In particular, we exhibit a new and elegant proof technique for showing lower bounds in QBF proof systems based on strategy extraction. This technique provides a direct transfer of circuit lower bounds to lengths of proofs lower bounds.

Ilario Bonacino
Total space in Resolution is at least width squared
Thursday, May 19. 16:45-17:15

Abstract: In this talk we cover some results on the space complexity of Resolution and in particular the new recent connection between total space and width in the title. Given a k-CNF formula F, the width is the minimal integer W such that there exists a Resolution refutation of F with clauses of at most W literals. The total space is the minimal size T of a memory used to write down a Resolution refutation of F, where the size of the memory is measured as the total number of literals it can contain. We show that $T = \Omega((W - k)^2)$. This connection between total space and width relies on some basic properties of another, perhaps less known, complexity measure in Resolution: the asymmetric width.

The talk is based on a paper to appear in ICALP16.

Sam Buss
Tutorial: Bounded arithmetic, proof complexity, and NP search problems
Sunday, May 15. 10:45-11:45, 12:15-13:15, 15:00-16:00, and 16:30-17:30.

Abstract: This tutorial will cover first- and second-order theories of bounded arithmetic, translations from bounded arithmetic to propositional proof systems, and associated NP search functions.

Hubie Chen

Proof Complexity Modulo the Polynomial Hierarchy: Understanding Alternation as a Source of Hardness

Tuesday, May 17. 16:45-17:15

Abstract: If one looks at typical proof systems for QBF, such as Q-resolution, a dilemma is encountered: lower bounds for Q-resolution are implied immediately by lower bounds for resolution, yet this says nothing about Q-resolution's ability to cope with quantifier alternation—and moreover clashes severely with the contemporary QBF view of SAT as "easy". In this talk, we will discuss this dilemma and present a possible way to escape it.

In particular, we present and study a framework in which one can present alternation-based lower bounds on proof length in proof systems for quantified Boolean formulas. A key notion in this framework is that of proof system ensemble, which is (essentially) a sequence of proof systems where, for each, proof checking can be performed in the polynomial hierarchy. We introduce a proof system ensemble called relaxing QU-res which is based on the established proof system QU-resolution. Our main technical results include an exponential separation of the tree-like and general versions of relaxing QU-res, and an exponential lower bound for relaxing QU-res; these are analogs of classical results in propositional proof complexity.

This talk will focus on a conceptual discussion of the work's motivation, the framework and the main definitions.

A version of this article is available at http://arxiv.org/abs/1410.5369.

Michal Garlik

Bounded arithmetic, ultrapowers, and replacement

Wednesday, May 18. 15:45-16:15

Abstract: We present a restricted reduced power construction of models of bounded arithmetic that yields nonelementary extensions without introducing new lengths. We apply the construction, sometimes together with a hardness assumption, to obtain models of bounded arithmetic which violate sharply bounded collection. As an example we show that if a sufficiently strong one-way permutation exists then $strictR^1_2$ is weaker than R^1_2.

Dima Grigoriev

Subtraction-free computations and cluster algebras

Wednesday, May 18. 10:45-11:45

Abstract: Using cluster transformations we design subtraction-free algorithms for computing Schur polynomials and for generating spanning trees and arborescences polynomials. The latter provides an exponential complexity gap between circuits admitting arithmetic operations $+$, $\times$, $/$ versus $+$, $\times$. In addition, we establish an exponential complexity gap between circuits admitting $+$, $-$, $\times$, $/$ versus $+$, $\times$, $/$. Together with V. Strassen's result on "Vermeidung von Divisionen" this closes a long-standing problem on comparative complexity power between all possible subsets of operations $+$, $-$, $\times$, $/$.

(a joint work with S. Fomin, G. Koshevoy)

Pavel Hrubeš
Semantic cutting planes
Wednesday, May 18. 9:45-10:45

Abstract: Cutting Planes is a refutation system which certifies unsatisfiability of a set of linear inequalities. Typically, it is defined using the addition rule and rounding rule. We consider the semantic version of the system, where every sound inference with a constant number of premises is allowed. We observe that the semantic system has feasible interpolation via monotone real circuits - a fact previously established for syntactic cutting planes by P. Pudlak. Nevertheless, we show that the semantic system is strictly stronger than the syntactic. Joint work with Y. Filmus and M. Lauria.

Rosalie Iemhoff
Regular properties and the existence of proof systems
Tuesday, May 17. 10:45-11:45

Abstract: During the last hundred years, proof systems of all kinds have been developed for a great variety of logics. Less common are results that establish that certain logics cannot have proof systems of a certain kind. The majority of such negative results use arguments showing that the complexity of the given logic does not match that of the proof system. Here we present a method of a very different nature, that applies to intermediate and modal propositional logics, where the proof systems under consideration are sequent calculi. The method uses what we call regular properties, of which interpolation and uniform interpolation are examples. Besides being a tool to prove the negative results, the method also provides a syntactic technique to prove that certain logics have uniform interpolation. The technique builds on a paper by Andrew Pitts from 1992 in which it is shown that intuitionistic propositional logic has uniform interpolation.

