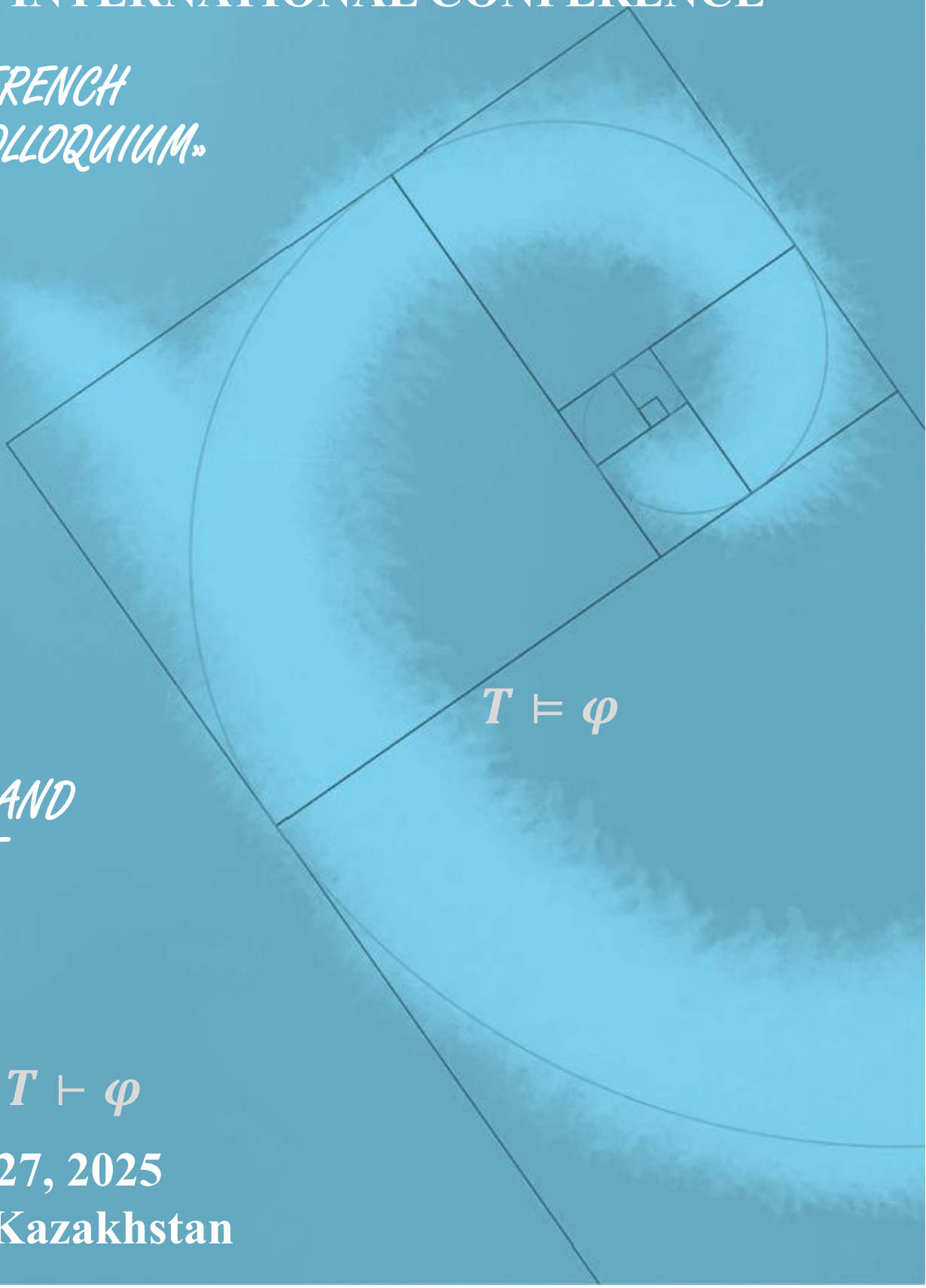
L.N. GUMILYOV EURASIAN NATIONAL UNIVERSITY

$T \models \varphi \Leftrightarrow T \vdash \varphi$

EIGHTH INTERNATIONAL CONFERENCE

«KAZAKH-FRENCH LOGICAL COLLOQUIUM»



PROGRAM AND ABSTRACT

$T \vdash \varphi$

June 24-27, 2025
Astana, Kazakhstan

MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE REPUBLIC OF KAZAKHSTAN
L.N. GUMILYOV EURASIAN NATIONAL UNIVERSITY

EIGHTH INTERNATIONAL CONFERENCE

"KAZAKH-FRENCH LOGICAL COLLOQUIUM"

24-27 June, 2025

Astana, Kazakhstan

PROGRAM AND ABSTRACT

ASTANA, 2025

INTERNATIONAL PROGRAMME COMMITTEE

Chairman:
Goncharov S.S., Academician of the Russian Academy of Sciences, Sobolev Institute of Mathematics SB RAS
Umirbayev U.U., Academician of the National Academy of Sciences of the Republic of Kazakhstan, Professor of Wayne State University, Detroit, USA

Co-Chairmen:
Badaev S.A., Professor of KBTU (Almaty)
Baizhanov B.S., Corresponding Member of the National Academy of Sciences of the Republic of Kazakhstan (Almaty), IMMM
Bruno Poizat, Professor of the Claude Bernard University of Lyon-1, Lyon, France
Dzhumadildayev A.S., Academician, Vice-President of the National Academy of Sciences of the Republic of Kazakhstan under the President of the Republic of Kazakhstan
Frank Olaf Wagner, Claude Bernard University (Lyon-1)

Deputy Chairmen of the Program Committee:
Kurmangaliyeva Zh.D., Member of the Board - Vice-Rector for Science and Commercialization of the "NP JSC ENU named after L.N. Gumilyov"
Kulpeshov B.Sh., Corresponding Member of the NAS RK (Almaty), IMMM
Morozov A.S., IM SB RAS (Novosibirsk)
Yeshkeev A.R., Professor of Karaganda University (Karaganda)
Sudoplatov S.V., Professor, Deputy Director of IM SB RAS (Novosibirsk)
Tusupov J.A., Professor of ENU named after L.N. Gumilyov (Astana)

Members of the Program Committee:
Bazhenov N.A., Senior Researcher, Institute of Mathematics SB RAS (Novosibirsk, Russia)
Baisalov E.R., Associate Professor, Department of Cryptology
Basheeva A.O., Associate Professor, Department of Algebra and Geometry
Bekenov M.I., Associate Professor, Department of Algebra and Geometry
Verbovsky V.V., Institute of Mathematical Mechanics and Mechanics (Almaty)
Zhetpisov K., Associate Professor, Department of Information Systems, ENU (Astana)
Isakhov A.A., IITU (Almaty)
Kasymov N.Kh., National University of Uzbekistan named after M. Ulugbek, (Tashkent, Uzbekistan)
Kozybaev D.Kh., Dean, Faculty of Mathematical and Mechanics
Latkin I.V., Associate Professor, VKTU named after D. Serikbaeva (Oskemen)
Marhabatov N.D., Head of the Department of Algebra and Geometry
Mustafa M., Nazarbayev University (Astana)
Naurazbekova A.S., Associate Professor of the Department of Algebra and Geometry
Nauryzbaev R.Zh., Associate Professor of the Department of Algebra and Geometry
Nurakunov A.M., Chief Researcher of the Institute of Mathematics of the National Academy of Sciences of the Kyrgyz Republic (Bishkek, Kyrgyzstan)
Nurtazin A.T., KazNU (Almaty)
Peretyatkin M.G., IMMM (Almaty)
Stepanova A.A., professor of Far Eastern Federal University (Vladivostok, Russia)

Tanirbergenov A.Zh., Head of the Department of Cryptology
Khisamiev A.N., Nazarbayev University (Astana)
Khisamiev Z.G., IIVT (Almaty)
Khisamiev N.G., ENU (Astana)

ORGANIZING COMMITTEE

Chairmen:
Kozybaev D.Kh., Dean of the Faculty of Mathematics and Mathematics

Deputy Chairmen:
Adilshina K.K., Head of the Department of Financing and Scholarship Provision of the Department of Finance
Zakirova A.B., Director of the Department of Science of ENU
Konirkhanova A.A., Head of the Department of Information Security
Markhabatov N.D., Head of the Department of Algebra and Geometry
Moldakhmetova A.E., Head of the Department of Scientific Projects and Publications
Mukanova A.A., Head of the Department of Information Systems
Tanirbergenov A.Zh., Head of the Department of Cryptology

Members of the Organizing Committee:
Alimbaev A.A., KRU A.Baitursynuly (Kostanay)
Dauletiyarova A.B., SDU (Almaty)
Zhumabekova G.E., KarU, (Karagandy)
Zambarnaya T.S., IMMM (Almaty)
Issaeva A.K., KarU, (Karagandy)
Kalmurzaev B.S., KBTU (Almaty)
Kasymetova M.T., KarU, (Karagandy)
Kerimbaev R.K., KazNU (Almaty)
Mashurov F.A., Southern University of Science and Technology, Shenzhen, China **(online)**
Musina N.M., KarU, (Karagandy)
Omarova M.T., KarU, (Karagandy)
Popova N.V., KarU, Kazpotrebsouyz(Karagandy)
Sartaev B.K., SDU, NARXOZ (Almaty)
Tulenbaev K.M., KazNU (Almaty)
Tungushbaeva I.O., KarU, (Karagandy)
Ulbricht O.I., KarU, (Karagandy)
Umbetbaev O., SDU (Almaty)
Yarullina A.D, KarU, (Karagandy)
Yershigeshova A. D., SDU (Almaty)

Scientific Secretary: Markhabatov N.D. (markhabatov@gmail.com)

Secretariat: Mamyrov A.O., Fazyl Zh., Nuraly A., Mamyraly A., Kydyrkhankyzy A., Amanbekov S., Koshekova A.K., Kabidenov A., Kasatova A., Arapbaeva M., Sakhanova Zh.A.

