ЯUSSIAN WORKSHOP ON COMPLEXITY AND MODEL THEORY

9–11 JUNE 2019

ABSTRACTS

ЯUS WCMT

The Ministry of Education and Science of the Russian Federation
Federal State Autonomous Institution of Higher Education
“Moscow Institute of Physics and Technology
(National Research University)” (MIPT)

RUSSIAN WORKSHOP ON COMPLEXITY AND MODEL THEORY

Abstracts

June 9–11, 2019 MIPT Moscow, Russia

MIPT
MOSCOW INSTITUTE OF PHYSICS AND TECHNOLOGY

UDK 519.17(043.2)
BBK 22.176я5

Workshop on graphs, networks and their applications
Abstracts / May 13–18, 2019. – Moscow, Russia. – M. : MIPT, 2019. – 48 p.
ISBN 978-5-6041-1875-7

ISBN 978-5-6041-1875-7

RUS WCMT

Organizing Committee

Andrei M. Raigorodskii (MIPT, Yandex)

Vladimir Remeslennikov (Institute of Mathematics, Siberian Branch of the Russian Academy of Sciences)

Maksim Zhukovskii (MIPT)

MIPT

Moscow Institute of Physics and Technology

algorithms

Algorithms an Open Access Journal by MDPI

Yandex

Yandex

HUAWEI

Huawei

CONTENTS

PLENARY TALKS

ERICH GRÄDEL

PROVENANCE ANALYSIS FOR LOGIC AND GAMES

A model checking computation checks whether a given logical sentence is true in a given finite structure. Provenance analysis, based on interpretations in commutative semirings, abstracts from such a computation mathematical information on how the result depends on the atomic data that describe the structure. In this approach, atomic facts are interpreted not just by true or false, but by values in an appropriate semiring, where 0 is the value of false statements, whereas any element $a \neq 0$ of the semiring stands for some shade of truth. These values are then propagated from the atomic facts to arbitrary statements in the language. In database theory, provenance analysis has been successfully developed for positive query languages such a unions of conjunctive queries, positive relational algebra, or datalog. However, it did not really offer an adequate treatment of negation or missing information.

We propose a new approach for the provenance analysis of logics with negation, such as first-order logic and fixed-point logics. It is closely related to a provenance analysis of the associated model-checking games, and based on new provenance semirings of polynomials and formal power series, which take negation into account. They are obtained by taking quotients of traditional provenance semirings by congruences generated by products of positive and negative provenance tokens; they are called semirings of dual-indeterminate polynomials or dual-indeterminate power series.

Beyond the use for model-checking problems in logics, provenance analysis of games is of independent interest. Provenance values in games provide detailed information about the number and properties of the strategies of the players, far beyond the question whether or not a player has a winning strategy from a given position.

This is joint work with Val Tannen

BRUNO COURCELLE

STRUCTURED GRAPHS AND THE VERIFICATION OF THEIR MONADIC SECOND-ORDER PROPERTIES BY MEANS OF AUTOMATA

Algorithmic meta-theorems relate the logical expression of a graph property to the complexity of checking it for graphs belonging to certain classes of graphs. Such results actually extend to relational structures. There are many results for first-order (FO) logic and classes of sparse, unstructured graphs, like planar graphs or graphs of bounded degree. However, FO logic is rather weak for expressing graph properties.

Monadic second-order (MSO) logic is much more expressive. This language uses quantifications on sets of vertices and, in some cases, on sets of edges. The graph classes that allow linear-time algorithms for verifying MSO properties are (necessarly) characterized by bounds on tree-width or clique-width. These bounds are parameters in the sense of Fixed Parameter Tractability. They are associated with hierarchical descriptions *(i.e.* tree-structurings) of the input graphs (of two different, but related types). Linear-time algorithms are obtained for graphs given with the relevant decompositions, that are not easy to compute.

The standard proofs of the meta-theorems construct from MSO sentences and given bounds on tree-width or clique-width, finite automata intended to run on tree-decompositions (expressed by algebraic terms) or on clique-width terms. However, these automata have so many states that their constructions are not usable in practice. This is actually unavoidable (Frick and Grohe, 2004). To overcome this difficulty, we (Irène Durand and myself) have introduced *fly-automata*. These automata do not store states and transitions but compute them, whenever needed. Only the necessary transitions are computed. They have been implemented and tested, in particular for NP-complete problems about coloring and Hamiltonicity.

The lecture will review : 1) the main results for FO logic, 2) the (well-known) notion of *tree-decomposition*, 3) the notion of *clique-width*, a graph complexity measure based on three elementary graph operations, from which graphs are constructed, 4) graph classes for which *tree-width*$(G) = O($*clique-width*$(G))$, 5) the construction of *fly-automata* for clique-width terms (and the verification of MSO graph properties), and 6) their extensions to *counting and optimization problems* : for example, computing the number of k-colorings, or of k-acyclic colorings, of a given graph.

An on-line software (called TRAG, by I. Durand and M. Raskin) implements some predefined fly-automata and the automatic construction of a fly-automaton from an MSO sentence. It also includes the construction of the necessary decompositions for « small » random graphs and for « large » regular ones. A demonstration can be made outside of the main lecture. This is joint work with Irène Durand (LaBRI, Bordeaux University).

References

[1] B.Courcelle and J.Engelfriet, *Graph structure and monadic second-order logic, a language theoretic approach,* 728 pages, *Cambridge University Press*, 2012.

[2] B. Courcelle and I.Durand, Automata for the verification of monadic second-order graph properties, *J. Applied Logic* **10** (2012) 368-409, http://hal.archives-ouvertes.fr/hal-00611853/fr/

[3] B. Courcelle and I.Durand, Computation by fly-automata beyond monadic second-order logic, *Theoretical Computer Science*, **619** (2016) 32-67, http://hal.archives-ouvertes.fr/hal-00828211

[4] B.Courcelle, From tree-decompositions to clique-width terms, *Discrete Applied Mathematics*, **248** (2018) 125-144, https://hal.archives-ouvertes.fr/hal-01398972

VLADIMIR REMESLENNIKOV

SWITCH TRANSFORMATIONS AND A TRIANGLE-CREATION PROCESS IN REGULAR GRAPHS

The main purpose of this report is to give an outline of important results on the universal theory of simple graphs in the formal language of two predicates: the "predicate of equality" $x = y$, and the "neighbourhood predicate" $E(x, y)$, defined on the vertices of the graph G.

Summary of the content of the report:

Three equivalences on the vertices of the graph $X = V(T)$ are made, and the concept of a squeezed graph introduced.

The definition of the category of simple graphs with labels is given.

The definition and properties of the three main universal graph invariants are given.

The main universal classes of finite squeezed graphs are described.

Pseudo-Boolean graphs are introduced and the Rado theorem for direct products of pseudo-Boolean graphs is stated.

Universal classes of graphs of finite height and width are defined, and the Rado theorem for them is stated.

As this material is difficult to cover in a single report, associated results, obtained by the application of this approach, will be presented in the reports of E. Daniarova and A. Treyer

VITALY ROMAN'KOV

ALGEBRAIC CRYPTOLOGY: METHODS OF CRYPTANALYSIS VIA (NON)LINEAR DECOMPOSITION AND NEW PROTECTION AGAINST THEM

The talk is devoted to algebraic cryptology, that is an area of investigation which operates with algebraic structures (groups, rings and so on) in construction of cryptographic schemes. This area is a part of post-quatum cryptography which developes schemes resistant against attacks via quatum computers of potentially high power,

See [1] and [2] for basic notions and results in algebraic cryptography.

In the first part of the talk, we discuss an attack, termed a *linear decomposition* attack, on many of known in literature group-based cryptosystems. This attack gives a polynomial time deterministic algorithm that recovers the secret shared key from the public data in the schemes under consideration. Furthermore, we show that in this case, contrary to the common opinion, the typical computational security assumptions are not very relevant to the security of the schemes, i.e., one can break the schemes without solving the algorithmic problems on which the assumptions are based. In a number of monographs and papers, we have shown that in many systems of algebraic cryptography, where the platform group G is a subset in a linear space over a finite or infinite field, we can efficiently solve the computational Diffie-Hellman-like problems and hence to compromise the corresponding cryptographic systems. Other and in some points similar approach was established by Tsaban et al. Also we discuss a non-linear decomposition attack that can be applied in many other cases, in particular, when the platform is a polycyclic group. We present two general schemes for which many schemes are specific realizations. One of these two schemes joins schemes based on two-side multiplications, the second scheme joins schemes based on automorphisms. The two mentioned above attacks show vulnerability of these two general schemes. The main ideas and applications of the (non)linear decomposition methods are presented in papers [3-8] and monographs [9-10] (see also the bibliography in [10]).

In the second part of the talk, we introduce a novel method that is resistant against linear algebra attacks. In particular, we propose an improved version of the famous Anshel-Anshel-Goldfeld algebraic cryptographic key-exchange scheme, that is in particular resistant against the Tsaban et al. linear span cryptanalysis. Unlike the original version, that based on the intractability of the simultaneous conjugacy search problem for the platform group, the proposed version is based on much more hard simultaneous membership-conjugacy search problem and needs to solve the membership problem for a subset of the platform group that can be easily and efficiently built as very complicated and without any good structure. A number of other hard problems should be previously solved by any intruder to start solving of the simultaneous membership-conjugacy search problem to obtain the exchanged key. We also show how this new approach

can be used to improve many schemes based on the conjugacy search algorithmic problem. These results are presented in [11]

REFERENCES.

