FEALORA Farewell Workshop 2018

Monday November 5

9:00 Petr Glivický Model theory of linear fragments of Peano arithmetic

We give a survey of our results (partialy a joint work with P. Pudlák) on linear arithmetics – linear fragments of Peano arithmetic (PA). For a cardinal k, the k-linear arithmetic LA_k is a theory extending Presburger arithmetic (in the language $(0, 1, +, <)$) by k unary functions of multiplication by distinguished (nonstandard) elements (called scalars) and containing the full scheme of induction for its language. We give a classification of all definable sets in models of LA_1 and, as a corollary, show that LA_1 is a tame theory – model complete, decidable, NIP, having recursive nonstandard models...

On the other hand we prove that LA_2 (as well as any LA_k with $k > 2$) is model theoretically wild. As a manifestation of this fact we show that there is a model M of LA_2 in which an infinitely large initial segment of Peano multiplication (i.e. a multiplication . such that $(M, .)$ is a model of PA) is 0-definable. Consequently, the theories LA_k with $k > 1$ are not model complete nor NIP. Each model of a linear arithmetic naturally corresponds to a discretely ordered module over the ordered ring generated by the scalars. Our results on LA_2 thus yield a non NIP ordered module answering negatively the question of Chernikov and Hils whether all ordered modules are NIP.

10:00 Jan Bydzovsky Polynomial time ultrapowers and the consistency of circuit lower bounds

(this is a join work with Moritz Müller) A polynomial time ultrapower is a structure given by the set of polynomial time computable functions modulo some ultrafilter. They model the universal theory $\forall PV$ of all polynomial time functions. Generalizing a theorem of Hirschfeld (1975), we show that every countable model of $\forall PV$ is isomorphic to an existentially closed substructure of a polynomial time ultrapower. Using a polynomial time ultrapower over a nonstandard Herbrand saturated model of $\forall PV$ we show that $\forall PV$ is consistent with a formal statement of a polynomial size circuit lower bound for a polynomial time computable function. This improves upon a recent result of Krajíček and Oliveira (2017).

10:30 Coffee

11:00 Leszek Kołodziejczyk Feasibility of some classical conservation results in arithmetic

The talk will be based on joint work with Tin Lok Wong and Keita Yokoyama. We show that some important results on partial conservativity between fragments of first- and second-order arithmetic are feasible in the sense that the conservativity can be witnessed by a polynomial-size translation of proofs.

12:00 End of Talks

12:30 Lunch

15:30 Coffee

16:00 Fedor Pakhomov Collection and Speed-up

Collection principles occur in various settings: axiom of Σ_1 collection is one of the axioms of Kripke-Platek set theory; collection principles $B\Sigma_n$ and $BB\Sigma^b_n$ are well-known axioms for systems of first-order and bounded arithmetic, respectively; choice principles $\Sigma^1_n - AC$ could be considered to be a form of collection for systems of second-order arithmetic. In many cases appropriate collection principles could be (partially) conservatively added to systems that couldn't prove them. Examples of results of this form are Π_2-conservativity of $B\Sigma_1$ over $I\Delta_0$ and Π^1_2-conservativity of $\Sigma^1_1 - AC_0$ over ACA_0. Similar results are present for other collection principles mentioned earlier. We develop a general result about partial conservativity of collection and reduce to it the mentioned and various other conservation results for collection principles. Next we show that our general conservation result corresponds to at most polynomial speed-up. And as a consequence we conclude that all the reduced conservation results corresponds to at most polynomial speed-up, e.g. $\Sigma^1_1 - AC_0$ have at most polynomial speed-up for Π^1_2-sentences over ACA_0.

17:00 Emil Jeřábek Bounded induction without parameters

We will investigate parameter-free versions of induction and polynomial induction axioms for bounded formulas, with particular emphasis on Π^b_i schemes. We are interested in implications among the fragments, conservation results, and connections to propositional reflection principles. Our conservation results are based on new witnessing theorems for unbounded $\forall\exists\forall\Pi^b_i$ or $\forall\exists\forall\Sigma^b_i$ consequences of T^i_2 and S^i_2.

17:30 Amir Tabatabai Reduction Programs and Higher Search Problems in Bounded Arithmetic

A reduction program between two k-turn games is a non-deterministic version of the usual reductions that transfer a winning strategy from one game to the other. In this talk we will present a new characterization of $\forall\Sigma^b_k$ consequences of the theory S^k_2 via the existence of a polynomially long sequence of k-turn games augmented with a sequence of reduction programs between them.

18:00 End of Talks

Tuesday November 6

9:00 Pavel Pudlák TBA

10:00 Arnold Beckmann On Transformations of Constant Depth Propositional Proofs

In this talk we study the complexity of constant depth propositional proofs in the cedent and sequent calculus. We discuss the relationships between the size of tree-like proofs, the size of dag-like proofs, and the heights of proofs. One focus is to correct a proof construction in an earlier paper of the same authors about transformations from proofs with polylogarithmic height and constantly many formulas per cedent. This is joint work with Sam Buss.