The conference will be held in the following sections:
1. Model Theory
2. Theories of Computability and Computable Models
3. Algebra
4. Cryptology
5. Applied Logic and Artificial Intelligence

Selected papers of the participants will be recommended for publication in the journals **"Bulletin of the Abai KazNPU, Series of Physical and Mathematical Sciences" and "Bulletin of Karaganda State University", Series "Mathematics"**, which are included in the Web of Science, Scopus database.
Plenary (30-40-50 min.), contributed and sectional (15-20 min.) are planned. The official languages of the conference are Kazakh, Russian and English.
E-mail of the organizing committee: markhabatov@gmail.com

The conference, including publication of the abstract book and other expenses, is fully supported by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Project No. AP19677451)

VIII International Conference "Kazakh-French Logical Colloquium"
L.N. Gumilyov Eurasian National University,
Faculty of Mechanics and Mathematics,
June 24-27, 2025

PROGRAM

$$T \models \varphi \Leftrightarrow T \vdash \varphi$$

24.06.2025

Tuesday

ZOOM

https://us06web.zoom.us/j/88066558366?pwd=FUOmKnpwqPnwuP2UCEProEfqHbgAdv.1

Conference ID: 880 6655 8366

Access code: 047734

Kazymukan str. 13, room 119

9.00–10.00 **Registration**

9.50–10.00 **Opening**

10.00–10.50 **Goncharov S.S.**

Strong constructibility of prime and saturated models of theory for recursive ordinal

10.50–11.40 **Nurakunov A.M.**

On the semigroups of theories

Coffee break

12.10–13.00 **Frank Wagner**

Simple pseudofinite groups of small dimension, without CFSG (online)

Lunch break

15.00–17.00 **Contributed Talks**

Model Theory — 224 room

Applied Logic and Artificial Intelligence — 205 room

25.06.2025

Wednesday

ZOOM

https://us06web.zoom.us/j/88066558366?pwd=FUOmKnpwqPnwuP2UCEProEfqHbgAdv.1

Conference ID: 880 6655 8366

Access code: 047734

Kazymukan str. 13, room 119

9.00–9.50 **Bruno Poizat**
Logicians and Geometers on Algebraic Groups
9.50–10.40 **Badaev S.A.**
Computable numberings in the Ershov hierarchy
10.40–11.10 Coffee break
11.10–12.00 **Bekenov M.I.**
Formula-definable quasivarieties
12.00–12.20 **Adrien Deloro**
Lie rings in model theory (online)
12.20–12.40 **Bazhenov N.A.**
On effective categoricity for computable structures
12.40–13.00 **Nurtazin A.T.**
Some properties of existentially closed companions

Lunch break

15.00–17.00 **Contributed Talks**
Model Theory — 205 room
Theories of Computability and Computable Models — 224 room

18.00 **Banquet**
Ğajayıp (Restaurant)
Magzhan Zhumabaev Avenue, 26

26.06.2025

Thursday

ZOOM

https://us06web.zoom.us/j/88066558366?pwd=FUOmKnpwqPnwuP2UCEProEfqHbgAdv.1

Conference ID: 880 6655 8366

Access code: 047734

Kazymukan str. 13, room 119

9.00–9.50 **Christian d'Elbée**

Lie methods in omega-categorical Engel groups

9.50–10.40 **Morozov A.S.**

On three kinds of holographicity

10.40–11.10 Coffee break

11.10–12.00 **Basheyeva A.O.**

On two problems of quasivarieties of modular lattices

Special session

12.00–12.20 **Sartayev B.K.**

4-type subvarieties of the variety of associative algebras (online)

12.20–12.40 **Kalmurzayev B.**

Rogers semilattices in finite levels of the Ershov hierarchy

12.40–13.00 **Nauryzbaev R.Zh.**

TBA

Lunch break

15.00–17.00 **Contributed Talks**

Cryptology — 205 room

Applied Logic and Artificial Intelligence — 224 room

18.00 The State Opera and Ballet Theater «Astana Opera»

Dinmuhamed Konaev Street, 1

27.06.2025

Friday

ZOOM

https://us06web.zoom.us/j/88066558366?pwd=FUOmKnpwqPnwuP2UCEProEfqHbgAdv.1

Conference ID: 880 6655 8366

Access code: 047734

Kazymukan str. 13, room 119

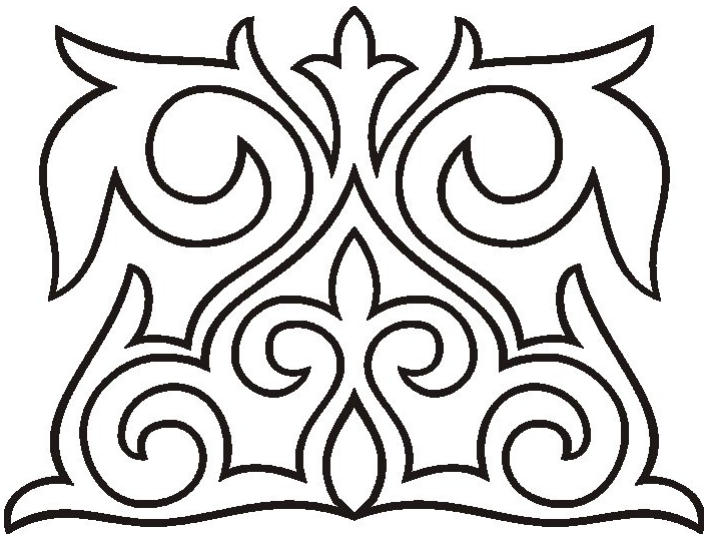
9.00–9.50 **Mashurov F.A.**
On Zinbiel and Tortkara superalgebras (online)
9.50–10.40 **Tokareva N.N.**
International Olympiad in Cryptography as the way to apply your mathematical knowledge
10.40–11.10 Coffee break
11.10–11.30 **Polyakov N.L.**
Generalizations of the Rudin–Keisler order and their model-theoretic applications
11.30–11.50 **Kyle Gannon**
Graphons, hypergraphons, and generic sampling
11.50–12.10 **Yvon Bossut**
A result on groups definable in omega-free PAC fields (online)
12.10–12.30 **Moreno Invitti**
Lie rings in finite dimensional theories (online)
12.30–12.50 **Viktor Verbovskiy**
On pure orderings of Morley o-rank 1

Lunch break

15.00–17.00 **Contributed Talks**
Cryptology (Round Table) — 205 room
Algebra — 224 room

17.00–17.30 **Closing**
room 119

Plenary Talks



Strong constructibility of prime and saturated models of theory for recursive ordinal

S.S. Goncharov, A.M. Petrenko, V.K. Kravtsov, E.I. Khlestova

Camille Jordan Institut, Université Claude Bernard Lyon 1
43 boulevard du 11 novembre 1918
F-69622 Villeurbanne Cedex, France
E-mail: altinel@math.univ-lyon1.fr

Abstract

In the talk, results acquired as a result of investigation into strong construtibility of models on the basis of ordinal constructions [1] will be presented. It was shown that ordinals smaller than ω^ω are strongly constructive on the basis of criteria for strong constructibility of prime models of decidable theories. The basis of this research is the well known paper by A. Tarski, A. Mostowski, and D. Doner[2] on the decidability of elementary theories of any ordinal. Using this technique and computability theory it was shown that for any recusive ordinal λ it is possible to build a strongly constructive presentation for ordinal $\omega^\omega \times \Omega^\lambda$.

Theorem. Any computable ordinal is strongly constructive and the prime and saturated their models of these theories decidable too.

This result can be used for some inductive constructions of models on the basis of ordinals in order to investigate their decidability.

Acknowledgements. *The research of E.I Khlestova was conducted with funding from grant № 23-11-00170 of the Russian Science Foundation, https://rscf.ru/project/23-11-00170/*

References

[1] Y.L. Ershov, S.S. Goncharov Constructive Models. Springer New York, NY, 2012.

[2] Doner J. E., Mostowski, A., Tarski, A. The Elementary Theory of Well-Odering—A Metamathematical Study—. in: Logic Colloquium '77 (A. Macintyre, L. Pacholski, and J. Paris, eds.), Studies in Logic and the Foundations of Mathematics. 1978. V.96. pp.1—54.

On the semigroups of theories

Anvar Nurakunov

Institute of Mathematics, NAS KR, pr. Chu 265a, 720071 Bishkek, Kyrgyzstan

E-mail: a.nurakunov@gmail.com

Abstract

Let $T(\sigma)$ denote the set of all first-order theories in a language σ. For any theories $T, S \in T(\sigma)$, we define a binary operation $\{\cdot\}$ by the rule: $T \cdot S = Th(\{A \times B \mid A \models T \text{ and } B \models S\})$. It is straightforward to verify that the structure $\langle T(\sigma); \cdot \rangle$ forms a commutative semigroup, referred to as the *semigroup of theories* of the language σ. It is is clear that the set of all complete theories in the language σ forms a subsemigroup of $\langle T(\sigma); \cdot \rangle$ which is called the *semigroup of complete theories*.

An idempotent element of the semigroup of theories is called an *idempotent theory*.

A subsemigroup S of $\langle T(\sigma); \cdot \rangle$ is called a *formula definable semigroup* if there is a theory $T \in T(\sigma)$ such that $S = \langle \{X \in T(\sigma) \mid X \cdot T = T\}; \cdot \rangle$. Formula definable semigroups of theories and idempotent theories naturally arise in Rees representations of the semigroup of theories.

In this talk, we will review published results on idempotent theories and formula definable semigroups of (complete) theories, as well as present new findings and examples.

Acknowledgements. The authors has been supported by Ministry of Education and Science of the Republic of Kazakhstan (Grant No. AP23485395)

Simple pseudofinite groups of small dimension, without CFSG

Frank Wagner

Université Claude Bernard Lyon 1

E-mail: wagner@math.univ-lyon1.fr

Abstract

Pseudofinite groups (resp. fields) are infinite groups (fields) which satisfy every first-order property that is true in all finite groups (fields). In [1], Ax characterised pseudofinite fields in purely algebraic terms. Using Ax's result and the classification of finite simple groups (CFSG), Wilson proved that a simple pseudofinite group is elementarily equivalent to a (twisted) Chevalley group over a pseudofinite field [6].