[1] A.G. Myasnikov, V. Shpilrain, and A. Ushakov. *Group-based Cryptography. Advanced Courses in Math.* – CRM Barselona, Birkhauser, Basel, 2008.

[2] A. Myasnikov, V. Shpilrain, and A. Ushakov. *Non-commutative Cryptography and Complexity of Group-theoretic Problems. With appendix by Natalia Mosina.* Math. Surveys and Monographs, Vol. 177, American Mathematical Society, Providence, Rhode Island, 2011.

[3]V.A. Roman'kov. *Cryptanalysis of some schemes applying automorphisms.* Prikladnaya Discretnaya Matematika. No. 21, 2013, 35–51 (in Russian).

[4] V.A. Roman'kov. *A nonlinear decomposition attack.* Groups, Complexity, Cryptology, Vol. 9, No. 2, 2017. 197–207.

[5] V.A. Roman'kov, A.A. Obzor. *General algebraic cryptographic key exchange scheme and its cryptanalysis.* Applied Discrete Math., No. 37, 2017, 52–61 (in Russian).

[6] A. Myasnikov, V. Roman'kov. *A linear decomposition attack.* Groups, Complexity, Cryptology, Vol. 7, No. 1, 2015. 81–94.

[7] V.A. Roman'kov. *Two general schemes of algebraic cryptography.* Groups, Complexity, Cryptology, Vol. 10, No. 2, 2018. 83–207.

[8] V.A. Roman'kov, A.A. Obzor. *General algebraic cryptographic key exchange scheme and its cryptanalysis.* Prikladnaya Discretnaya Matematika. No. 37, 2017, 52–61 (in Russian).

[9] V. A. Roman'kov. Algebraic cryptography. Omsk, Omsk State University, 2013, 135 p. (in Russian).

[10] V.A. Roman'kov. Essays in algebra and cryptology: Algebraic cryptanalysis. Omsk: OmSU, 2018. 207 p.

[11] V.A. Roman'kov. *An improved version of the AAG cryptographic protocol.* Groups, Complexity, Cryptology, Vol. 11, No. 1, 2019.

ANUJ DAWAR

APPROXIMATIONS OF GRAPH ISOMORPHISM

The problem of deciding whether two given graphs are isomorphic is a well-studied problem in computational complexity as it is one of the few natural problems which is not known to be solvable in polynomial time nor known to be NP-hard. In this talk, I will discuss equivalence relations that over-approximate graph isomorphism but are decidable in polynomial-time. One such class of relations are the Weisfeiler-Lehman equivalences, which have a large variety of equivalent characterisations emerging separately from algebra, combinatorics and logic. I will then discuss equivalence relations that strengthen this by considering invertible maps over finite fields, and present some recent results on them.

JAROSLAV NEŠETŘIL

LIMITS OF FINITE STRUCTURES

Starting from graph limit theory emerged structural limits on the crossroad of model theory, combinatorics and algorithms. We survey recent activity related to structural limits which is both analytic and model theoretic and leads to a surprising connection to new techniques in clustering and modeling of sparsity and stability.

This is a joint work with Patrice Ossona de Mendez (Paris and Prague).

JOHANN A. MAKOWSKY

A LOGICIAN'S VIEW OF GRAPH POLYNOMIALS

We give a survey on graph polynomials, their expressive power and their complexity of evaluation, based on the following recent papers. We also discuss some conjectures and open problems.

- JA Makowsky, EV Ravve, T Kotek,
  A logician's view of graph polynomials
  Annals of Pure and Applied Logic, to appear 2019
  https://arxiv.org/abs/1703.02297
- A Goodall, M Hermann, T Kotek, JA Makowsky, SD Noble
  On the complexity of generalized chromatic polynomials
  Advances in Applied Mathematics 94, 71-102, 2018
  https://arxiv.org/abs/1701.06639
- V Rakita, JA Makowsky
  On Weakly Distinguishing Graph Polynomials
  Discrete Mathematics Theoretical Computer Science 21, 2019
  https://arxiv.org/pdf/1810.13300
- JA Makowsky, RX Zhang
  On P-unique hypergraphs
  Australasian Journal of Combinatorics , 2019
  https://arxiv.org/abs/1712.07357

NIKOLAY VERESHCHAGIN

A CONDITIONAL INFORMATION INEQUALITY AND ITS COMBINATORIAL APPLICATIONS

We show that the inequality $H(A|B,X)+H(A|B,Y) \leqslant H(A|B)$ for jointly distributed random variables A, B, X, Y, which does not hold in general case, holds under some natural condition on the support of the probability distribution of A, B, X, Y. This result generalizes a version of the conditional Ingleton inequality: if for some distribution $I(X:Y|A) = H(A|X,Y) = 0$, then $I(A:B) \leqslant I(A:B|X) + I(A:B|Y) + I(X:Y)$.

We present two applications of our result. The first one is the following easy-to-formulate theorem on edge colorings of bipartite graphs: assume that the edges of a bipartite graph are colored in K colors so that each two edges sharing a vertex have different colors and for each pair (left vertex x, right vertex y) there is at most one color a such both x and y are incident to edges with color a; assume further that the degree of each left vertex is at least L and the degree of each right vertex is at least R. Then $K \geqslant LR$. The second application is a new method to prove lower bounds for biclique cover of bipartite graphs.

Joint works Tarik Kacedy, Andrei Romashchenkoz and Nikolay Vereshchaginx

*While working on the paper the authors were in part supported by RFBR grants 14-01-93107, 16-01-00362, by an ANR-15-CE40-0016-01 grant RaCAF, and by the Russian Academic Excellence Project '5-100'.

LANCE FORTNOW

THE P V NP PROBLEM IN THE ERA OF BIG DATA AND FAST COMPUTING

The P v NP problem asks if every problem where we can efficiently verify a solution, we can also efficiently find that solution. The P v NP problem is a great mathematical challenge, one of the Clay Math Millennial problems, and we'll review the (limited) progress towards separating P and NP.

The importance of the P v NP came from real-world algorithmic challenges and advances in hardware and algorithms have let us solve NP problems in ways we never thought we could solve years ago. We discuss this progress and the implications across computer science and society in general.

ANDREI BULATOV

THE COMPLEXITY OF THE CONSTRAINT SATISFACTION PROBLEM

It has been observed long time ago that 'natural' computational problems tend to be complete in 'natural' complexity classes such as NL, P, NP, or PSPACE. Although Ladner in 1975 proved that if P≠NP then there are infinitely many complexity classes between them, all the examples of such intermediate problems are based on diagonalization constructions and are very artificial. Since the seminal work by Feder and Vardi [8] this phenomenon is known as complexity dichotomy (for P and NP), see also Valiant's work [14] in the context of counting problems. Concerted efforts have been made to make this observation more precise, and since the concept of a 'natural' problem is somewhat ambiguous, a possible research direction is to pursue dichotomy results for wide classes of problems. The Constraint Satisfaction problem (CSP) is one of such classes.

Feder and Vardi in [8] observed that the CSP can be conveniently represented as the problem of deciding the existence of a homomorphism between relational structures. In particular, they emphasized the importance of nonuniform CSPs, that is, ones of the form $\mathrm{CSP}(\mathcal{H})$, which asks, given a structure $\mathcal{G}$, whether there exists a homomorphism from a structure $\mathcal{G}$ to a fixed structure $\mathcal{H}$. This problem belongs to NP in general, but can be solved in polynomial time for some structures $\mathcal{H}$. Early dichotomy results on nonuniform CSPs can be traced back to Schaefer [13] for the Generalized Satisfiability problem ($\mathcal{H}$ is 2-element), and Hell and Nesetril [9] for the H-Colouring problem ($\mathcal{H}$ is a graph). A systematic study of the complexity of nonuniform CSPs was initiated in [8], where among other advances Feder and Vardi posed the CSP Dichotomy Conjecture, which is the focus of this tutorial: For every relational structure $\mathcal{H}$ the problem $\mathrm{CSP}(\mathcal{H})$ is either solvable in polynomial time or is NP-complete.

While a wide variety of methods based on model theory, database theory, graph homomorphisms, etc. have been used to attack the dichotomy conjecture, it was the discovery of the *algebraic approach* by Jeavons et al. [11] (see also [2]) that played the decisive role in resolving the conjecture. Using the algebraic approach the dichotomy conjecture was confirmed in a number of important cases, see, e.g., [1, 3, 4, 5, 10]. A recent collection of surveys on intermediate results on the complexity of the CSP and its variants, as well as, other applications of the algebraic approach can be found in [12]. Finally, in 2017 the Bulatov and Zhuk independently confirmed the dichotomy conjecture [6, 15] for arbitrary finite relational structures. For a less technical presentation of the first of these results see [7].

In the first half of this tutorial we survey the connections of the CSP and the dichotomy conjecture with other areas of logic and computer science, and outline the history of the problem. In the second half we explain the main ideas of the first of the solution algorithms [6, 15] for nonuniform CSPs and provide some examples.

References

[1] Libor Barto and Marcin Kozik. Constraint satisfaction problems solvable by local consistency methods. *J. ACM*, 61(1):3:1–3:19, 2014.