10:30 Coffee

11:00 Sam Buss DRAT proofs and Extensions

12:00 End of Talks

12:30 Lunch

15:30 Coffee

16:00 Ilario Bonacina k-Clique is Hard on Average for Regular Resolution

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

This talk is based on on a joint work with A. Atserias, S. De Rezende, M. Lauria, J. Nordström and A. Razborov

16:30 Massimo Lauria Graph Colouring is Hard for Algorithms Based on Hilbert's Nullstellensatz and Gröbner Bases

We consider the graph k-colouring problem encoded as a set of polynomial equations in the standard way. We prove that there are bounded-degree graphs that do not have legal k-colourings but for which the polynomial calculus proof system defined in [Clegg et. al. '96, Alekhnovich et. al. '02] requires linear degree, and hence exponential size, to establish this fact. This implies a linear degree lower bound for any algorithms based on Gröbner bases solving graph k-colouring using this encoding. The same bound applies also for the algorithm studied in a sequence of papers [De Loera et. al. '08, '09, '11, '15] based on Hilbert's Nullstellensatz proofs for a slightly different encoding, thus resolving an open problem mentioned, e.g., in [De Loera et. al. '09] and [Li et. al. '16]. We obtain our results by combining the polynomial calculus degree lower bound for functional pigeonhole principle (FPHP) formulas over bounded-degree bipartite graphs in Miksa and Nordström '15] with a reduction from FPHP to k-colouring derivable by polynomial calculus in constant degree.

Joint work with Jakob Nordstrom (appeared on CCC, 2017)

17:00 Stefan Dantchev Resolution and the binary encoding of combinatorial principles

We investigate the size of refutations in Res(k), an extension of Resolution working on k-DNFs instead of clauses, for certain contradictions given in the less usual binary encoding. In particular, we prove lower bounds for binary k-Clique principle as well as for the Weak Pigeon-Hole Principle. Previously, a resolution lower bound was known for the former while the later was considered in the more usual unary encoding only.

17:30 Neil Thapen Approximate counting and NP search problems

18:00 End of Talks

Wednesday November 7

9:00 Azza Gaysin The structure of weighted clones over the clones of the Post lattice

There is well-known Galois correspondence between function clones and relational clones, that allows one to study the computational complexity of the constraint satisfaction problem (CSP) in an alternative and very useful way. D. A. Cohen, M. C. Cooper, P. Creed, P. G. Jeavons and S. Živný introduced the concepts of weighted relational clones and weighted clones, that for valued constraint satisfaction problem (VCSP) play the same role as relational clones and function clones for CSP, and proved a one-to-one correspondence between these structures. We efforted to characterize weighted clones over the clones of the Post lattice. We fully describe the structure of all binary parts of weighted clones over the Boolean clones generated by one of the semilattice operations and one or two of the constant operations. We also give a complete description of all atomic and maximal weighted clones over these clones.

9:30 Lukáš Folwarczný Graph communication protocols

Graph communication protocols are a generalization of communication protocols to the case when the underlying graph is a directed acyclic graph. Recently, new types of these protocols have been introduced. In the talk, we will discuss our theorems on the relative strength of various types of these protocols. Furthermore, we explain how obtaining lower bounds for stronger types of the considered protocols would lead to applications in proof complexity. For example, lower bounds for resolution with parities could be obtained via this direction of research. The talk is based on the speaker's master thesis, supervised by Pavel Pudlák.

10:00 Raheleh Jalali On lengths of proofs in centered calculi

Iemhoff introduced the notion of a centered axiom and a centered rule as the building blocks of a certain form of sequent calculus which she calls a centered proof system. She then showed how the existence of a terminating centered system implies the uniform interpolation property for the logic that the calculus captures. In this talk, we first generalize her centered rules to semi-analytic rules, a dramatically powerful generalization, and then we will show how the semi-analytic calculi consisting of these rules together with our generalization of her centered axioms, lead to the feasible Craig interpolation property. Then, we will define a certain specific type of semi-analytic calculus which we call PPF systems. We will show that all such PPF calculi are exponentially slower than the classical Hilbert-style proof system (or equivalently $\mathbf{LK} + \mathbf{Cut}$*). We will then present a similar exponential lower bound for a certain form of complete PPF calculi, this time for any super-intuitionistic logic.*

10:30 Coffee

11:00 Navid Talebanfard On the Fine-Grained Proof Complexity of Tseitin Tautologies

In the light of Non-deterministic Exponential Time Hypothesis I will talk about non-trivial exponential size refutations of unsatisfiable k-CNF formulas. I will show that for Tseitin formulas on graphs and hypergraphs it is possible to achieve better than the usual $1/k$ *savings even in tree-like resolution. Based on ongoing work with Vojtěch Rödl.*

11:30 End of Talks