A structure is *supersimple of finite SU-rank* if its definable sets (in some monster model) are equipped with a notion of dimension, called SU-*rank*, taking integer values. It is well known [2] that a pure pseudofinite field F is supersimple of SU-rank 1. Hence, using Wilson's classification, the theory of any simple pseudofinite group G is supersimple of finite SU-rank [4, Theorem 4.1]. In particular, it is easy to see [3, Proposition 6.1] that a simple pseudofinite group G with $\mathrm{SU}(G) = 3$ is isomorphic to $\mathrm{PSL}_2(F)$ for some pseudofinite field F. However, this observation heavily relies on CFSG.

A more general notion was introduced by the second author in [5, Definition 1.1]: A structure is *finite-dimensional* if there is a dimension function dim from the collection of all interpretable sets (again, in some monster model) to $\mathbb{N} \cup \{-\infty\}$. In particular, supersimple structures of finite SU-rank are finite-dimensional, where the dimension is SU-rank. In this case the dimension is *additive* and *fine*.

We reprove Wilson's identification for a pseudofinite groups of dimension 3 withut CFSG, thus answering positively [3, p. 3, Question (3)] and [4, p. 171].

Theorem (Without CFSG). *Let G be a pseudofinite finite-dimensional group with additive and fine dimension. If $\dim(G) = 3$, then either G is soluble-by-finite, or $\widetilde{Z}(G)$ is finite and $G/\widetilde{Z}(G)$ has a definable subgroup of finite index isomorphic to $\mathrm{PSL}_2(F)$ where F is a pseudofinite field.*

Our result suggests the following question.

Question. *Let G be a non-abelian definably simple pseudofinite group. Can one show, independently of CFSG, that G is finite-dimensional with additive and fine dimension?*

This is joint work with Ulla Karhumäki.

References

[1] James Ax. The Elementary Theory of Finite Fields. Annals of Mathematics, 88(2):239–271, 1968.

[2] Zoé Chatzidakis, Lou van den Dries, and Angus Macintyre. Definable sets over finite fields. J. Reine Angew. Math., 427:107–135, 1992.

[3] Richard Elwes, Eric Jaligot, Dugald Macpherson, and Mark Ryten. Groups in supersimple and pseudofinite theories. Proceedings of the London Mathematical Society, 103(6):1049–1082, 2011.

[4] Dugald Macpherson. Model theory of finite and pseudofinite groups. Archive for Mathematical Logic, 57:159–184, 2018.

[5] Frank O. Wagner. Dimensional groups and fields. The Journal of Symbolic Logic, 85(3):918–936, 2020.

[6] John S. Wilson. On simple pseudofinite groups. Journal of the London Mathematical Society, 51(2):471–490, 1995.

Logicians and Geometers on Algebraic Groups

Bruno POIZAT

Université Claude Bernard Lyon 1

E-mail: poizat@math.univ-lyon1.fr

Abstract

Algebraic groups are defined in Algebraic Geometry in a very specific way, permitting them to produce a Group scheme whose rational points over an arbitrary field K form a group GK ; the only constraint is that K contains the parameters involved in the definition of the group. The geometric isomorphisms, allowing Geometers to identify two algebraic groups, are similarly defined in a very restricted manner.

On the other hand, the Model Theorists, while working in an algebraically closed field K, consider the groups and the group-homomophisms which are definable in K; they are called constructible by the Geometers. In some sense, constructible groups are the same as algebraic groups, since it is a theorem that a constructible group is constructibly isomorphic to an algebraic group, which is unique in characteristic 0, when any constructible group-homomorphism between algebraic groups is in fact geometric.

But this is no more the case in characteristic p, where two algebraic groups may be constructibly isomorphic without being geometrically isomorphic: in other words, they have the same rational points over every algebraically closed field, but not over every field. They are considered as the same object by Model Theorists, but not by Geometers. This phenomenon may be a source of confusion when we transfer a result from one domain to the other.

In this talk I will approach the simple algebraic groups from a model theoretic perspective, keeping in mind the Algebraicity Conjecture of Zilber and Cherlin, which is open since 50 years, and which claims that they represent the general case of simple groups of finite Morley rank. We shall study the connection between the automorphisms of the simple group G and the automorphisms of the base field K.

The essential fact is that such a group form what I call an Autonomous constructible structure. In characteristic 0, in any such structure S we can define without parameters a copy L of the base field, and as a consequence we show that the group of constructible automorphisms of S is definable, and is the largest superstable group of automorphisms of S.

In characteristic p, we can define without parameters only a multifield $(L_1, \ldots, L_n)$ of copies of K, but there exists in this case also a maximal definable group $Aut_{max}(S)$ of automorphisms of S, which is also its maximal superstable group of automorphisms.

We obtain a constructible version of Borel-Tits Theorem: if two autonomous contructible structures, and in particular two simple algebraic groups, defined over the same algebraically closed field K, are abstractly isomorphic, they are constructively isomorphic.

All the results above are obtained by general methods from Model Theory, but to identify, in the case of an algebraic simple group G, the group $Aut_{max}(S)$ with the group of geometric automorphisms of G, we need a deep result from Algebraic Geometry, namely the Theorem of Borel and Tits, taking into full account the special isogenies discovered by Chevalley.

References

Paramètres dans les corps algébriquement clos, to appear in Annales Mathématiques du Québec

Logique et Géométrie, to appear in Béziau Festschrift, Springer

Logiciens et Géomètres: deux points de vue sur les groupes algébriques, to appear in Atlantika

Computable numberings in the Ershov hierarchy

Serikzhan Badaev

Kazakh-British Technical University

E-mail: sbadaev@gmail.com

Abstract

The paper of Yuri L. Ershov [1] and the joint paper of Sergey S. Goncharov and Andrea Sorbi [3] have played a fundamental role in research on the theory of computable numberings over the past half century.

In [1], Ershov formulated the notion of the upper semilattice of computable numberings for an arbitrary family of computably enumerable sets and posted several problems that attracted many researchers and indeed simulated great activity in the study of the computable numberings of the families of c.e. sets. Two main problems posted by Ershov in this article as well as in his lectures at the Novosibirsk University in 1967–68 are the following:

1. Find a structural criterion for a family of c.e. sets to have one-element upper semilattice of computable numberings.

2. What is a possible number of minimal elements in upper semilattice of computable numberings.

The results in attempts forwards solving these and many other problems during the first decade after their posting were accumulated in the monograph [2].

In [3], Goncharov and Sorbi suggested the notion of generalized computable numbering for a family of sets that admit definability in some formal language. Their approach implies that a generalized computable numbering is an 'uniformly enumerable' sequence of the sets of a family for which one could define a notion of an 'enumeration procedure'. The approach of Goncharov-Sorbi allowed to introduce the notion of the upper semilattice of generalized computable numberings (currently known as Rogers semilattice) for a family of sets from a couple known classes such as the classes of arithmetical and analytical sets and to formulate the generalized Ershov problems as follows:

What is a possible cardinality of Rogers semilattices? What is a possible number of minimal elements in Rogers semilattices of infinite families of sets?

Besides, the problem of an existence of the greatest element and the problem of an existence and number of minimal elements, especially of well-known types (Friedberg, positive, non-positive) arose in a natural way.

Remind the basic notions. Let n be a positive integer.

A numbering α of a family $\mathcal{A}$ of Σ^i_n sets is called Σ^i_n-computable if $\{(m,x) \mid x \in \alpha(m)\} \in \Sigma^i_n$. Here $i \in \{-1,0,1\}$. $\mathrm{Com}^i_n(\mathcal{A})$ denotes the set of all Σ^i_n-computable numberings of $\mathcal{A}$.

A numbering α is reducible to a numbering β ($\alpha \leqslant \beta$) if $\alpha = \beta \circ f$ for some computable function f. α is equivalent to β ($\alpha \equiv \beta$) if $\alpha \leqslant \beta$ and $\beta \leqslant \alpha$. Rogers semilattice $\mathcal{R}^i_n(\mathcal{A})$ is the quotient structure $\langle \mathrm{Com}^i_n(\mathcal{A})_{/\equiv}, \leqslant \rangle$ w.r.t. equivalence of numberings.

The talk is aimed to show results in the study of Rogers semilattices of the families in the Ershov hierarchy in compare with achievements in the arithmetical case for which the solution of both problems of Ershov have succeeded, [3], [4].

We have to mention only two surprising facts to illustrate the difference between the Rogers semilattices in the case of c.e. sets and the case of the differences of c.e. sets:

Theorem 1 (Badaev and Talasbaeva, [5]). *There exists a family* $\mathcal{A} = \{A \subset B\} \subseteq \Sigma_2^{-1}$ *s.t.* $|\mathcal{R}_2^{-1}(\mathcal{A})| = 1$.

Theorem 2 (Abeshev, [6]). *There is a family which consists of disjoint two non-empty* Σ_2^{-1} *sets and has no principal numberings.*

The following theorem played a crucial role in the understanding of the structure of $\mathcal{R}_2^{-1}(\mathcal{A})$ for the families $\mathcal{A} \subseteq \Sigma_2^{-1}$.

Theorem 3 (Badaev and Lempp, [7]). *There exists a family of d.c.e. sets whose Rogers semilattice consists of an upper cone and exactly one element that is outside of that cone.*

Due to the Frank Stephan operator Γ_k, [8]: for every family $\mathcal{A} \subseteq \Sigma_k^{-1}$ there is a family $\Gamma_k(\mathcal{A} \subseteq \Sigma_{k+1}^{-1}$ such that $\mathcal{R}_k^{-1}(\mathcal{A})$ and $\mathcal{R}_{k+1}^{-1}(\Gamma_k(\mathcal{A})$ are isomorphic.

And now we stop at the current state of Ershov's problems:

Theorem 4 (Badaev and Goncharov, in preparation). *There is a family* $\mathcal{A} \subseteq \Sigma_2^{-1}$, *whose Rogers semilattice* $\mathcal{R}_{n+2}^{-1}(\mathcal{A})$ *has the greatest element and exactly two minimal elements.*

Theorem 5 (Badaev, Bazhenov, Goncharov, Kalmurzaev, Mel'nikov, and Ng, in preparation). *There is a family* $\mathcal{A} \subseteq \Sigma_2^{-1}$ *with two-element Rogers semilattice* $\mathcal{R}_2^{-1}(\mathcal{A})$.

References

[1] Ershov, Yu.L. *Numberings of the families of total recursive functions*, Sib. Math. J., 1967, v.8, no.5., pp.771–778.

[2] Ershov Yu.L. Theory of Numberings. Nauka, Moscow, 1977.