[2] Andrei A. Bulatov, Peter Jeavons, and Andrei A. Krokhin. Classifying the complexity of constraints using finite algebras. *SIAM J. Comput.*, 34(3), 720–742, 2005.

[3] Andrei A. Bulatov. A dichotomy theorem for constraint satisfaction problems on a 3-element set. *J. ACM*, 53(1):66–120, 2006.

[4] Andrei A. Bulatov. Complexity of conservative constraint satisfaction problems. *ACM Trans. Comput. Log.*, 12(4):24, 2011.

[5] Andrei A. Bulatov. Graphs of relational structures: restricted types. In *LICS*, pages 642–651, 2016.

[6] Andrei A. Bulatov. A dichotomy theorem for nonuniform CSPs. In *FOCS*, pages 319–330, 2017. (A full version of the paper can be found in CoRR abs/1703.03021.)

[7] Andrei A. Bulatov. Constraint satisfaction problems: complexity and algorithms. *SIGLOG News*, 5(4):4–24, 2018.

[8] Tomas Feder and Moshe Y. Vardi. Monotone monadic SNP and constraint satisfaction. In *STOC*, pages 612–622, 1993.

[9] Pavol Hell and Jaroslav Nešetřil. On the complexity of H-coloring. *J. Comb. Th., Ser.B*, 48:92–110, 1990.

[10] Paweł M. Idziak, Petar Markovic, Ralph McKenzie, Matthew Valeriote, and Ross Willard. Tractability and learnability arising from algebras with few subpowers. *SIAM J. Comput.*, 39(7), 3023–3037, 2010.

[11] Peter G. Jeavons, David A. Cohen, and Marc Gyssens. Closure properties of constraints. *J. ACM*, 44(4):527–548, 1997.

[12] Andrei A. Krokhin and Stanislav Zivny (eds.). The Constraint Satisfaction Problem: Complexity and Approximability. *Dagstuhl Follow-Ups*, vol. 7, Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2017.

[13] Thomas J. Schaefer. The complexity of satisfiability problems. In *STOC*, pages 216–226, 1978.

[14] Leslie G. Valiant. Accidental Algorithms. In *FOCS*, pages 509–517, 2006.

[15] Dmitriy Zhuk. A Proof of CSP Dichotomy Conjecture. In *FOCS*, pages 331–342, 2017.

IGOR PAK

COUNTING INTEGER POINTS IN POLYTOPES

What is the number of integer points in a convex polytope? This problem is of great interest in combinatorics and discrete geometry, with many important applications ranging from integer programming to statistics. From computational point of view it is hopeless in many dimensions, as the knapsack problem is a special case. Perhaps surprisingly, in bounded dimension the problem becomes tractable. How far can one go? Can one count points in projections of polytopes, finite intersections of such projections, etc?

We will survey both classical and recent results on the problem, emphasizing both algorithmic and complexity aspects. Some elegant hardness results will make an appearance in dimension as small as three. If time permits, we will discuss connections to Presburger Arithmetic and decidability problems for irrational polyhedra.

Joint work with Danny Nguyen.

NOAM NISAN

THE COMMUNICATION COMPLEXITY OF CAKE-CUTTING

This talk concerns the well-studied model of "cake-cutting" for studying questions regarding notions of fair division of resources. We focus on discrete versions rather than using infinite-precision real values, specifically, focusing on the communication complexity. Using general discrete simulations of classical infinite-precision protocols (Robertson-Webb and moving-knife), we roughly partition the various fair-allocation problems into 3 classes: "easy" (constant number of rounds of logarithmic many bits), "medium" (poly-log total communication), and "hard".

Our main technical result concerns two of the "medium" problems (perfect allocation for 2 players and equitable allocation for any number of players) which we prove are not in the "easy" class. Our main open problem is to separate the "hard" from the "medium" classes.

Joint work with Simina Brânzei

ALEXEI MIASNIKOV

HARD INSTANCES, CHALLENGER-SOLVER COMPLEXITY, AND DEHN MONSTERS

Every hard computational problem has some hard instances, that form a "hard core" of the problem. In this talk I will discuss if the hard cores do exist, how easy is to sample hard cores, how one can measure "hardness" of the instances, etc. Our approach is based on Challenger-Solver games, introduced some time ago by Yuri Gurevich. A modification of the famous Golod-Shafarevich construction of infinite periodic groups provides first examples of natural easily samplable "really hard" cores. This leads to a discussion of computational hardness of search problems and descriptive complexity.

MOSHE VARDI

THE AUTOMATED-REASONING REVOLUTION: FROM THEORY TO PRACTICE AND BACK

For the past 40 years computer scientists generally believed that NP-complete problems are intractable. In particular, Boolean satisfiability (SAT), as a paradigmatic automated-reasoning problem, has been considered to be intractable. Over the past 20 years, however, there has been a quiet, but dramatic, revolution, and very large SAT instances are now being solved routinely as part of software and hardware design. In this talk I will review this amazing development and show how automated reasoning is now an industrial reality.

I will then describe how we can leverage SAT solving to accomplish other automated-reasoning tasks. Sampling uniformly at random satisfying truth assignments of a given Boolean formula or counting the number of such assignments are both fundamental computational problems in computer science with applications in software testing, software synthesis, machine learning, personalized learning, and more. While the theory of these problems has been thoroughly investigated since the 1980s, approximation algorithms developed by theoreticians do not scale up to industrial-sized instances. Algorithms used by the industry offer better scalability, but give up certain correctness guarantees to achieve scalability. We describe a novel approach, based on universal hashing and Satisfiability Modulo Theory, that scales to formulas with hundreds of thousands of variables without giving up correctness guarantees.

TALKS

ALEXANDER TREYER

UNIVERSAL EQUIVALENCE OF NILPOTENT GRAPH GROUPS

Let Γ be a finite simple graph. The graph group G_Γ (also known as partially commutative group) is the group such that the vertex set of Γ serves as the generator set, and relations are as follows: two generators x and y commute (i.e. $[x, y] = 1$) if and only if the vertices x and y are connected by an edge in the graph Γ. Graph groups can be defined in various varieties of groups, for example, in the variety of nilpotent groups, solvable groups, etc. Two groups are called universally equivalent if the sets of all universal sentences which hold on these groups coincide. Five years earlier, the author together with A.A. Mishchenko proved a criterion for universal equivalence of two nilpotent graph groups. The resulting criterion was complicated and computationally hard. In the talk a new convenient approach to the description of universally equivalent nilpotent graph groups will be proposed. The new approach based on the notion of closed subset of vertices of Γ, compression of Γ and lattice of closed subsets of Γ.

MIKHAIL MAKAROV

LOGICAL COMPLEXITY OF INDUCED SUBGRAPH ISOMORPHISM FOR CERTAIN GRAPH FAMILIES

For a given graph F, let $v(F)$ be the number of its vertices, $\mathcal{I}(F)$ denote the class of all graphs containing a copy of F as an induced subgraph, and $D[F]$ denote the minimum quantifier depth of a sentence in first-order logic with adjacency and equality relations that defines $\mathcal{I}(F)$. It is obvious that $D[F] \leq v(F)$. In [1] it has been shown that $D[F] = 4$ for all graphs F on 4 vertices except for paw graph $K_3 + e$ and its complement, for which $D[F] = 3$.

Our contribution is the following. For all $\ell > 4$, we give an example of graph F on ℓ vertices such that $D[F] = \ell - 1$. Also, we prove that if all of the components of F are pairwise isomorphic complete multipartite graphs, then $D[F] = \ell$. Finally, we show that, for every F on 5 vertices, $D[F] \geq 4$.

References

[1] O. Verbitsky, M. Zhukovskii, "On the First-Order Complexity of Induced Subgraph Isomorphism", *26th EACSL Annual Conference on Computer Science Logic (CSL 2017)*, Leibniz International Proceedings in Informatics (LIPIcs), Vol. **82** (2017), 40:1–40:16.

(joint work with E.D. Kudryavtsev,
A.S. Shlychkova, M.E. Zhukovskii)

YURY YAROVIKOV

THERE ARE NO FO SENTENCES WITH QUANTIFIER DEPTH 4 AND AN INFINITE SPECTRUM

We study asymptotic behaviour of the first order properties (properties expressible in first order logic) of binomial random graphs $G(n,p)$. We say that the random graph $G(n,p)$ *obeys the Zero-One Law* if for each first-order graph property its probability tends to 0 or tends to 1. We also say that the random graph $G(n,p)$ *obeys the Zero-One k-Law* if for each first-order graph property with quantifier depth no more than k its probability tends to 0 or tends to 1.

Let $\alpha \in (0,1)$ be a real number. It was proven by J. Spencer and S. Shelah in 1988 that the Zero-One Law holds for $G(n,n^{-\alpha})$ if and only if α is irrational. We say that the rational α *is in k-spectrum* if the random graph $G(n,n^{-\alpha})$ does not obey the Zero-One k-Law.

In 2012, M. Zhukovskii proved that the smallest number in k-spectrum is $\frac{1}{k-2}$. The full structure of k-spectrum remains unexplained. It is known, however (J. Spencer, 1990), that 14-spectrum is infinite. Moreover, M. Zhukovskii proved that $\frac{1}{2}$ is the limiting point of 5-spectrum while 3-spectrum is finite. Finally, it was proven by A. Matushkin and M. Zhukovskii in 2018 that there can be no limiting points in 4-spectrum but $\frac{1}{2}$ and $\frac{3}{5}$.

