# Prague Bounded Arithmetic Workshop 2017

Institute of Mathematics of the ASCR, Žitná 25, 115 67 Praha 1.
Talks are in the blue lecture room. From the main street door of the institute, go across the courtyard and through the glass doors at the back. The lecture room is then through the door on the left.

## Thursday November 2

**9:00** coffee

**9:20** opening

**9:30 Sam Buss** Expander construction in $\mathrm{VNC}_1$

*This talk discusses a combinatorial analysis of a variant of the iterative expander construction due to Reingold, Vadhan, and Wigderson [2002], and that this analysis can be formalized in the bounded-arithmetic system $VNC_1$. This proves the assumption made by Jeřábek [2011] that a construction of certain bipartite expander graphs can be formalized in $VNC_1$. This in turn implies that every proof in Gentzen's sequent calculus LK of a monotone sequent can be simulated in the monotone version MLK of LK with only polynomial blowup in proof size, strengthening the quasipolynomial simulation result of Atserias, Galesi, and Pudlák [2002]. This is joint work with Valentine Kabanets, Antonina Kolokolova, and Michal Koucký.*

**10:30** coffee

**11:00 Andrés Cordón Franco** Local variants of the induction principle: an overview

Local induction *theories are subsystems of first-order Peano Arithmetic obtained by restricting the conclusion of the induction principle to elements of a prescribed class only. In this talk we investigate the theories of $\Sigma_n$-induction restricted to $\Sigma_m$-definable elements $I(\Sigma_n, \mathcal{K}_m)$ for each $1 \leq n, m$. For $n = m$, we show that these theories provide us with reformulations of the scheme of parameter free $\Pi_n$-induction $I\Pi_n^-$. For $n > m$, we prove that these theories correspond to* local reflection principles. *For $n < m$, it is still pending to determine the exact proof-theoretic strength of local induction.*

**12:00** lunch

**13:00** coffee

**14:00 Emil Jeřábek** Pigeons for Lagrange

*The Lagrange four-square theorem is provable in bounded arithmetic, as was observed by Berarducci and Intrigila a long time ago. However, it is not clear how strong a fragment we actually need to prove the theorem. We will have a look at the options.*

**15:00 Francisco Félix Lara Martín** On collapse properties of local induction rules

*We say that an inference rule $R$ collapses over a theory $T$ if $T + R$ (the closure of $T$ under first order logic and nested applications of $R$) is equivalent to $[T, R]$ (the closure of $T$ under first order logic and unnested applications of $R$). In this talk we discuss general collapse results for local induction rules. Applications to conservation results will also be described for fragments of Peano Arithmetic axiomatized by parameter free induction schemes.*

**15:30** coffee

**16:00 Gilda Ferreira** Analysis in weak systems

*Weak analysis can be described as the formalization and development of analysis in very weak systems of second-order arithmetic. These systems do not prove the totality of the exponential function.*

*In this talk we present systems of weak analysis and show how they are constructed from well-known bounded arithmetic theories connected with some classes of computational complexity such as polytime, polyspace and counting functions. We briefly illustrate how the formalization of analysis is done in such systems.*

**16:30 Ján Pich** Feasibly constructive proofs of succinct weak circuit lower bounds

*The existing circuit lower bounds for explicit Boolean functions are very constructive, as captured in the notion of natural proofs. Following initial work of Razborov and Krajíček, we investigate the constructive aspects of circuit lower bounds from the perspective of mathematical logic and show that $AC^0$, $AC^0[p]$ and monotone circuit lower bounds expressed by $\forall\Sigma^b_1$ formulas are provable in Jeřábek's theory of approximate counting $APC_1$. Consequently, we obtain short propositional (almost WF) proofs of poly$(n)$-size tautologies expressing these circuit lower bounds, where $n$ is the number of inputs of the circuit.*

**17:00** (end of talks)

**19:00 Villa Lanna**

Presentation of the Bolzano medal. Buffet dinner. The villa is at the corner of Pelléova and Na Seníku streets, a short walk from Hradčanská metro station.