[3] Goncharov, S.S., Sorbi, A. *Generalized computable numerations and non-trivial Rogers semilattices.* Algebra and Logic, 1997, vol. 36, no. 6, 359–369.

[4] Badaev S.A., Goncharov S.S. *On Rogers semilattices of families of arithmetical sets.* Algebra and Logic, 2001, vol. 40, no. 5, pp. 283–291.

[5] Badaev S., Talasbaeva Zh. *Computable numberings in the Hierarchy of Ershov.* Proceedings of 9th Asian Logic Conference, Novosibirsk, August 2005, S.Goncharov (Novosibirsk), H.Ono (Tokyo), and R.Downey (Wellington)(eds.). World Scientific Publishers. 2006, pp.17–30.

[6] Abeshev K. *On the existence of universa numberings for finite families of d.c.e. sets.* Mathematical Logic Quaterly, 2014, vol. 60, no. 3, 161–167.

[7] Badaev S.A., Lempp S. *A decomposition of the Rogers semilattice of a family of d.c.e. sets.* Journal of Symbolic Logic, 2009, no 2, 618–640.

[8] Herbert I, Jain S., Lempp S, Mustafa M., Stephan F. *Reductions between types of numberings.* Annals of Pure and Applied Logic, vol, 170(12), 102716.

Formula-definable quasivarieties

Bekenov M.I.

L.N. Gumilyov Eurasian National University

st. Pushkina, 11

010008, Astana, Kazakhstan

E-mail: bekenov50@mail.ru

Abstract

Some results of the ongoing research on the study of the properties of formula-definable quasivarieties by the participants (Bekenov M.I., Kasatova A.M., Kabidenov A.A., Kozybaev D.Kh., Mamyraly A., Makhrabatov N.D., Nurakunov A.M.) of the scientific seminar named after A.D. Taimanov at the L.N. Gumilev ENU are proposed.

Lie methods in omega-categorical Engel groups

Christian d Elbee

University of the Basque Country

E-mail: christian.delbee@ehu.eus

Abstract

In 1981, Wilson conjectured that any ω-categorical locally nilpotent p-group is nilpotent. If true, a quite satisfactory decomposition of ω-categorical groups would follow. This conjecture is very much open more than 40 years later. The analogue statement for Lie algebras (every locally nilpotent ω-categorical Lie algebra is nilpotent) is also open. Both statement can be reformulated as: any omega-categorical Engel group/Lie algebra is nilpotent. As such, those questions are connected to Burnside-type problems and the work of Higman, Kostrikin, Zelmanov, Vaughan-Lee, Traustason, etc. For instance, using a classical result of Zelmanov, the conjecture for Lie algebras is true asymptotically in the following sense: for each $n \in \mathbb{N}$, every n-Engel Lie algebra over $\mathbb{F}_p$ is nilpotent for all but finitely many p's. There is a similar statement for groups. The situation for small values of the pair (n, p) is highly characteristic-dependent, for instance, 4-Engel Lie algebras over a field of characteristic p are nilpotent except if $p = 2, 3$ or 5. I recently proved that ω-categorical n-Engel Lie algebras over a field of characteristic p are nilpotent for $(n, p) = (3, 5)$ and $(n, p) = (4, 3)$. In this talk I will convey ideas of the proof for $(n, p) = (3, 5)$ and explain how to use this result to prove that ω-categorical 5-Engel 5-groups are nilpotent. This work is at the intersection of model theory, group theory and computer algebra.

On three kinds of holographicity

A. S. Morozov

Sobolev institute of mathematics SB RAS, Novosibirsk, Russia

E-mail: morozov@math.nsc.ru

Abstract

In the talk, we present a series of results on the power of methods of reconstruction of algebraic structures from their finite parts (sets of prototypes) provided that some family of transformations preserving the structure is known.

We consider the following three methods of reconstruction of structures from their finite parts:

- Reconstruction of a structure from a finite set of prototypes if we know its automorphisms, which corresponds to the notion of *holographicity*.
- Reconstruction of a structure from a finite set of prototypes if we know its self–embeddings, which corresponds to the notions of*weak holographicity* and *weak coholographicity*.

Structures that can be defined up to isomorphism using these methods are called respectively holographic, weakly holographic and weakly coholographic.

We give descriptions of such structures in some classes of structures and describe the relationship between these three notions and countable categoricity.

On two problems of quasivarieties of modular lattices

A. O. Basheyeva

L. N. Gumilev Eurasian National University
Astana

Kazakhstan

E-mail: basheyeva3006@gmail.com

Abstract

A quasi-variety of lattices is an axiomatic class of lattices closed under sublattices, direct products and ultra products of lattices. A finite lattice has no finite basis of quasi-identities if the quasivariety generated by this lattice is not finitely axiomatizable.

A (topological) algebra is *profinite* if it is representable as an inverse limit of finite algebras (endowed with the product topology). A quasivariety $\mathcal{N}$ is profinite if every profinite algebra in $\mathcal{N}$ is an inverse limit of finite algebras from $\mathcal{N}$.

For a finite algebra A, the class $\mathbb{S}_c\mathbb{P}(A)$ of all topologically closed subalgebras of non-zero direct powers of A with respect to the product topology is called a *topological quasivariety* generated by A. It is well known results of the general topology state that an algebra B belongs to $\mathbb{S}_c\mathbb{P}(A)$ if and only if B is an inverse limit of some set of finite algebras, moreover, B carrying a Boolean topology τ (compact, Hausdorff and with a basis of clopen sets) such that each operation in B is continuous relative τ. According to [1], a topological quasivariety generated by a finite algebra is *standard* if it is profinite.

There are two well-known and closely related problems in universal algebra and lattice theory: Which finite lattices generate finitely based quasivarieties? and Which finite lattices generate standard topological quasivarieties? The first problem is attributed to V. A. Gorbunov and D. M. Smirnov (1978) [2], while the second is due to D. M. Clark, B. A. Davey, M. G. Jackson, and J. G. Pitkethly (2008) [1].

The main goal of this talk is to discuss the results obtained on both problems and to present some new ones.

References

[1] D.M. Clark, B.A. Davey, M. Haviar, J.G. Pitkethly, R. Talukder, *Standard topological quasi-varieties*, Houston Journal of Mathematics, 29 (2003), 859–887.

[2] V.A. Gorbunov, D.M. Smirnov, *Finite algebras and the general theory of quasivarieties*, Colloq. Mathem. Soc. Janos Bolyai, Finite algebra and multipli-valued logic, Szeged (Hungary), 28 (1979), 325–332.

On Zinbiel and Tortkara superalgebras

F. Mashurov

Shenzhen International Center for Mathematics, SUSTech, Shenzhen, China

E-mail: invitti@math.univ-lyon1.fr

Abstract

This talk presents the main results on Zinbiel superalgebras and special Tortkara superalgebras, highlighting key differences between the super and the non-super setting. We present examples of Zinbiel superalgebras with Rota-Baxter operators and construct a basis for free Zinbiel superalgebras. Moreover, we establish a superalgebraic analogue of the Lie criterion for Zinbiel superalgebras. In contrast to the classical case, some homomorphic images of special Tortkara superalgebras on two generators are exceptional. Finally, we present a classification of all Tortkara superalgebras of dimensions 2 and 3.

The talk is based on my recent joint work with Sofiane Bouarroudj. This research was supported by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP22683764)

International Olympiad in Cryptography as the way to apply your mathematical knowledge

Natalia Tokareva

Novosibirsk State University

E-mail: crypto1127@mail.ru

Abstract

In this talk we want to attract your attention to some practical applications of methods of discrete mathematics, algebra and logics in cryptography. Solutions of many real cryptographic tasks that appear in applications are based on math achievements. That is why we invite professionals and students to apply their knowledge to solving olimpiad tasks of NSUCRYPTO.

Non-Stop University CRYPTO (**NSUCRYPTO**) is the unique international competition for professionals, school and university students, providing various problems on theoretical and practical aspects of modern cryptography, see [1]. The main goal of the olympiad is to draw attention of young researchers not only to educational tasks, but also to complicated scientific problems at the intersection of mathematics and cryptography. That is why every year we include open problems into the list of tasks; some of them deserve an individual publication in case of being solved. Since NSUCRYPTO holds via the Internet, everybody can easily take part in it.

The first Olympiad was held in 2014, since then several thousands students and specialists from more than 70 countries took part in it. The Program committee includes 31 members from cryptographic groups all over the world. Main organizers and partners are Cryptographic center (Novosibirsk), National Technology Center for Digital Cryptography, Novosibirsk State University, Kryptonite, Aktiv company, KU Leuven, Southern Federal University, Infotecs, Kovalevskaya North-West Center of Mathematical Research, Belarusian State University, Tomsk State University and Nsucrypto-lab.

In 2024 there were more than 1250 participants from 47 countries.

Following the results of each Olympiad we publish scientific articles with detailed solutions and some analysis of the solutions proposed by the participants, including advances on unsolved ones, see for instance [3, 2, 14, 7, 8, 9, 10, 11, 13].

One of the main characteristic of the Olympiad is that unsolved scientific problems are proposed to the participants in addition to problems with known solutions. All 38 open problems that were offered since the first NSUCRYPTO can be found here [1]. Some of these problems are of great interest to cryptographers and mathematicians for many years. These are such problems as “APN permutation” (2014), “Big Fermat numbers” (2016), “Boolean hidden shift and quantum computings” (2017), “Disjunct Matrices” (2018), and others.

We are proud that some researchers continue to work on solutions of unsolved problems even after the Olympiad was over. For example, authors of [12] proposed a complete solution for problem “Orthogonal arrays” (2018). Partial solutions for another open problem, “A secret sharing”, (2014) were presented in [5], [6], and a recursive algorithm for finding the solution was proposed in [4].

We invite students and young researchers to participate in the Olympiad.

Acknowledgements. *The work is supported by National Technology Center for Digital Cryptography, Novosibirsk State University, Kryptonite, Aktiv company, Southern Federal University, Kovalevskaya North-West Center of Math. Research.*

References

[1] Website of the Olympiad https://nsucrypto.nsu.ru/

[2] Agievich S., Gorodilova A., Idrisova V., Kolomeec N., Shushuev G., Tokareva N. Mathematical problems of the second international student's Olympiad in cryptography, Cryptologia, **41**:6 (2017), 534–565.