Our result is the following. We prove that $\frac{1}{2}$ and $\frac{3}{5}$ are not the limiting points in 4-spectrum. Thus, we conclude that the 4-spectrum is finite. Therefore, the minimal k such that k-spectrum is infinite is 5.

References

[1] S. Shelah, J.H. Spencer, "Zero-one laws for sparse random graphs", J. Amer. Math. Soc., **1** (1988), 97-115.

[2] M.E. Zhukovskii, "Zero-One k-Law", Discrete Mathematics, **312** (2012), 1670-1688.

[3] A.D. Matushkin, M.E. Zhukovskii, First order sentences about random graphs: small number of alternations, Discrete Applied Mathematics, 2018, **236**: 329–346.

[4] J. H. Spencer, "The Strange Logic of Random Graphs", Number **22** in Algorithms and Combinatorics, Springer-Verlag, Berlin, 2001.

ALEXEY NIKITIN

DECIDABILITY PROBLEMS FOR UNIVERSAL AND EXISTENTIAL THEORIES OF THE CLASS OF PARTIALLY ORDERED SETS

We consider the decidability problems of the universal and existential theories of the class of all partially ordered sets in a language without constants.

A partially ordered set (poset) is an algebraic structure $\mathcal{P} = \langle P \mid L \rangle$ with domain set P and language $L = \langle \leqslant^{(2)} \rangle$, where $\leqslant$ – partial order predicate. On $\mathcal{P}$ three axioms hold:

(1) $\forall p \in P\ p \leqslant p$ *(reflexivity)*;
(2) $\forall p_1, p_2 \in P\ p_1 \leqslant p_2 \wedge p_2 \leqslant p_1 \to p_1 = p_2$ *(antisymmetry)*;
(3) $\forall p_1, p_2, p_3 \in P\ p_1 \leqslant p_2 \wedge p_2 \leqslant p_3 \to p_1 \leqslant p_3$ *(transitivity)*.

Atomic formula of language L in variables X is either equality $x_i = x_j$ or the inequality $x_i \leqslant x_j$, where $x_i, x_j \in X$.

Formula of language L is an expression that is defined recursively as follows:

(1) Atomic formula is a formula;
(2) If φ is a formula, then $\neg\varphi$ is also a formula;
(3) If φ, ψ are formulas, then $\varphi \vee \psi$ and $\varphi \wedge \psi$ are also formulas;
(4) If φ is a formula, then $\exists x_i\ \varphi$ and $\forall x_i\ \varphi$ are also formulas.

Sentence of language L is a formula without free variables. *Universal* sentence is a sentence of following form $\forall x_1 \ldots \forall x_n \Psi(x_1, \ldots, x_n)$, where Ψ is a formula in n free variables. The *existential* sentence is defined similarly.

The class of posets of language L is denoted by $\mathbf{P}$. *Elementary* theory of class $\mathbf{P}$ is set $Th(\mathbf{P})$ of all sentences of the language L that is true in all posets in $\mathbf{P}$. The universal theory of the class $\mathbf{P}$ is the subset $Th_\forall(\mathbf{P}) \subseteq Th(\mathbf{P})$ of universal sentences of the elementary theory of class $\mathbf{P}$. The existential theory of the class $\mathbf{P}$ is defined similarly.

Theory T of posets class $\mathbf{P}$ of language L is *decidable* if there is an algorithm that checks whether φ in theory T or not for any sentence φ in language L.

Now, we formulate the main results of the work.

Theorem 1. *The universal theory of the class of all posets in a language L without constants is decidable.*

Theorem 2. *The existential theory of the class of all posets in the language L without constants is decidable.*

Also, results were obtained that characterize the complexity of these problems.

Theorem 3. *The problem of decidability of the existential theory of a class of posets is NP-hard.*

Theorem 4. *The problem of decidability of the universal theory of a class of posets is co-NP-hard.*

ARTEM SHEVLYAKOV

ON OUTLIER DETECTION WITH DENDROGRAMS. ALGEBRAIC APPROACH

We apply algebraic approach to the study of algorithms of hierarchical clustering. Moreover, we discuss the outlier detection by such algorithms and prove that almost all datasets contain outliers relative to the given data generation procedure. Also, we show the connection between the last result and the zero-one law in monadic second-order logic for linear orders.

Let us explain our results more carefully.

The clustering is an important problem of data analysis. Let us consider a general scheme of agglomerative clustering process. In the beginning, each element is in a cluster of its own. The clusters are then sequentially combined into larger clusters, until all elements end up being in the same cluster. At each step, the two clusters separated by the shortest distance are merged. In our research we will use the following cluster distance function

$$d(A, B) = \min\{d(a, b) \mid a \in A, b \in B\} \text{ (single-linkage clustering).}$$

The result of any agglomerative clustering can be visualized as a dendrogram, which shows the sequence of cluster fusions.

Thus, the process of agglomerative clustering starts with the distance matrix of a data. Since the singly-linkage clustering use order (not values) on matrix entries, we propose to generate $n \times n$-matrices as follows:

1. randomly generate the upper triangle of a matrix by elements of linearly ordered set of $n(n-1)/2$ elements;
2. write zeros on the diagonal;
3. reflect the upper triangle to the lower one.

Thus, we have exactly $(n(n-1)/2)!$ distance $n \times n$-matrices.

For the given procedure of matrix generation, one can prove the following.

Theorem 1.1. *Let $D(M)$ be the dendrogram defined by the agglomerative clustering for a distance $n \times n$-matrix M. Then the probability $Pr(D(M)$ has a leaf adjacent to the tree root$)$ tends to 1 with $n \to \infty$.*

*The author was supported by Russian Science Foundation (project 18-71-10028)

One can apply this theorem to the problem of outlier detection. We say that an element x is an outlier if the agglomerative clustering puts x into a leaf adjacent to the dendrogram root. In other words, x is very far from other data elements $x_1, x_2, \ldots, x_n$, and we have two clusters $\{x_1, x_2, \ldots, x_n\}$, $\{x\}$ before the last cluster fusion.

Hence, the last theorem states that almost all datasets contain outliers with respect to the given procedure of data generation.

There are connections between the obtained result and the famous zero-one law in model theory. One can prove that the property "a dataset contains an outlier" may be written as a sentence of the monadic second-order logic over linear orders. Above we show this sentence is almost surely true. Probably, it is a consequence of the more general result

Conjecture. Does the zero-one law hold for linear orders in monadic second-order logic?

ALBERT GARETTA

EQUATIONS IN SOLVABLE GROUPS

We study the Diophantine problem (decidability of systems of equations) in different families of solvable groups. Whe show that for any group G in each of these families there exists a ring of algebraic integers O that is interpretable in G by systems of equations. This reduces the Diophantine problem of O – conjectured undecidable– to the same problem in G, and it leads us to conjecture that the Diophantine problem in G is undecidable. The families where such result is obtained include all finitely generated non-virtually abelian nilpotent groups and all polycyclic groups that are not virtually metabelian. Note that the Diophantine problem of virtually abelian groups has long been known to be decidable (their first-order theory is). We also prove undecidability of the Diophantine problem in free solvable groups and in 'most' nilpotent groups by studying asymptotic properties of random nilpotent groups.

Joint work with Alexei Miasnikov and Denis Ovchinnikov

ILNUR KHUZIEV

DISTRIBUTED SEARCH OF AN ANTIPODAL VERTEX IN SYMMETRIC CAYLAY GRAPH OVER BOOLEAN CUBE

We consider a $Cay(Z_2^n, s)$ - a caylay graph over boolean cube group, there generating set contains all vectors with exactly s non zero coordinates. Each vertex is associated with computing node in network with synchronized time, exactly one node is marked as a leader. Vertexes b is called *antipodal* to a iff each automorphism which has a as fixed point also have b as fixed point. The task is to find out the vertex, that is antipodal to the leader (we consider range of parameters, there each vertex has exactly one antipodal vertex). We present fast protocol that solves this problem: it stops in $O(\frac{n}{s})$ steps, at each step at most $O(\log n)$ bits transferred through each edge.

DMITRY ZHUK

ON THE COMPLEXITY OF THE QUANTIFIED CONSTRAINT SATISFACTION PROBLEM

The *Quantified Constraint Satisfaction Problem* $QCSP(\Gamma)$ is the problem to evaluate a sentence of the form $\forall x_1 \exists y_1 \dots \forall x_n \exists y_n \ (R_1(\dots) \wedge \dots \wedge R_s(\dots))$, where $R_1, \dots, R_s$ are relations from the constraint language Γ. This problem is a generalization of the Constraint Satisfaction Problem, where only existential quantifiers are allowed.

We study the complexity of $QCSP(\Gamma)$ for different constraint languages on finite sets. Unlike the Constraint Satisfaction Problem, where the problem for every constraint language is either tractable, or NP-complete, $QCSP(\Gamma)$ can be PSpace-complete. It was conjectured by Hubie Chen that $QCSP(\Gamma)$ is either tractable, or NP-complete, or PSpace-complete.

We disproved this conjecture and showed that for some constraint languages Γ the problem $QCSP(\Gamma)$ can be coNP-complete, DP-complete and so on.

Also, we characterized the complexity of the Quantified Constraint Satisfaction Problem for constraint languages on 3-element domain containing all unary singleton relations (so called idempotent case), i.e. we showed that for such languages $QCSP(\Gamma)$ is either tractable, or NP-complete, or coNP-complete, or PSpace-complete.