## Friday November 3

**9:00** coffee

**9:15 Petr Glivický** Shepherdson's theorems for fragments of open induction

*By a well-known result of Shepherdson, models of the theory IOpen (open induction) are exactly all the discretely ordered semirings that are integer parts of their real closures. In this talk we show several analogous results that provide algebraic equivalents to various fragments of IOpen. This is a joint work with Jana Glivická.*

**9:45 Jan Krajíček** Expansions of pseudo-finite structures

*I shall explain how some problems in computational and proof complexity can be viewed as tasks to construct expansions of pseudo-finite structures with particular properties, and how one can go about it. In particular, I will discuss the method of forcing with random variables.*

**10:45** coffee

**11:15 Arnold Beckmann** Consistency of equational theories and the separation problem for bounded arithmetic

*Consistency statements of formal theories have been considered as candidates for separating theories of bounded arithmetic. The most promising ones are given by consistency statements of certain equational theories. The starting points are results by Buss and Ignjatovic 1995, which showed that the consistency of an induction free version of the equational theory PV is not provable in $S^1_2$, and Beckmann 2002, which showed that a further restricted induction free version of PV is provable in $S^1_2$.*

*We review those results and in particular state them precisely. We then explain the progress that has been made over recent years to narrow the gap between provability and unprovability, and the potential research programme that is related to this question.*

**12:15** lunch

**13:00** coffee

**14:00 Leszek Kołodziejczyk** Separating Jeřábek's theory for approximate counting from bounded arithmetic

*A major open problem in bounded arithmetic concerns separating relativized versions of the theories $T^n_2$ by means of universal closures of $\Sigma^b_1$ formulas. A challenging subcase of this problem, first noticed around 2010, was to find a sentence of the above form provable in bounded arithmetic but not in Jeřábek's theory for approximate counting, sometimes known as $APC_2$. A number of papers by various researchers led to independence results for interesting fragments of $APC_2$, and finally, this year, for the full theory itself. My talk will be a survey of these developments.*

**15:00 Anupam Das** Some theories of bounded arithmetic for monotone (proof) complexity

*I will introduce some intuitionistic versions of second-order theories of bounded arithmetic for reasoning about monotone (proof) complexity. The main result is the development of a system, $I^1U^1_2$, corresponding to the tree-like monotone sequent calculus (tree-MLK). The propositional translation of $\Pi_1$-theorems of $I^1U^1_2$ into tree-MLK relies on a calibration of the usual Paris-Wilkie translation with a sort of 'realisability' interpretation of intuitionistic implication, at the level of propositional derivations, and operates in quasipolynomial time. Time permitting, I will also present some ideas in an ongoing line of work on identifying theories for complexity classes of monotone functions in general.*

**15:30** coffee

**16:00 Konrad Zdanowski** Truth predicates for $\Delta_0$ formulas and PSPACE computations

*We consider a bounded arithmetic in Buss's language enriched with a predicate Tr which is assumed to be a truth definition for bounded sentences. Among other things we assume polynomial induction for $\Sigma^b_1(Tr)$ formulas. We show that such an arithmetic captures PSPACE. It follows that the problem of the existence of a truth definition for $\Delta_0$ sentences without the totality of* exp *might be more about separating subexponential time alternation hierarchies from PSPACE.*

**16:30 Chris Pollett** Normal forms from witnessing arguments

*An early bounded arithmetic result of Sam Buss shows that for $i \geq 1$, $S^{i+1}_2$ is $\forall\Sigma^b_{i+1}$-conservative over $T^i_2$. Although not shown in the paper of this result, the technique of query definitions used to show this implies that all $\Delta^b_{i+1}$-predicates of $S^{i+1}_2$ can be provably in $T^i_2$ converted to formulas of a normal form related to bit comprehension for $\Sigma^b_i$-formulas. In this talk, we explore this normal form and its variants as well as normal forms for the $\hat{\Delta}^b_1$-consequences of $S^1_2$ and $\hat{R}^1_2$. We look at how these normal forms can be used to simplify finite axiomatization results, and, in turn, how this may help in trying to separate $S^1_2$ from $\hat{R}^1_2$.*

**17:00 Amir Tabatabai** Computational flows in arithmetic

*A computational flow is a pair consisting of a sequence of computational problems of a certain sort and a sequence of computational reductions among them. In this talk we will explain the basics of the theory of computational flows and how they make a sound and complete interpretation for bounded theories of arithmetic. This property helps us to decompose a first order arithmetical proof into a sequence of computational reductions by which we can extract the computational content of the low complexity statements in some bounded theories of arithmetic such as $I\Delta_0$, $T^k_n$, $I\Delta_0$+EXP and PRA.*

**17:30** (end of talks)