[3] Agievich S., Gorodilova A., Kolomeec N., Nikova S., Preneel B., Rijmen V., Shushuev G., Tokareva N., Vitkup V. Problems, solutions and experience of the first international student's Olympiad in cryptography, Prikladnaya Diskretnaya Matematika (Applied Discrete Mathematics), 3 (2015), 41–62.

[4] Ayat S. M., Ghahramani M. A recursive algorithm for solving "a secret sharing" problem", Cryptologia, **43**:6 (2019), 497–503.

[5] Geut K., Kirienko K., Sadkov P., Taskin R., Titov S. On explicit constructions for solving the problem "A secret sharing", Prikladnaya Diskretnaya Matematika. Prilozhenie, 10 (2017), 68–70 (in Russian).

[6] Geut K. L., Titov S. S. On the blocking of two-dimensional affine varieties, Prikladnaya Diskretnaya Matematika. Prilozhenie, 12 (2019), 7–10 (in Russian).

[7] Gorodilova A., Agievich S., Carlet C., Gorkunov E., Idrisova V., Kolomeec N., Kutsenko A., Nikova S., Oblaukhov A., Picek S., Preneel B., Rijmen V., Tokareva N. Problems and solutions of the Fourth International Students' Olympiad in Cryptography (NSUCRYPTO), Cryptologia, **43**:2 (2019), 138–174.

[8] Gorodilova A., Agievich S., Carlet C., Hou X., Idrisova V., Kolomeec N., Kutsenko A., Mariot L., Oblaukhov A., Picek S., Preneel B., Rosie R., Tokareva N. The Fifth International Students' Olympiad in Cryptography — NSUCRYPTO: problems and their solutions, Cryptologia, **44**:3 (2020), 223–256.

[9] Gorodilova A., Tokareva N., Agievich S., Carlet C., Gorkunov E., Idrisova V., Kolomeec N., Kutsenko A., Lebedev R., Nikova S., Oblaukhov A., Pankratova I., Pudovkina M., Rijmen V., Udovenko A. On the Sixth International Olympiad in Cryptography NSUCRYPTO, Journal of Applied and Industrial Mathematics, **14**:4 (2020), 623–647.

[10] Gorodilova A. A., Tokareva N. N., Agievich S. V., Carlet C., Idrisova V. A., Kalgin K. V., Kolegov D. N., Kutsenko A. V., Mouha N., Pudovkina M. A., Udovenko A. N. The Seventh International Olympiad in Cryptography: problems and solutions, Siberian Electronic Mathematical Reports, **18**:2 (2021), A4–A29.

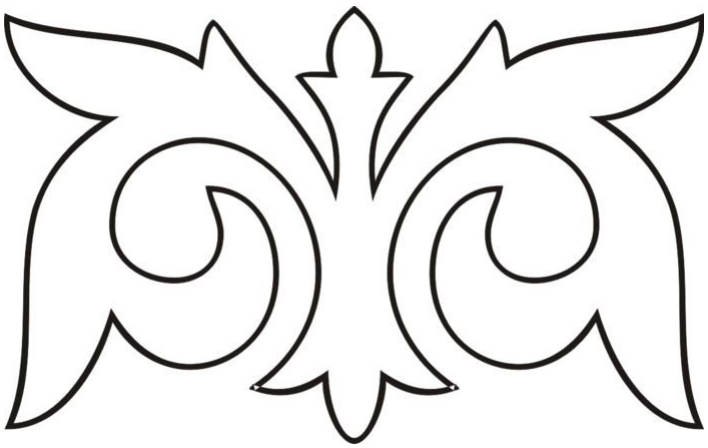
[11] Gorodilova A. A., Tokareva N. N., Agievich S. V., Beterov I.I., Beyne T., Budaghyan L., Carlet, C., Dhooghe S., Idrisova V.A., Kolomeec N.A., Kutsenko A.V., Malygina E.S., Mouha N., Pudovkina M.A., Sica F., Udovenko A.N. An overview of the Eight International Olympiad in Cryptography "Non-Stop University CRYPTO", Siberian Electronic Mathematical Reports, **19**:1 (2022), A9–A37.

[12] Kiss R., Nagy G. P. On the nonexistence of certain orthogonal arrays of strength four, Prikladnaya Diskretnaya Matematika (Applied Discrete Mathematics), 52 (2021), 65–68.

[13] Idrisova V.A., Tokareva N.N., A. A. Gorodilova, I. I. Beterov, T. A. Bonich, E. A. Ishchukova, N. A. Kolomeec, A. V. Kutsenko, E. S. Malygina, I. A. Pankratova, M. A. Pudovkina, A. N. Udovenko // Mathematical problems and solutions of the Ninth International Olympiad in cryptography NSUCRYPTO // Prikladnaya Diskretnaya Matematika (Applied Discrete Mathematics). 2023, No. 4, P. 29-54.

[14] Tokareva N., Gorodilova A., Agievich S., Idrisova V., Kolomeec N., Kutsenko A., Oblaukhov A., Shushuev G. Mathematical methods in solutions of the problems from the Third International Students' Olympiad in Cryptography, Prikladnaya Diskretnaya Matematika (Applied Discrete Mathematics), 40 (2018), 34–58.

Special Session



Lie rings in model theory

Adrien Deloro

Sorbonne Université

E-mail: adrien.deloro@imj-prg.fr

Abstract

This is a talk in model-theoretic algebra. A *Lie ring* is an abelian group $(V, +)$ equipped with a bracket $[\cdot, \cdot]\colon V \times V \to V$ which is additive in each variable, antisymmetric, and satisfies the Jacobi identity. This is like a Lie algebra, but without an underlying vector space structure.

One conjectures that under reasonable model-theoretic assumptions, an infinite, simple Lie ring should be a Lie *algebra* over an interpretable field. This is the Lie-analogue of the Cherlin-Zilber conjecture on groups. The difficulty concentrates in positive characteristic (where Lie algebras are notoriously more challenging than in characteristic 0).

Mostly due to the lack of a 'Lie correspondence' in model theory, the Cherlin-Zilber conjecture and its Lie-analogue have no relationship. However the latter deserves some attention, recently regained after seminal (and forgotten for decades) work by Zilber and Rosengarten.

The talk will survey what is known in this direction, and possible next steps. No knowledge of Lie theory is required.

ON EFFECTIVE CATEGORICITY FOR COMPUTABLE STRUCTURES

Nikolay Bazhenov

Sobolev Institute of Mathematics (Novosibirsk, Russia)

E-mail: nickbazh@yandex.ru

Abstract

The systematic investigations of computable categoricity (autostability) go back to the works of A.I. Mal'tsev [3]. For a Turing degree $\mathbf{d}$, a computable structure $\mathcal{S}$ is $\mathbf{d}$-*computably categorical* if the degree $\mathbf{d}$ can compute isomorphisms between arbitrary computable copies of $\mathcal{S}$. The *categoricity spectrum* of the structure $\mathcal{S}$ contains all degrees $\mathbf{d}$ such that $\mathcal{S}$ is $\mathbf{d}$-computably categorical. If the categoricity spectrum of $\mathcal{S}$ has a least degree $\mathbf{x}$, then $\mathbf{x}$ is called the *degree of categoricity* for $\mathcal{S}$. In the last 15 years, the categoricity spectra theory [2] has been one of the actively developing areas of the modern computability theory.

The talk gives an overview of the recent results on categoricity spectra and degrees of categoricity. We focus on effective categoricity for structures belonging to familiar classes, including decidable models [3], linear orders [4, 5], Heyting algebras [6, 7].

References

[1] A. I. Mal'tsev, *Constructive algebras. I*, *Russian Mathematical Surveys, 16*(3), 77–129, 1961. https://doi.org/10.1070/RM1961v016n03ABEH001120

[2] E. B. Fokina, I. Kalimullin, and R. Miller, *Degrees of categoricity of computable structures*, *Archive for Mathematical Logic, 49*(1), 51–67, 2010. https://doi.org/10.1007/s00153-009-0160-4

[3] N. A. Bazhenov, *Autostability spectra for decidable structures*, *Mathematical Structures in Computer Science, 28*(3), 392–411, 2018. https://doi.org/10.1017/S096012951600030X

[4] N. A. Bazhenov, *Degrees of autostability for linear orders and linearly ordered abelian groups*, *Algebra and Logic, 55*(4), 257–273, 2016. https://doi.org/10.1007/s10469-016-9395-4

[5] N. A. Bazhenov, *Categoricity spectra of computable structures*, *Journal of Mathematical Sciences, 256*(1), 34–50, 2021. https://doi.org/10.1007/s10958-021-05419-x

[6] N. A. Bazhenov, *Effective categoricity for distributive lattices and Heyting algebras*, *Lobachevskii Journal of Mathematics, 38*(4), 600–614, 2017. https://doi.org/10.1134/S1995080217040035

[7] N. Bazhenov, *Computable Heyting algebras with distinguished atoms and coatoms*, *Journal of Logic, Language and Information, 32*(1), 3–18, 2023. https://doi.org/10.1007/s10849-022-09371-0

Some properties of existentially closed companions

Nurtazin A.T.

al-Farabi Kazakh National University

E-mail: abyznurtazin80@gmail.com

Abstract

From the existential closeness of the structure $\mathcal{M}$ in the extension $\mathcal{N}$ follows the coincidence of their existential and universal theories. Then their union $T^c = Th_\exists(\mathcal{M}) \cup Th_\forall(\mathcal{M})$ is called a companion theory of the structure $\mathcal{M}$, and the class of all the models of this companion theory is called a companion-class $C(\mathcal{M})$ of the structure $\mathcal{M}$. Research in this area was started by A. Robinson in the early fifties, when he proved some remarkable properties of algebraically closed fields and created a complete and beautiful theory of model completeness. He also proposed to generalize the concept of "a structure being existentially closed in its extension" to the concept of "a structure being existentially closed in some theory." It is easy to see that this property reduces to the property of "being existentially closed in any of its companion extensions".