JAKUB BULIN

ALGEBRAIC APPROACH TO PROMISE CONSTRAINT SATISFACTION

The Constraint Satisfaction Problem provides a common framework for expressing many common computational tasks from diverse areas of computer science. In its purest form, CSP with a fixed constraint language on a finite set, it is amenable to a computational complexity classification via polymorphisms (higher-arity symmetries of solution spaces), and abstract algebraic objects capturing their properties. An extensive research program exploring this connection to universal algebra culminated in resolving the so-called algebraic CSP dichotomy conjecture.

Recently, Brakensiek and Guruswami proposed a substantial generalization of the CSP, called Promise CSP, which is motivated by open questions about the approximability of variants of satisfiability and graph colouring. They demonstrated that the basic algebraic approach can be extended to this new setting and successfully employed to study computational complexity of Promise CSPs.

Similarly to the CSP, to fully exploit the algebraic approach we must lift it from concrete properties of polymorphisms to their abstract properties. In this talk, I will introduce the abstract polymorphism theory for Promise CSPs and demonstrate how it can be applied to improve the state-of-the-art in approximate graph coloring by showing that it is NP-hard to find a 5-coloring of a given 3-colorable graph. This is joint work with Andrei Krokhin and Jakub OprÅ¡al from Durham University.

ARMIN WEISS

THE ISOMORPHISM PROBLEM FOR FINITE EXTENSIONS OF FREE GROUPS IS IN PSPACE

While, in general, the isomorphism problem for finitely presented groups is undecidable, for virtually free groups it has been shown to be decidable by Krstić. Later the complexity has been improved to primitive recursive by Sénizergues in the case that the input is either given as two context free grammars for the word problems or as finite extensions of free groups.

Here, we present an algorithm for the following problem: given a context-free grammar for the word problem of a virtually free group G, compute a finite graph of groups with finite vertex groups and fundamental group G. Our algorithm is non-deterministic and runs in doubly exponential time. Using Krstić's algorithm for testing fundamental groups of graphs of groups for isomorphism, it follows that the isomorphism problem of context-free groups can be solved in doubly exponential space.

Moreover, if, instead of a grammar, a finite extension of a free group is given as input, the construction of the graph of groups is in NP and, consequently, the isomorphism problem in PSPACE.

While the algorithm itself is rather simple and uses only standard tools from formal language theory, its proof of correctness is more geometric and makes use of the structure tree theory introduced by Dicks and Dunwoody.

This talk is based on joint work with Géraud Sénizergues.

EVELINA DANIYAROVA

ALGEBRAIC GEOMETRY OVER ABELIAN GROUPS

Universal algebraic geometry is a relatively new direction in mathematical research. The results in algebraic geometry over specific groups, rings, algebras, graphs, etc., can be called the practical part of this branch of mathematics, many articles and even books are devoted to them. The theoretical part of universal algebraic geometry is a new section of the model theory, within the framework of which the basic algebraic-geometric concepts are introduced, problems are posed and results are proved for an arbitrary algebraic structure of an arbitrary language. In the monograph by E. Yu. Daniyarova, A. G. Myasnikov, V. N. Remeslennikov "Algebraic geometry over algebraic structures", Novosibirsk: Publ. SB RAS, 2016, 243 p., the theoretical part of universal algebraic geometry is introduced. The main ideas of this monograph will be presented on the talk. For clarity and ease of understanding, algebraic-geometric concepts and solutions of algebraic-geometric problems will be described in the projection to the category of abelian groups. In the talk,

- there will be defined equations, algebraic sets, irreducible algebraic sets, radicals, coordinate groups over abelian groups;
- it will be shown how all coordinate groups, irreducible coordinate groups, all algebraic sets, irreducible algebraic sets over abelian groups are classified;
- there will be described geometrically equivalent abelian groups and universally geometrically equivalent abelian groups;
- it will be shown that among all special algebraic-geometric classes in the category of abelian groups, only the class of equational co-domains is of interest, and also the description of abelian groups from this class will be given.

NIKOLAI POLYAKOV

DICHOTOMY THEOREM IN COMPUTATIONAL SOCIAL CHOICE THEORY

We consider some problems of aggregation of individual preferences. We show that under rather general assumptions there are only two clones of aggregation rules that allow invariant symmetric classes of preferences, each of these clones being generated by a single function.

Let A be a finite set and r a natural number. The symbol $[A]^r$ denotes the set of all r-element subsets of A. *Individual preferences* are modeled by *r-choice functions* on a set A, i.e. functions $\mathfrak{c} : [A]^r \to A$ satisfying $f(p) \in p$ for any $p \in [A]^r$. The set of all r-choice functions on a set A is denoted by $\mathfrak{C}_r(A)$. A set $\mathfrak{D} \subseteq \mathfrak{C}_r(A)$ is called *symmetric* if $\mathfrak{c} \in \mathfrak{D} \Rightarrow \mathfrak{c}_\sigma \in \mathfrak{D}$ for any permutation σ of A where $\mathfrak{c}_\sigma(p) = \sigma^{-1}\mathfrak{c}(\sigma p)$ for any $p \in [A]^r$. A (simple local) *aggregation rule* is a function $f : A^n_{\leq r} \to A$ where $A^n_{\leq r} = \{\mathbf{a} \in A^n : |\operatorname{ran}\mathbf{a}| \leq r\}$, see [1] (cf [2]). For all $\mathfrak{c}_1, \mathfrak{c}_2, \dots, \mathfrak{c}_n \in \mathfrak{C}_r(A)$ and $f : A^n_{\leq r} \to A$ the symbol $f(\mathfrak{c}_1, \mathfrak{c}_2, \dots, \mathfrak{c}_n)$ denotes the r-choice function $\mathfrak{c}$ defined by $\mathfrak{c}(p) = f(\mathfrak{c}_1(p), \mathfrak{c}_2(p), \dots, \mathfrak{c}_n(p))$ for all $p \in [A]^r$. An aggregation rule $f : A^n_{\leq r} \to A$ *preserves* a set $\mathfrak{D} \subseteq \mathfrak{C}_r(A)$ if $f(\mathfrak{c}_1, \mathfrak{c}_2, \dots, \mathfrak{c}_n) \in \mathfrak{D}$ for all $\mathfrak{c}_1, \mathfrak{c}_2, \dots, \mathfrak{c}_n \in \mathfrak{D}$. The Galois connection generated in natural sense by the preservation relation is denoted $(\mathrm{Inv}_r, \mathrm{Pol}_r)$. A set $\mathfrak{D} \subseteq \mathfrak{C}_r(A)$ has the *Arrow property* if $\mathrm{Pol}_r(\mathfrak{D})$ contains only projections (dictatorship rules). All symmetric sets without the Arrow property were classified in [3], see also [1]. In addition, it is shown [4] that if $r = 2$ (this is the most important case) and $|A| \geq 5$ then for any set $\mathfrak{D} \subseteq \mathfrak{C}_r(A)$ without the Arrow property the set $\mathrm{Pol}_r(\mathfrak{D})$ consists of functions generated by the "counting-out game" function ℓ defined by $\ell(x, y, y) = \ell(y, x, y) = \ell(y, y, x) = x$. This result can be considered as a generalization of Arrow's impossibility theorem [5]. In essence, it means that there are no acceptable aggregation rules for symmetric sets of preferences.

For positive results, we consider a more general situation. A set $\mathfrak{D} \subseteq \mathfrak{C}_r(A)$ is called *trivial* if $\mathfrak{D} = \{\mathfrak{c} \in \mathfrak{C}_r(A) : \mathfrak{c} \restriction_B = \mathfrak{d} \restriction_B\}$ for some $\mathfrak{d} \in \mathfrak{C}_r(A)$ and $B \subseteq [A]^r$ (a trivial set $\mathfrak{D}$ is preserved by any aggregation rule). A set $\mathbb{D} \subseteq \mathscr{P}(\mathfrak{C}_r(A))$ is called trivial if it contains only trivial sets. A set $\mathbb{D} \subseteq \mathscr{P}(\mathfrak{C}_r(A))$ is called *symmetric* if $\mathfrak{D} \in \mathbb{D} \Rightarrow \mathfrak{D}_\sigma \in \mathbb{D}$ for any permutation σ of A where $\mathfrak{D}_\sigma = \{\mathfrak{c}_\sigma : \mathfrak{c} \in \mathfrak{D}\}$ (for example, the class of all *single-peaked* domain [6] is symmetric). Let $\partial : A^3_{\leq 2} \to A$ be a *majority* function. We prove the following dichotomy theorems.