Dimitry Itsykson

On OBDD based algorithms and proof systems that dynamically change order of variables

Thursday, May 19. 10:45-11:45

Abstract: We study OBDD-based proof systems supplied with an additional rule that allows to change the order in OBDDs. At first we consider a proof system OBDD($\wedge$, reorder) that uses the conjunction (join) rule and the rule that allows to change the order. We exponentially separates this proof system from OBDD($\wedge$)-proof system that uses only conjunction rule. We prove two exponential lower bounds on the size of OBDD($\wedge$, reorder)-refutation of Tseitin formulas and the pigeonhole principle. The first lower found was previously unknown even for OBDD($\wedge$)-proofs and the second one extends the result of Tveretina et. al from OBDD($\wedge$) to OBDD($\wedge$, reorder).

At second we add the operation of changing the order in the approach to the propositional satisfiability problem based on OBDDs and symbolic quantifier elimination proposed by Pan and Vardi in 2004. An instance of the propositional satisfiability problem is considered as existential quantified propositional formula. The algorithm chooses an order on variables and creates an ordered binary decision diagram D that initially represents the constant 1 function. Then the algorithm downloads to D clauses of the CNF one by one and applies to D the elimination of the existential quantifier for variable x if all clauses that contain x are already downloaded and sometimes changes the order of variables in D. We denote such algorithms as OBDD($\wedge$, $\exists$, reorder)-algorithms and denote the version without reordering by OBDD($\wedge$, $\exists$)-algorithms.

Even OBDD($\wedge$, $\exists$)-algorithms are enough powerful, in particular they solves the pigeonhole principle (Chn and Zhang, 2009) and Tseitin formulas in polynomial time. Exponential lower bounds for OBDD($\wedge$, $\exists$) algorithms follow from exponential lower bounds for OBDD($\wedge$, weakening)-proof systems; lower bounds for tree-like refutations was proved by Segerlind in 2007 and for dag-like refutations by Krajicek in 2008.

Practical experiments show that the addition of a reordering heuristic makes OBDD($\wedge$, $\exists$)-algorithms faster. However we prove exponential lower bounds for OBDD($\wedge$, $\exists$, reorder)-algorithms. Our hard instances are satisfiable formulas that represent systems of linear equations over GF(2) that correspond to some checksum matrices of error correcting codes. We left the question concerning a superpolynomial lower bound for the OBDD($\wedge$, weakening, reorder)-proof system as a challenging open problem.

The talk is based on the joint work with Alexander Knop, Andrey Ro-

mashchenko and Dmitry Sokolov.

Leszek Kołodziejczyk
Some subsystems of constant depth Frege with parity
Thursday, May 19. 9:45-10:45

Abstract: I will discuss relationships between constant depth Frege with a parity connective and some of its subsystems, with a focus on systems that combine full constant depth reasoning with limited forms of reasoning about parity. I plan to emphasize the fact that for systems of this kind, the separations we can prove are mostly just superpolynomial, whereas some quasipolynomial simulation results can also be obtained.

The talk will be based on joint work with Michal Garlik.

Jan Krajíček
Computational content of propositional proofs
Wednesday, May 18. 12:15-13:15

Abstract: I shall review several known situations where efficient propositional proofs of particular formulas yield some non-trivial computational information, and discuss a few less known or new situations where this is, or may be, also the case.

Massimo Lauria
On the search of low complexity proofs
Thursday, May 19. 14:45-15:45

Abstract: It is known that several proof systems have proof search algorithms that look for a refutation of "complexity" d in time $n^{O}(d)$. We will show that these algorithms are optimal in the sense that there are k-CNF formulas with resolution refutations of width d and refutations in polynomial calculus, Sherali-Adams and Sums-of-Squares of degree d, and nonetheless the length of a refutation in any such system is $n^{\Omega}(d)$, even if we allow unrestricted width/degree. This implies that the worst case running-time of the standard proof search algorithms cannot be improved significantly.

We will briefly describe the algorithm for each of the proof systems mentioned, and then we will show a corresponding lower bound.

This talk is based on a joint work with Albert Atserias and Jakob Nordström (CCC 2014), and a joint work with Jakob Nordström (CCC 2015).

Jakob Nordström

A Generalized Method for Proving Polynomial Calculus Degree Lower Bounds

Thursday, May 19. 12:15-13:15

Abstract: We study the problem of obtaining lower bounds for polynomial calculus (PC) and polynomial calculus resolution (PCR) on proof degree, and hence by [Impagliazzo et al. '99] also on proof size. [Alekhnovich and Razborov '03] established that if the clause-variable incidence graph of a CNF formula F is a good enough expander, then proving that F is unsatisfiable requires high PC/PCR degree. We further develop the techniques in [AR03] to show that if one can "cluster" clauses and variables in a way that "respects the structure" of the formula in a certain sense, then it is sufficient that the incidence graph of this clustered version is an expander. As a corollary of this, we prove that the functional pigeonhole principle (FPHP) formulas require high PC/PCR degree when restricted to constant-degree expander graphs. This answers an open question in [Razborov '02], and also implies that the standard CNF encoding of the FPHP formulas require exponential proof size in polynomial calculus resolution. Thus, while Onto-FPHP formulas are easy for polynomial calculus, as shown in [Riis '93], both FPHP and Onto-PHP formulas are hard even when restricted to bounded-degree expanders.