It was clear from the beginning that the problem of identifying existentially closed structures even in classical algebras turned out to be very difficult. Therefore, in 1970, A. Robinson and John Barwise proposed to use a new method of "forcing" from set theory for their construction. They proved that the structures obtained using this method are existentially closed. Due to the importance of this class, it received a separate name "forcing companion". It is well known that all forcing structures are existentially closed. Therefore, the following statement seems unexpected, and has several important consequences.

Theorem 1. *Existentially closed and forcing companions coincide.*

As it turns out, this theorem implies that a number of properties of existentially closed companions are similar to the corresponding properties of model-complete ones.

Theorem 2. *The elementary theory of any existentially closed companion is complete, and the usual inclusion between two existentially closed structures belonging to it is elementary.*

The question of the quantifier complexity of existentially closed companions is still open. Any companion theory has quantifier complexity one, and its completeness is a very exotic property. At the same time, there are many natural and important complete axiomatizable theories. It can be shown that any companion theory has a unique $\forall\exists-$axiomatizable extension, which is naturally called its inductive companion.

Theorem 3. *Any inductive companion is contained in an existentially closed one.*

It follows from this theorem that if a given inductive companion is complete, it coincides with the elementary theory of existential closure.

It should be noted that in the proofs of all the theorems given above, "Fraisse classes" play an important role. But in the following theorem, which provides necessary and sufficient conditions for the model completeness of the elementary theory of an existentially closed companion, the properties of finite structures from its Fraisse class are used directly.

References

[1] Robinson A/, *On the Metamathematics of Algebra, Amsterdam: North-Holland, 1951.*

[2] Robinson A, *Infinite forcing in model theory, Proceedings of the second Scandinavian Logic Symposium, Amsterdam, North-Holland, 1971, 317-340.*

[3] Nurtazin A.T., Countable existentially closed models of universally axiomatizable theories, Mathematical works, Novosibirsk, Institute of Mathematics SB RAS named after S.L. Sobolev, 2015, .18, No. 1, 48-97

[4] A. T. Nurtazin, Forcing formulas in Fraïssé structures and classes, Algebra and Logic, 57:5 (2018), 368–380

4-type subvarieties of the variety of associative algebras

B. K. Sartayev

Narxoz University, Almaty, Kazakhstan

E-mail: baurjai@gmail.com

Abstract

Associative algebras are closely related to several important classes of algebras, including Lie algebras, Jordan algebras, dendriform algebras, and noncommutative Novikov algebras. For example, the Poincaré-Birkhoff-Witt theorem provides the embedding of any Lie algebra into an appropriate associative algebra under the commutator. Some Jordan algebras can be obtained from associative algebras using the anti-commutator. However, there exist exceptional Jordan algebras that cannot be embedded into any associative algebra via the anti-commutator [1].

In this talk, we define four types of associative algebras based on Mal'cev's classification. In [2], it was shown that the space of identities of degree 3 in associative algebras can be decomposed into subspaces defined by the following identities:

$$abc + bac + acb + cab + bca + cba = 0, \tag{1}$$
$$abc - bac - acb + cab + bca - cba = 0, \tag{2}$$
$$abc + bac - bca - cba = 0, \tag{3}$$
$$abc + acb - cba - cab = 0. \tag{4}$$

Using these identities, we define the corresponding subvarieties.

We study these subvarieties from the point of view of operads and show connections with well-known algebras such as dendriform algebras and noncommutative Novikov algebras. Finally, we define new operations—commutator and anti-commutator on these algebras and obtain some identities under these new operations.

References

[1] P. M. Cohn, On homomorphic images of special Jordan algebras, Canadian Journal of Mathematics, 6, 1954, 253–264.

[2] A. I. Mal'cev, On algebras defined by identities (Russian), Mat. Sbornik N. S., 26(68), 1950, 19–33.

ROGERS SEMILATTICES IN FINITE LEVELS OF THE ERSHOV HIERARCHY

B. S. KALMURZAYEV, K. M. NG, N. A. BAZHENOV, D. NURLANBEK

Kazakh-British Technical University, E-mail: birzhan.kalmurzayev@gmail.com

Abstract

The Rogers semilattice is one of the main objects in numbering theory. The most basic invariant of Rogers semilattices is their cardinality. A classical result in this area is the famous Khutoretskii's theorem, which states that the cardinality of a Rogers semilattice for computable families is either one or infinite [1]. Badaev and Lempp showed in their paper that Khutoretskii's construction does not work in the case of Rogers semilattices for families from the Ershov hierarchy [2].

The talk will discuss some cases where a Khutoretskii-type construction does work for families from finite levels of the Ershov hierarchy.

References

[1] Khutoretskii, A. B. (1971). The power of the upper semilattice of computable numerations. Algebra i logika, 10(5), 561-569.

[2] S. A. Badaev, S. Lempp, A decomposition of the Rogers semilattice of the family of d.c.e. sets, The Journal of Symbolic Logic, 2009, vol. 74, no. 2, p. 618–640.

Generalizations of the Rudin–Keisler order and their model-theoretic applications

Nikolai L. Poliakov, Denis I. Saveliev

HSE University, Higher School of Modern Mathematics MIPT

E-mail: niknikols0@gmail.com, d.i.saveliev@gmail.com

Abstract

As usual, $\boldsymbol{\beta}X$ denotes the standard Čech–Stone compactification of the discrete space X, which we identify with the set of ultrafilters over X (see [2, 6]). We consider here ultrafilters over ω although most of our results remain true for ultrafilters over any infinite set X. The *Rudin–Keisler* preorder $\leq_{\mathrm{RK}}$ on $\boldsymbol{\beta}\omega$ is defined by letting $\mathfrak{u} \leq_{\mathrm{RK}} \mathfrak{v}$ iff there exists $f : \omega \to \omega$ such that $\widetilde{f}(\mathfrak{v}) = \mathfrak{u}$, where $\widetilde{f} : \boldsymbol{\beta}\omega \to \boldsymbol{\beta}\omega$ is the continuous extension of f. The *Comfort* preorder $\leq_{\mathrm{C}}$ on $\boldsymbol{\beta}\omega$ is defined by letting $\mathfrak{u} \leq_{\mathrm{C}} \mathfrak{v}$ iff any $\mathfrak{v}$-compact space is $\mathfrak{u}$-compact, where a space X is $\mathfrak{u}$-*compact* iff $\widetilde{f}(\mathfrak{u}) \in X$ for any $f : \omega \to X$. (See [2, 6] for more on ultrafilters and $\leq_{\mathrm{RK}}$, and [3, 4] for $\leq_{\mathrm{C}}$.)

For $\mathfrak{u}, \mathfrak{v} \in \boldsymbol{\beta}\omega$ and any ordinal α, define: $\mathfrak{u}\, R_0\, \mathfrak{v}$ iff $\mathfrak{u}$ is principal, $R_{<\alpha} = \bigcup_{\beta<\alpha} R_\beta$, and $\mathfrak{u}\, R_\alpha\, \mathfrak{v}$ iff there exists a continuous map $f : \boldsymbol{\beta}\omega \to \boldsymbol{\beta}\omega$ such that $f(\mathfrak{v}) = \mathfrak{u}$ and $f(n)\, R_{<\alpha}\, \mathfrak{v}$ for all $n < \omega$. The hierarchy is non-degenerate and lies between $\leq_{\mathrm{RK}}$ and $\leq_{\mathrm{C}}$ as stated in the following theorem.

Theorem 1. *$R_1 = \leq_{\mathrm{RK}}$; $R_{<\alpha} \subset R_\alpha$ for all $\alpha < \omega_1$; $R_{<\omega_1} = R_{\omega_1} = \leq_{\mathrm{C}}$.*

If X, Y are spaces and α is an ordinal, $f : X^\alpha \to Y$ is *right-continuous w.r.t. $A \subseteq X$* iff for all $\beta < \alpha$ the shift $x \mapsto f(a_0, a_1, \dots, x, b_{\beta+1}, b_{\beta+2}, \dots)$ is continuous whenever $a_0, a_1, \dots \in A$ and $b_{\beta+1}, b_{\beta+2}, \dots \in X$. As shown in [8, 9], if $n < \omega$, X is discrete, and Y is compact Hausdorff, then every $f : X^n \to Y$ uniquely extends to $\widetilde{f} : (\boldsymbol{\beta}X)^n \to Y$ that is right-continuous w.r.t. X. This fact provides a canonical way to obtain, for an arbitrary first-order model $\mathfrak{A}$, its *ultrafilter extension* $\boldsymbol{\beta}\mathfrak{A}$ ([8, 9]), generalizing the well-known construction of ultrafilter extensions of semigroups comprehensively treated in [6]. (Some historical remarks can be found in [7].)

If $n < \omega$, the relations R_n can be redefined in terms of ultrafilter extensions of n-ary operations on ω as follows: $\mathfrak{u}\, R_n\, \mathfrak{v}$ iff there exists $f : \omega^n \to \omega$ such that $\widetilde{f}(\mathfrak{v}, \dots, \mathfrak{v}) = \mathfrak{u}$. Moreover, $R_m \circ R_n = R_{nm}$ (so R_n are not preorders for $2 \leq n < \omega$). These observations can be expanded to all R_α by using ω-ary operations on ω. Such an operation is identified with a continuous map of the Baire space ω^ω into the discrete space ω; these maps admit a natural hierarchy ranked by countable ordinals.

Proposition 1. *Any continuous $f : \omega^\omega \to \omega$ uniquely extends to $\widetilde{f} : (\boldsymbol{\beta}\omega)^\omega \to \boldsymbol{\beta}\omega$ that is right-continuous w.r.t. ω (in other words, ω-ary operations on ω extend to such operations on $\boldsymbol{\beta}\omega$).*

Proposition 2. *Let $\alpha < \omega_1$ and $\mathfrak{u}, \mathfrak{v} \in \boldsymbol{\beta}\omega$. Then $\mathfrak{u}\, R_\alpha\, \mathfrak{v}$ iff there exists a continuous $f : \omega^\omega \to \omega$ of rank α such that $\widetilde{f}(\mathfrak{v}, \mathfrak{v}, \dots) = \mathfrak{u}$.*

The composition of arbitrary $R_{<\alpha}$ is expressed via a multiplication-like operation on ordinals. To simplify notation, denote $\sup_{\gamma<\alpha}(\gamma \cdot \beta)$ by $(<\alpha) \cdot \beta$; the explicit calculation of these ordinals, used in getting the following result, is rather cumbersome.