Theorem 1. *Let $|A| \geq 5$. Let $f : A^n_{\leq 2} \to A$ be a non-dictatorship aggregation rule and $\mathbb{D} \subseteq \mathrm{Inv}_2(f)$ a non-trivial symmetric set. Then $\mathbb{D} \subseteq \mathrm{Inv}_2(\partial)$ or $\mathbb{D} \subseteq \mathrm{Inv}_2(\ell)$*

Let $f : A^n_{\leq r} \to A$ and $\mathfrak{C} \subseteq \mathfrak{C}_r(A)$. A set $\mathfrak{D}$ is *compatible with the pair* $(f, \mathfrak{C})$ if $\mathfrak{D} \subseteq \mathfrak{C}$ and $f(\mathfrak{c}_1, \mathfrak{c}_2, \ldots, \mathfrak{c}_n) \in \mathfrak{C}$ for all $\mathfrak{c}_1, \mathfrak{c}_2, \ldots, \mathfrak{c}_n \in \mathfrak{D}$ A set of all sets what is compatible with $(f, \mathfrak{C})$ is denoted by $\mathrm{Comp}\,(f, \mathfrak{C})$**.** A function $\mathfrak{c} \in \mathfrak{C}_r(A)$ is called rational if $\mathfrak{c}(p) = \max_{\succ} p$ for some linear order $\succ$ on A. The set of all rational function $\mathfrak{c} \in \mathfrak{C}_r(A)$ is denoted by $\mathfrak{R}_r(A)$.

Theorem 2. *Let* $|A| \geq 5$. *Let* $f : A^n_{\leq 2} \to A$ *be a non-dictatorship aggregation rule and* $\mathbb{C} \subseteq \mathrm{Comp}(f, \mathfrak{R}_2(A))$ *a non-trivial symmetric set. Then there is a symmetric class* $\mathbb{D} \subseteq \mathscr{P}(\mathfrak{R}_2(A))$ *such that*

1. $\mathbb{D} \subseteq \mathrm{Inv}_2(\partial) \cap \mathrm{Inv}_2(f)$ *or* $\mathbb{D} \subseteq \mathrm{Inv}_2(\ell) \cap \mathrm{Inv}_2(f)$ *and*
2. *For all* $\mathfrak{C} \in \mathbb{C}$ *there is* $\mathfrak{D} \in \mathbb{D}$ *such that* $\mathfrak{C} \subseteq \mathfrak{D}$.

References

[1] Shelah S. On the Arrow property. Adv. in Ap. Mat., vol. 34 (2005), pp. 217–251.

[2] Aleskerov F. T. Arrovian Aggregation Models. Springer US (1999).

[3] Polyakov N., Shamolin M. On a generalization of Arrow's impossibility theorem. Doklady Mathematics, vol. 89, no. 3 (2014), pp. 290-292.

[4] Polyakov, N. Galois connections for classes of discrete functions and their application to mathematical problems of social choice theory. PhD thesis. Moscow University (2016), Russian.

[5] Arrow K. Social Choice and Individual Values. 2 edition. Yale University Press (1963).

[6] Moulin, H. Axioms of Cooperative Decision Making. Cambridge University Press (1991).

ALEXANDER ZAPRYAGAEV

LINEAR ORDERINGS INTERPRETED IN PRESBURGER ARITHMETIC

For the interpretations of linear orderings in the standard model of Presburger arithmetic $(\mathbb{N}, +)$, we show that a Hausdorff-style rank can be used as a necessary condition of multi-dimensional definability. We constructively establish a connection between the interpretability properties of an order and its Cantor condensation and, furthermore, conjecture a criterion of Presburger definability of linear orderings for all dimensions, proving it for $m = 2$.

Classification of linear orderings according to complexity of their representation encompasses a number of interconnected problems and approaches. This question is naturally connected with the various notions of *rank* going back to Hausdorff's seminal work [3]. Khoussainov, Rubin & Stephan [4] develop the theory of Kantor-Bendixson-style rank for linear orderings based on the operation of *condensation*, which fuses the points at a final distance between them. One could notice that all orderings that are trivialized after a, maybe transfinite, number of such iterations, are scattered (SLO). We give an overview of the results obtained (partially jointly with F. Pakhomov) in classifying the scattered linear orderings according to their definability in Presburger arithmetic, that is, by a formula with (standard) order and addition, without multiplication.

The question of interpreting Presburger arithmetic in its own finitely axiomatizable subtheories naturally leads to the behaviour of the implied interpretation of its order relation, which further generalizes into the study of all linear orderings interpretable in Presburger arithmetic in some number of dimensions. Using a modification of rank description, the following was established [7]:

Theorem 1 *(A. Zapryagaev, F. Pakhomov, 2017) All linear orderings m-dimensionally interpretable in Presburger arithmetic have a rank m or below.*

Note that this gives only a necessary condition, as for the trivial argument of cardinality, there are more scattered linear orderings of any rank ≥ 2 than formulas in Presburger signature. However, the following holds nevertheless:

Theorem 2 *(A. Zapryagaev, 2018) Let $\iota\colon L \to \mathbb{N}$ be an m-dimensional interpretation of an SLO L in the standard model of aritmetic $(\mathbb{N}, +)$. Then its condensation cL possessed an $m-1$-dimensional interpretation.*

Furthermore, this interpretation of cL can be extracted from a particular interpretation of L through a canonical construction.

In order to establish this, one requires to match to each Presburger-definable set (see also [5]) its dimension, akin to [2], which expresses the maximal number of linearly independent vectors generating some sublattice in it, based on .

Using this, the it is possible to establish:

Theorem 3 *(A. Zapryagaev, 2019) Let Let* $\iota\colon L \to \mathbb{N}$ *be a* 2*-dimensional interpretation of an SLO* L *in the standard model of aritmetic* $(\mathbb{N}, +)$*. Then there is some* $n \in [2; 4]$ *that* L *is a limiting of the lexicographical ordering of* $\mathbb{Z}^n$ *onto some Presburger-definable set.*

The conjecture is that it holds for each $n \geq 1$. This construction gives a possibility to create a lambda calculus producing all definable orderings. The problem can be further generalized to automatic linear orderings which, per [1], are exactly ones interpretable in Presburger arithmetic with one additional predicate, and which still do not possess an exact explicit necessary and sufficient condition.

References

[1] Bruyere, V., Hansel, G., Michaux, C., Villemaire, R.: Logic and p-recognizable sets of integers. Bull. Belg. Math. Soc. Simon Stevin 1.2, 191-238 (1994)

[2] Cluckers, R.: Presburger sets and p-minimal fields. J. Symbolic Logic 68.1, 153-162 (2003)

[3] Hausdorff, F.: Grundzüge einer Theorie der geordneten Mengen. Math. Ann. 65.4, 435-505 (1908)

[4] Khoussainov, B., Rubin, S., Stephan, F.: Automatic linear orders and trees. ACM Trans. Comput. Log. 6.4, 675-700 (2005)

[5] Muchnik, A,: The definable criterion for definability in Presburger arithmetic and its applications. Theoret. Comput. Sci. 290.3, 1433-1444 (2003)

[6] Presburger M.: Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt. Comptes Rendus du I congrès de Mathématiciens des Pays Slaves 92101 (1929)

[7] Zapryagaev, A., Pakhomov, F.: Interpretations of Presburger Arithmetic in Itself. International Symposium on Logical Foundations of Computer Science 354-367 (2018)

IVAN PRIKHODKO

COMMUNICATION COMPLEXITY IN T-CELL RECEPTORS SIGNALLING DURING ANTIGEN RECOGNITION

The time required for pathogen recognition by the immune system is critical for the organism survival. For viral diseases, recognition is performed by clones of T-lymphocytes with different types of receptors. During maturation, those T-lymphocyte clones are selected, which receptors have high dissociation constants with most of the body's epitopes (short protein fragments). Viral proteins for which there was no such selection can be detected by the unexpectedly low dissociation constant of their epitopes with receptors [1].

Each individual receptor is contacting thousands of epitopes. The time of each contact is determined by the dissociation constant only on average. According to the developed ideas, signal transmission through the membrane occurs with as great probability, as large the clusters consisting of laterally related receptors it has [2].

It is shown that an increase in the duration of lateral bonds in the vicinity of the receptor in contact with the epitope makes possible the nucleation of macroclusters formation. Each cluster of receptors is assigned a value (playing the role of entropy) representing the degree of disorder of lateral bonds in it at a particular point in time [3]. The cluster entropy changes statistically insignificantly for clusters smaller than the critical size. The development of supercritical clusters is characterized by an increase in entropy. The probability of supercritical clusters formation is calculated as a function of the dissociation constant of pathogenic epitopes.

REFERENCES

1. *Klein, L., Kyewski, B., Allen, P. M., Hogquist, K. A.,* "Positive and negative selection of the T cell repertoire: what thymocytes see (and don't see)" Nature Reviews Immunology, **14**, No. 6, 377–391 (2014).
2. *Pageon, S. V., Tabarin, T., Yamamoto, Y., Ma, Y., Nicovich, P. R., Bridgeman, J. S., ... Tungatt, K.,* "Functional role of T-cell receptor nanoclusters in signal initiation and antigen discrimination," Proceedings of the National Academy of Sciences, **113**, No. 37, E5454–E5463 (2016).
3. *Dairyko, M., Hogben, L., Lin, J. C. H., Lockhart, J., Roberson, D., Severini, S., Young, M.,* "Note on von Neumann and Rnyi entropies of a graph," Linear Algebra and its Applications, **521**, 240–253 (2017).

MARKOV PAVEL

ANALYSIS OF METHODS FOR SOLVING OF SYSTEMS OF EQUATIONS FOR MODELING OF ONE- AND TWO-PHASE FLOW IN NETWORK MODELS OF PORES AND CAPILLARIES

Modelling of multiphase flow in porous media of oil and gas natural reservoirs is a very important part of modern design of development of oil and gas fields. All decisions in development are made on the basis of comprehensive multivariate set of models. It is crucial to estimate filtration (reservoir) parameters for these models - absolute permeability, capillary pressure and relative permeability. These filtration parameters can be estimated experimentally but it is expensive, difficult to recreate reservoir conditions, difficult to provide sufficient number of experiments. Pore-scale modelling of flow in porous media along with digital core analysis can solve these problems what is briefly described in the report.