This is joint work with Mladen Miksa that appeared at CCC '15.

Jan Pich

Gentzen and Frege systems for QBF

Tuesday, May 17. 15:45-16:15

Abstract: Recently Beyersdorff, Bonacina, and Chew [1] introduced a natural class of Frege systems for quantified Boolean formulas (QBF) and showed strong lower bounds for restricted versions of these systems. We provide a comprehensive analysis of the new extended Frege systems from [1], denoted EF+$\forall$-red, which is a natural extension of classical extended Frege EF. Our main results are the following: Firstly, we prove that the standard Gentzen-style system G_1^* p-simulates EF+$\forall$-red and that G_1^* is strictly stronger under standard complexity-theoretic hardness assumptions. Secondly, we show a correspondence of EF+$\forall$-red to bounded arithmetic: EF+$\forall$-red can be seen as a nonuniform propositional version of intuitionistic S_2^1. Specifically, intuitionistic S_2^1 proofs of arbitrary statements in prenex form translate to polynomial-size EF+$\forall$-red proofs, and EF+$\forall$-red is in a sense the weakest system with this property. Finally, we show that superpolynomial lower

bounds for EF+∀-red would imply either $PSPACE \not\subseteq P/poly$ or superpolynomial lower bounds for classical EF, and in fact the converse implication holds as well. Therefore, the system EF+∀-red naturally unites the central problems from circuit and proof complexity. Technically, our results rest on a formalized strategy extraction theorem for EF+∀-red akin to witnessing in intuitionistic S^1_2 and a normal form for EF+∀-red proofs.

Toniann Pitassi
Tutorial: Propositional Proof Systems, and Algebraic and Semi-algebraic proof systems
Monday, May 16. 10:45-11:45, 12:15-13:15, 15:00-16:00, and 16:30-17:30.

Abstract: This tutorial will cover propositional proof systems, and then algebraic and semi-algebraic systems, focusing on lower bound methods and state of the art results thus far, and open problems and barriers. It will cover algebraic systems (including Nullstellensatz, PC, IPS) and semi-algebraic ones (CP, SA, SOS), as well as progress on standard propositional proof systems and some surprising upper bounds.

Toniann Pitassi
Poly-logarithmic Frege Depth Lower Bounds via an Expander Switching Lemma
Friday, May 20. 12:15-13:15

Abstract: Joint with Benjamin Rossman, Li-Yang Tan and Rocco A. Servedio

Neil Thapen
Random resolution
Tuesday, May 17. 9:45-10:45

Abstract: A random resolution refutation of a CNF formula F is a resolution refutation of F in which we are allowed to introduce new clauses as axioms, as long as the conjunction of all the new axioms is true with high probability. I will talk about some ongoing work on upper and lower bounds for this system. The system arises from a question connected to separating bounded arithmetic theories by their $\forall\Sigma^b_1$ consequences. I will describe a lower bound for a special case of the system, answering the original question. This is joint work with Albert Atserias and Pavel Pudlák.

Iddo Tzameret
Frege Lower Bounds and Algebraic Circuit Complexity
Wednesday, May 18. 14:45-15:45

Abstract: This talk is dedicated to emerging connections between proof-size lower bounds on strong systems, such as Frege, and lower bounds on the size of algebraic circuits.

First, I will show that lower bounds on Frege proofs follow from certain size lower bounds on a fairly weak model of computation, namely, non-commutative algebraic formulas. For this weak model of computation, many strong size lower bounds are already known since the early 90s. The argument is a new characterization of propositional proofs as non-commutative formulas (Li-Tzameret-Wang 2015).

Second, I will discuss how lower bounds techniques from algebraic circuit complexity yield almost directly lower bounds on the proof-size of fairly strong systems such as the Nullstellensatz and the Ideal Proof System defined by Grochow and Pitassi (2014), when refutations in both systems are written as algebraic circuits taken from some restricted circuit classes (Forbes-Shpilka-Tzameret-Wigderson 2016).

I will conclude with some open questions related to advancing the frontiers of algebraic proof complexity.

Marc Vinyals
How Limited Interaction Hinders Real Communication
Wednesday, May 18. 16:45-17:15

Abstract: In this talk we will show size-space trade-offs for the cutting planes proof system. This is, we exhibit a family of formulas that have both short proofs and proofs in small space, but optimizing either measure blows up the other. The proof goes through communication complexity, and a key insight is to use a model of communication that captures short cutting planes proofs: communication with limited rounds and with real numbers.