Theorem 2. *Let $\alpha, \beta < \omega_1$.*

(i) $R_\alpha \circ R_\beta = R_\gamma$ *where* $\gamma = \beta \cdot \alpha$ *if* $\beta = 0$ *or* $\alpha < \omega$, $\gamma = \beta \cdot (\alpha + 1) - 1$ *if* $0 < \beta < \omega$ *and* $\alpha \geq \omega$, *and* $\gamma = \beta \cdot (\alpha + 1)$ *if* $\alpha, \beta \geq \omega$;

(ii) If $\alpha > 0$ *is limit, then* $R_{<\alpha} \circ R_\beta = R_{<\gamma}$ *where* $\gamma = \beta \cdot \alpha$;

(iii) If $\beta > 0$ *is limit, then* $R_\alpha \circ R_{<\beta} = R_{<\gamma}$ *where* $\gamma = (<\beta) \cdot \alpha$ *if* $\alpha < \omega$, *and* $\gamma = (<\beta) \cdot (\alpha + 1)$ *otherwise;*

(iv) If $\alpha, \beta > 0$ *are limit, then* $R_{<\alpha} \circ R_{<\beta} = R_{<\gamma}$ *where* $\gamma = (<\beta) \cdot \alpha$.

Corollary 1. *Let* $2 \leq \alpha \leq \omega_1$. *Then* $R_{<\alpha}$ *is a preorder iff* α *is multiplicatively indecomposable.*

Define preorders between $\leq_{\mathrm{RK}}$ and $\leq_{\mathrm{C}}$ by letting $\leq_0 = \leq_{\mathrm{RK}}$ and $\leq_{1+\alpha} = R_{<\omega^{\omega^\alpha}}$ for all $\alpha \leq \omega_1$. So, if α is infinite, $R_{<\alpha} = \leq_\alpha$ iff α is an epsilon number. Also $\leq_\alpha \circ \leq_\beta = \leq_\gamma$ where $\gamma = \max(\alpha, \beta)$.

Let us now consider two applications in model theory. The first concerns ultrafilter extensions. As shown in [5], for any ultrafilter $\mathfrak{v}$ and semigroup S, the set $\{\mathfrak{u} : \mathfrak{u} \leq_{\mathrm{C}} \mathfrak{v}\}$ forms a subsemigroup of $\boldsymbol{\beta}S$. This can be expanded to arbitrary first-order models and relations $R_{<\alpha}$ as follows.

Corollary 2. *For all ordinals* $\alpha > 1$, *ultrafilters* $\mathfrak{v}$, *and models* $\mathfrak{A}$, *the following are equivalent:*

(i) $\{\mathfrak{u} : \mathfrak{u}\, R_{<\alpha}\, \mathfrak{v}\}$ *forms a submodel of the model* $\boldsymbol{\beta}\mathfrak{A}$;

(ii) α *is additively indecomposable.*

Consequently, for all $\alpha > 0$, $\mathfrak{v}$, *and* $\mathfrak{A}$, $\{\mathfrak{u} : \mathfrak{u} \leq_\alpha \mathfrak{v}\}$ *forms a submodel of* $\boldsymbol{\beta}\mathfrak{A}$.

The second application concerns ultrapowers. For a model $\mathfrak{A}$ with the universe A, a set I, an ultrafilter $\mathfrak{u}$ over I, and $f : I \to A$, let $f_\mathfrak{u}$ denote the $\mathfrak{u}$-equivalence class of f, and $\prod_\mathfrak{u} \mathfrak{A}$ the ultrapower of $\mathfrak{A}$ by $\mathfrak{u}$. As shown in [1], the Rudin–Keisler preorder has a natural characterization in terms of ultrapowers: $\mathfrak{u} \leq_{\mathrm{RK}} \mathfrak{v}$ iff $\prod_\mathfrak{u} \mathfrak{A} \preceq \prod_\mathfrak{v} \mathfrak{A}$ for all models $\mathfrak{A}$, and also iff $\prod_\mathfrak{u} \mathfrak{N} \preceq \prod_\mathfrak{v} \mathfrak{N}$ where $\mathfrak{N}$ is the *full model of* ω, i.e., it has the universe ω and all relations and operations on ω.

It is not difficult to characterize R_n with $n < \omega$ via ultrapowers in a similar manner:

Proposition 3. *For all* $\mathfrak{u}, \mathfrak{v}$, *and* $n < \omega$, *the following are equivalent:*

(i) $\mathfrak{u}\, R_n\, \mathfrak{v}$;

(ii) $\prod_\mathfrak{u} \mathfrak{A} \preceq \prod_\mathfrak{v} \ldots \prod_\mathfrak{v} \mathfrak{A}$ *(n times) for all models* $\mathfrak{A}$;

(iii) $\prod_\mathfrak{u} \mathfrak{N} \preceq \prod_\mathfrak{v} \ldots \prod_\mathfrak{v} \mathfrak{N}$ *(n times).*

To handle the case $\alpha \geq \omega$, the following "skew version" of limit ultrapowers is used. First for any $e : A \to B$ define $e^\mathfrak{u} : \prod_\mathfrak{u} A \to \prod_\mathfrak{u} B$ by letting $e^\mathfrak{u}(g_\mathfrak{u}) := (e \circ g)_\mathfrak{u}$. Clearly, $e : \mathfrak{A} \preceq \mathfrak{B}$ implies $e^\mathfrak{u} : \prod_\mathfrak{u} \mathfrak{A} \preceq \prod_\mathfrak{u} \mathfrak{B}$. Then for every model $\mathfrak{A}$, ultrafilter $\mathfrak{u}$, and ordinals α, define the models $\mathfrak{A}_{\mathfrak{u},\alpha}$ and their embeddings $e_{\beta\alpha}$ for $\beta < \alpha$:

(i) $\mathfrak{A}_{\mathfrak{u},0} := \mathfrak{A}$, $\mathfrak{A}_{\mathfrak{u},1} := \prod_\mathfrak{u} \mathfrak{A}$, and $e_{01} = d$ (the diagonal map);

(ii) if α is limit, then $\mathfrak{A}_{\mathfrak{u},\alpha} := \lim_{\beta\to\alpha}\mathfrak{A}_{\mathfrak{u},\beta}$ w.r.t. the system $\{e_{\gamma\beta}\}_{\gamma<\beta<\alpha}$, and the maps $e_{\beta\alpha}$ $(\beta<\alpha)$ are defined naturally;

(iii) if $\alpha=\beta+1$, then $\mathfrak{A}_{\mathfrak{u},\alpha} := \prod_{\mathfrak{u}}\mathfrak{A}_{\mathfrak{u},\beta}$, and the maps $e_{\delta\alpha}$ $(\delta<\alpha)$ are defined as follows:

(a) if $\beta=\gamma+1$, then $e_{\beta\alpha} := e^{\mathfrak{u}}_{\gamma\beta}$;

(b) if $\beta>0$ is limit, then for any $g\in A_{\mathfrak{u},\beta}$

$$\theta_{\beta\alpha}(g) := \theta^{\mathfrak{u}}_{\gamma\beta}(h)$$

for some $\gamma<\beta$ and $h\in g\cap A_{\mathfrak{u},\gamma+1}$;

(c) for any $\delta<\beta$, $e_{\delta\alpha} := e_{\beta\alpha}\circ e_{\delta\beta}$.

Lemma 1. *All $\mathfrak{A}_{\mathfrak{u},\alpha}$ are well defined, and if $\beta<\alpha$ then $e_{\beta\alpha}:\mathfrak{A}_{\mathfrak{u},\beta}\preceq\mathfrak{A}_{\mathfrak{u},\alpha}$.*

Theorem 1. *For $\mathfrak{u},\mathfrak{v}\in\boldsymbol{\beta}\omega$, and a limit ordinal $\alpha>0$, the following are equivalent:*

(i) $\mathfrak{u}\,R_{<\alpha}\,\mathfrak{v}$;

(ii) there is $\beta<\alpha$ such that $\mathfrak{A}_{\mathfrak{u},1}\preceq\mathfrak{A}_{\mathfrak{v},\beta}$ for all models $\mathfrak{A}$;

(iii) there is $\beta<\alpha$ such that $\mathfrak{N}_{\mathfrak{u},1}\preceq\mathfrak{N}_{\mathfrak{v},\beta}$.

Consequently, $\mathfrak{u}\leq_{\mathrm{C}}\mathfrak{v}$ iff $\mathfrak{A}_{\mathfrak{u},1}\preceq\mathfrak{A}_{\mathfrak{v},\omega_1}$ for all models $\mathfrak{A}$, and also iff $\mathfrak{N}_{\mathfrak{u},1}\preceq\mathfrak{N}_{\mathfrak{v},\omega_1}$.

References

[1] A. R. Blass, *Orderings on ultrafilters*, PhD Thesis, Harward University, Cambridge, Mass., 1970.

[2] W. W. Comfort, S. Negrepontis, *The theory of ultrafilters*, Grundlehren math. Wiss., 211, Springer, 1974.

[3] S. García-Ferreira, Three orderings on $(\omega)\setminus\omega$, *Top. Appl.*, 50 (1993), 119–216.

[4] S. García-Ferreira, "Comfort types of ultrafilters", *Proc. Amer. Math. Soc.*, 120 (1994), 1251–1260.

[5] S. García-Ferreira, N. Hindman, D. Strauss, "Orderings of the Stone–Cech remainder of a discrete semigroup", *Top. Appl.*, 97:1–2 (1999), 127–148.

[6] N. Hindman, D. Strauss, *Algebra in the Stone–Cech Compactification: Theory and Applications*, sec. rev. and ext. ed., De Gruyter, 2012.

[7] N.L. Poliakov, D.I. Saveliev, "On ultrafilter extensions of first-order models and ultrafilter interpretations", *Arch. Math. Log.*, 60 (2021), 625–681.

[8] D.I. Saveliev, "Ultrafilter extensions of models", *Log. Appl., Lect. Notes Comp. Sci.*, Springer, 2011, 162–177.

[9] D.I. Saveliev, "On ultrafilter extensions of models", *The Infinity Project Proc.*, CRM Documents, 11, S.-D. Friedman et al. (eds.), 2012, 599–616.