Solving of the mentioned above problems depends on time spent for numerical calculations and computational recourses needed for pore-scale modelling because multivariate sets of calculations have to be done. This report briefly describes modelling of one- and two-phase flow in network models of pores and capillaries (pore network models [3]) as a part of pore-scale modelling. Pore network modelling has optimal combinations of detalization and simplicity of porous media models, calculation time and computational recourses what is important for fast multivariate calculations.

This report is intended to show used systems of difference equations for pore network modelling and their specific aspects. It shows comparisons (specific aspects of applications, calculation time, computational complexity and so on) of different methods for solving of this kind of systems of equations: the algebraic multigrid method (AMG), the biconjugate gradient stabilized method (BiCGStab), the conjugate gradient method with the symmetric successive overrelaxation (CG-SSOR), the method with using of continuous symmetry groups and others. Applications of the developed method on the basis of continuous symmetry groups [4], [5] are presented for the considered systems using obtained results of group classifications of similar to pore network models difference schemes of equation of gas flow in porous media. The results of group classification of difference schemes have been obtained using results from [1], [2].

Obtained results of comparison of numerical methods can be applied in problems of filtration parameters estimations of core samples for oil and gas natural reservoirs. It can save calculation time and computational recourses what is important in practical problems because of increasing number of used model variants and their detalization.

Acknowledgments. The reported study was funded by RFBR according to the research project 16-29-15119.

References

[1] Baikov V.A., Gazizov R.K., Ibragimov N.H., Kovalev V.F. Water Redistribution in Irrigated Soil Profiles: Invariant Solutions of the Governing Equation // Nonlinear Dynamics. - 1997. - 13. - P. 395-409.

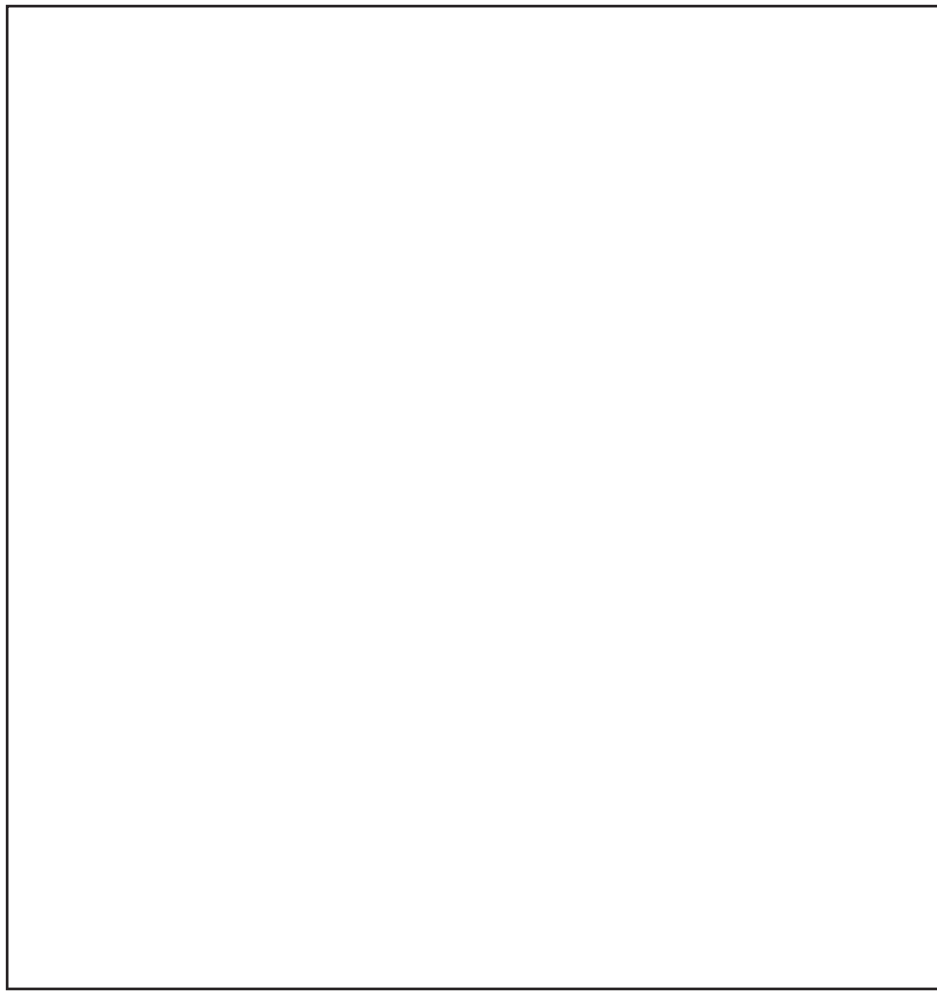
[2] Dorodnitsyn, V. Applications of Lie Groups to Difference Equations - Chapman and Hall/CRC, 2011. - 344 p.

[3] Markov P.V., Rodionov S.P. Application of porous media microstructure models when calculating filtration characteristics for hydrodynamic models // Oilfield Engineering. - 2015. - 11. - pp. 64-75 (in Russian)

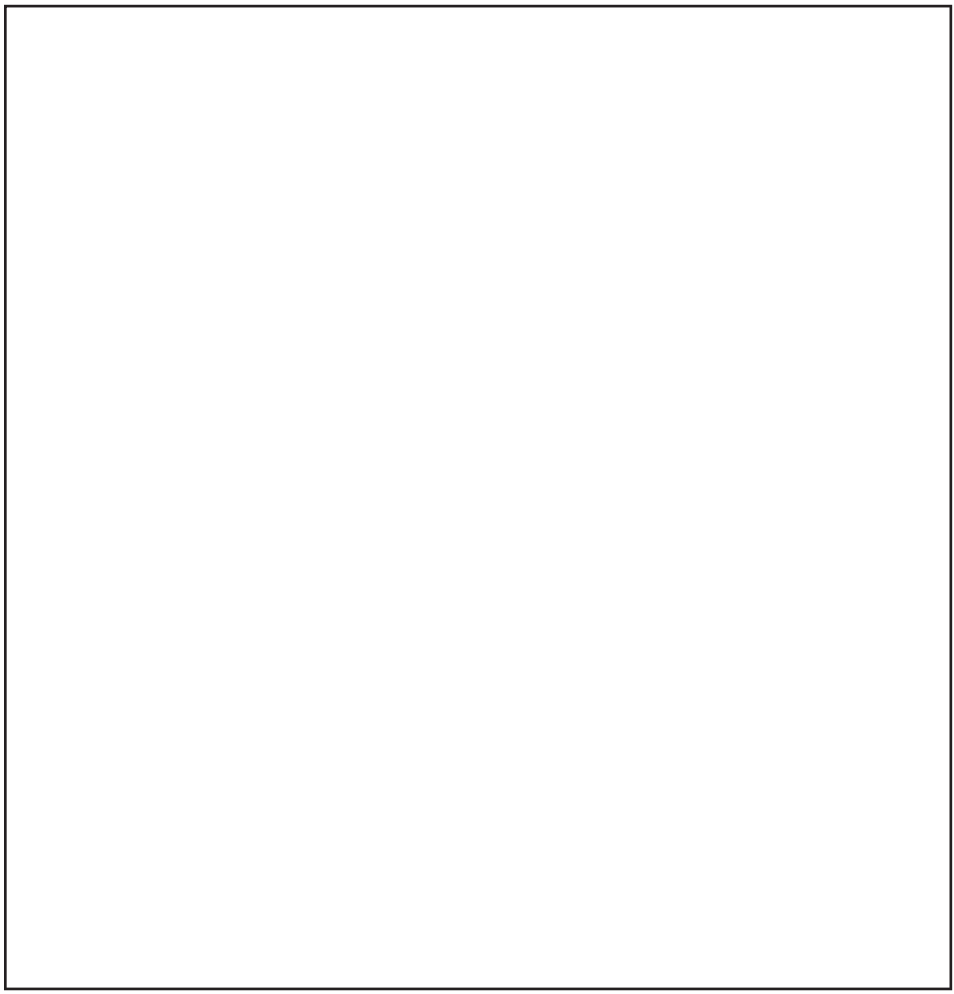
[4] Markov P.V., Rodionov S.P. The method of accelerations of serial numerical calculations for multiphase flow equations in porous media using continuous groups of symmetries // Automation, telemechanization and communication in oil industry. 2015. - No 12. - pp. 23-30 (in Russian)

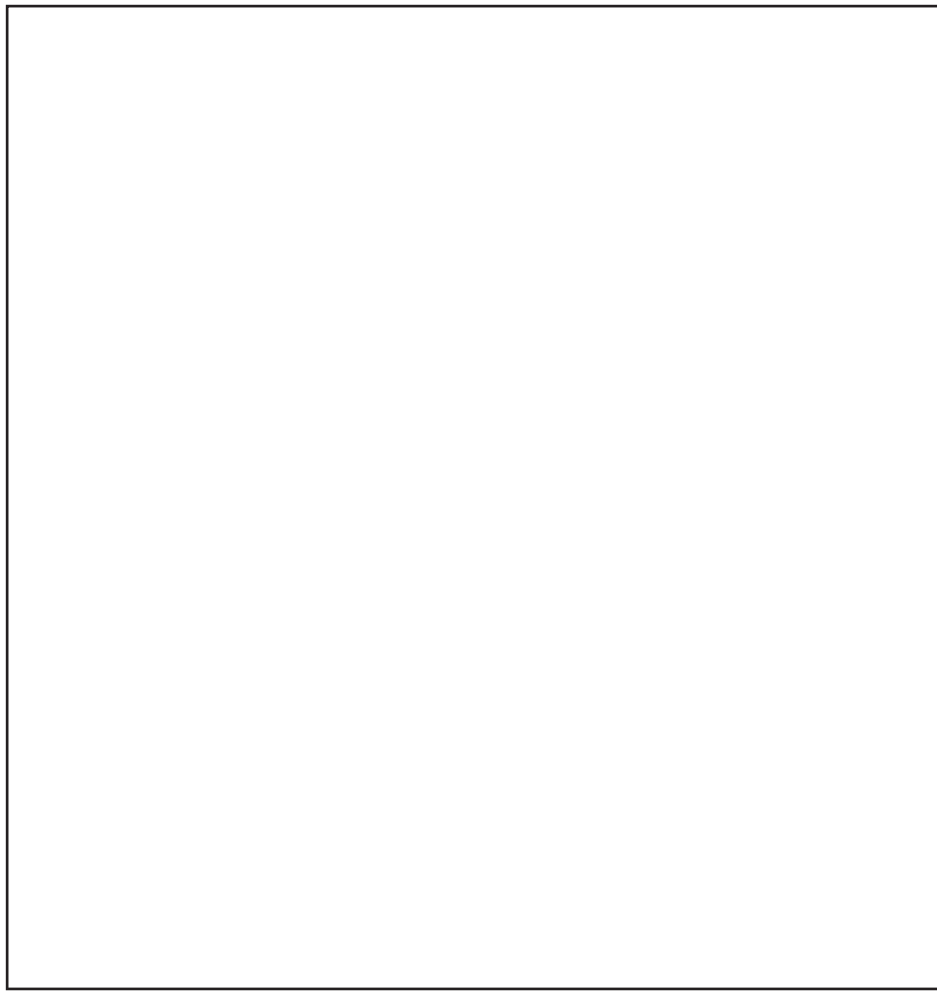
[5] Markov P.V. Group classification applications for analysis of discrete models of flow in porous media // Journal of Physics: Conference series. - 2017. - Vol. 894, Num. 1.

FOR NOTES

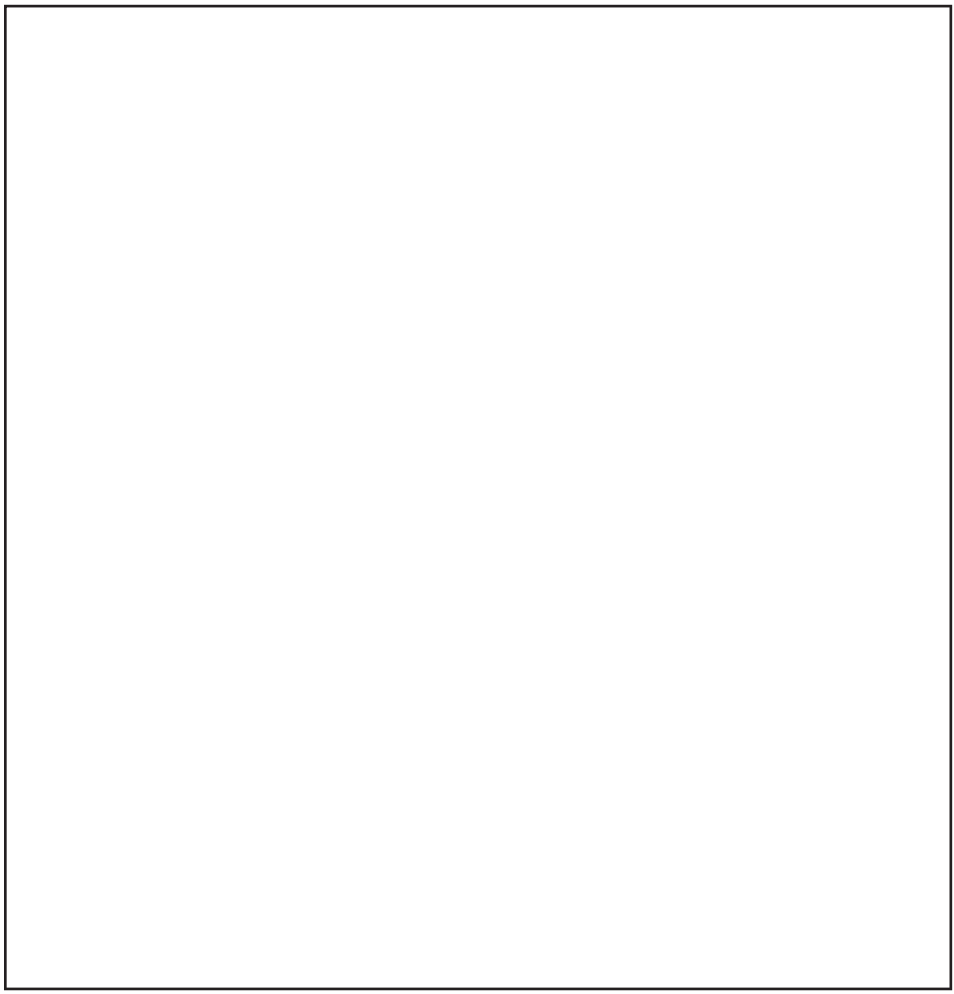


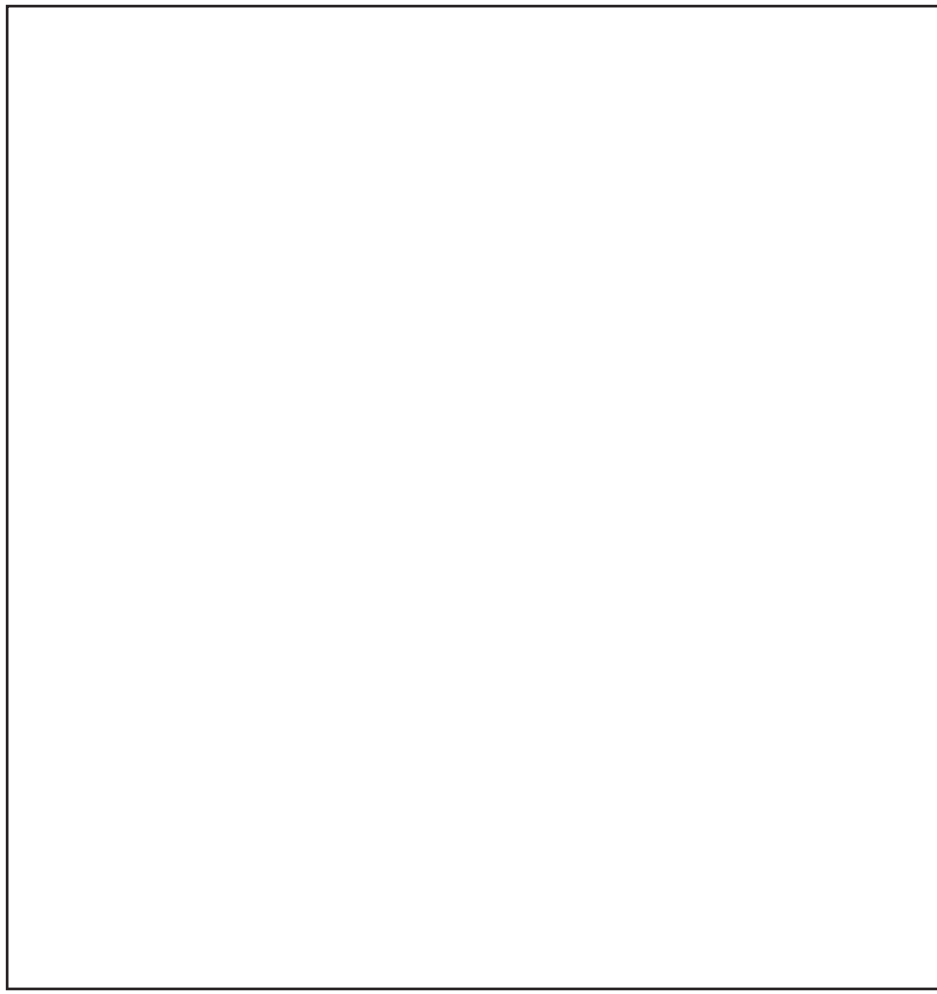
FOR NOTES





FOR NOTES





RUS WCMT

Russian Workshop on Complexity and Model Theory

Abstracts

June 9–11, 2019 MIPT Moscow, Russia

Number of copies printed 100. Format 60 x 84 1 / 16. Order № 190605
Federal State Autonomous Educational Institution of Higher Professional Education
“Moscow Institute of Physics and Technology (National Research University)”
Institutskii per. 9, Dolgoprydny, Moscow Region, 141700, Russia
Printed: Admiral print LLC, 121309, Moscow, Barklaya str., 13, bld. 1

ЯUS WCMT

ISBN 978-5-6041187-5-7

MIPT algorithms Yandex HUAWEI