Graphons, hypergraphons, and generic sampling

Kyle Gannon

Peking University

E-mail: kgannon@bicmr.pku.edu.cn

Abstract

Intuitively, generic sampling is a method for sampling types over monster models of a first-order theory with respect to a Keisler measure. In practice, this involves studying countably iterated Morley products of relatively tame Keisler measures. Given such a measure, one can straightforwardly derive a corresponding Borel measure on the space of L-structures over the natural numbers. In particular, if the original monster model is a graph (respectively, a hypergraph), then generic sampling yields measures on the space of all graphs (respectively, hypergraphs) on the natural numbers.

A graphon is a symmetric measurable map from $[0,1]^2$ to $[0,1]$. These graph-like objects also give rise to a notion of sampling. It turns out that all Sym(N)-invariant measures on the space of graphs (over the natural numbers) are mixtures of sampling procedures arising from graphons. We remark that graphons admit a higher-arity generalization to hypergraphs, called hypergraphons, which exhibit a similar property.

We prove a representation theorem: (hyper)graphon sampling can be encoded within the framework of generic sampling. We remark that generic sampling in practice can give rise to non-Sym(N)-invariant measures and so generic sampling is strictly more general than what arises from (hyper)graphons. This is joint work with Nathanael Ackerman, Cameron Freer, James Hanson, and Rehana Patel.

On Definable Groups in Omega-Free PAC Fields

Yvon Bossut

ICJ-Université Claude Bernard Lyon1

E-mail: bossut@math.univ-lyon1.fr

Abstract

PAC fields have long been studied by model theorists. Hrushovsky showed that any group definable in an e-free PAC field (for finite e) is definably isogenous to the rational points of an algebraic group. Chatzidakis and Ramsey also defined a measure on definable subsets of an irreducible variety in e-free PAC fields. Using Hrushovsky's result, they deduced that groups definable in e-free PAC fields are definably amenable. Omega-free PAC fields can be obtained as non-principal ultraproducts of e-free PAC fields; therefore, groups definable in omega-free PAC fields are also definably amenable. A natural question is whether these groups are also definably isogenous to the rational points of an algebraic group. In this talk, I will present a result that partially answers this question.

Lie rings in finite dimensional theories

Moreno Invitti

ICJ-Université Claude Bernard Lyon1

E-mail: invitti@math.univ-lyon1.fr

Abstract

Lie rings are algebraic structures that have recently attracted attention in model theory, following the work of Deloro and Ntsiri. A Lie ring g is an abelian group equipped with a bilinear map [,] that is antisymmetric and satisfies the Jacobi identity. A natural question in this context is an analogue of the Algebraicity Conjecture for Lie rings: if g is a simple Lie ring of finite Morley rank, then is g definably isomorphic to a Lie algebra over an algebraically closed field? Although the conjecture remains open, Deloro and Ntsiri have classified simple connected Lie rings of Morley rank up to 4. Finite-dimensional theories, introduced by Frank Wagner, are a generalization of theories of finite Morley rank and so provide a broader context in which to study this question. Therefore one may ask whether the results known for Lie rings of finite Morley rank extend to finite-dimensional Lie rings. While the general case remains unresolved, we show that such extensions hold for connected finite-dimensional Lie rings and for NIP finite dimensional Lie rings. Specifically, a connected Lie ring of dimension 1 is abelian; of dimension 2, it is solvable; and of dimension 3, it is either isomorphic to sl2(K) for a definable field K of dimension 1, or it is "bad." In the NIP setting, a Lie ring of dimension 1 is virtually abelian; of dimension 2, virtually solvable; and of dimension 3, virtually connected. In the latter case, we obtain a full classification using the results established for connected finite-dimensional Lie rings.

On pure orderings of Morley o-rank 1

V.V. Verbovskiy, A.D. Yershigeshova

Insitute of mathematics and mathematical modeling

E-mail: verbovskiy@math.kz

Abstract

Pure linear ordering and its classification are one of the classical mathematical questions. Descriptions of o-minimal and weakly o-minimal pure linear orderings are known, as well as we know that any pure linear ordering has an o-superstable elementary theory. The aim of this paper is to start investigation of pure linear ordering that have o-ω-stable elementary theory. So, we give the complete description of pure linear ordering of Morley o-rank 1.

Definition 1 (V. Verbovskiy, 2010)

1. *We say that Morley o-rank of a formula $\phi(x)$ inside a cut $\langle C, D\rangle$ in $\mathcal{M}$ is equal to or greater than 1 and write $o\text{-}RM_{\langle C,D\rangle,\mathcal{M}}(\phi) \geq 1$ for this, if $\{\phi(x)\} \cup \langle C, D\rangle$ is consistent.*

2. *$o\text{-}RM_{\langle C,D\rangle,\mathcal{M}}(\phi) \geq \alpha + 1$ if there are infinitely many pairwise $\langle C, D\rangle$-inconsistent formulae $\psi_i(x)$ such that $RM_{\langle C,D\rangle,\mathcal{M}}\big(\phi(x) \wedge \psi_i(x)\big) \geq \alpha$.*

3. *If α is a limit ordinal, then $o\text{-}RM_{\langle C,D\rangle,\mathcal{M}}(\phi) \geq \alpha$ if $o\text{-}RM_{\langle C,D\rangle,\mathcal{M}}(\phi) \geq \beta$ for all $\beta < \alpha$.*

4. *$o\text{-}RM_{\langle C,D\rangle,\mathcal{M}}(\phi) = \alpha$ if $o\text{-}RM_{\langle C,D\rangle,\mathcal{M}}(\phi) \geq \alpha$ and $o\text{-}RM_{\langle C,D\rangle,\mathcal{M}}(\phi) \ngeq \alpha + 1$.*

5. *We define Morley o-rank of a formula $\phi(x)$ inside $\mathcal{M}$ as follows:*

$$o\text{-}RM_{\mathcal{M}}(\phi) = \sup\{o\text{-}RM_{\langle C,D\rangle,\mathcal{M}}(\phi) : \langle C, D\rangle \text{ is a cut in } \mathcal{M}\}.$$

6. *We define Morley o-rank of a formula $\phi(x)$ as follows:*

$$o\text{-}RM(\phi) = \sup\{o\text{-}RM_{\langle C,D\rangle,\mathcal{M}}(\phi) : \mathcal{M} \models T \text{ and } \langle C, D\rangle \text{ is a cut in } \mathcal{M}\}.$$

Similarly, we can define the Morley o-degree of a formula inside a cut.
Let F be the set of all finite linear orderings, and

$$G = F \cup \{\omega, \omega^*, \omega + \omega^*, \omega^* + \omega, \mathbb{Q}\}$$

Also, let WO be the collection of all ordered sums of the form $C_1 + \cdots + C_m$, where C_i is elementarily equivalent to some member of G for each $i \leq m$.

Theorem 1. *Any totally ordered structure $\mathcal{M}$, whose elementary theory has Morley o-rank 1 and Morley o-degree 2, restricted to the signature $\{=, <\}$ is a member of $\mathcal{O}_{1,2}$, and conversely, the first-order theory of any infinite member of $\mathcal{O}_{1,2}$ has Morley o-rank 1 and Morley o-degree at most 2.*

Let $\mathcal{M}$ be an ordered structure and $F(x)$ a formula. We define the *convex hull* F^c of F as:

$$F^c(x) = \exists y \exists z (F(y) \wedge F(z) \wedge y \leq x \leq z)$$

Let p be a 1-type. We define the *convex hull* p^c of p as the following partial type:

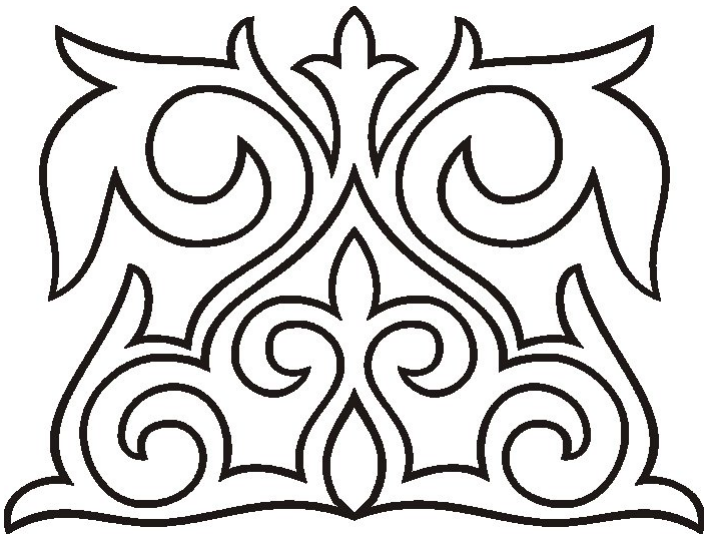
$$p^c(x) = \{F^c(x) \mid F(x) \in p(x)\}$$

Similarly, we can define Morley c-rank $RM_{p^c,\mathcal{M}}(\phi(x))$ and c-degree, replacing a cut with a convex type.

Let us define $\mathcal{C}_{1,2}$ as the set of all finite ordered sums of the form $C_1 + ... + C_m$, where each C_i is elementarily equivalent to some element of $G_{1,2}$.

Theorem 2. *c-$RM(\mathcal{M}) = 1$ and c-$DM(\mathcal{M}) \leq 2$ if and only if $\mathcal{M} \equiv \mathcal{N}$ for some $\mathcal{N} \in \mathcal{C}_{1,2}$.*

MODEL THEORY



Characterization of strongly minimal partial orderings with infinite non-trivial width

YE.K. NETALIYEVA, B.SH. KULPESHOV

Insititute of Mathematics and Mathematical Modeling, Kazakh-British Technical University

Email address: e netalieva@kbtu.kz, b.kulpeshov@kbtu.kz

Abstract

In the present lecture, we study strongly minimal partial orderings in the signature containing only the symbol of binary relation for a partial order. We use for partial orderings such characteristics as the height of a structure that is the supremum of lengths of ordered chains, and the width of a structure that is the supremum of lengths of antichains, where an antichain is the set of pairwise incomparable elements. We also differ trivial width and non-trivial width. Recently in [1], B.Sh. Kulpeshov, In.I. Pavlyuk and S.V. Sudoplatov described strongly minimal partial orderings having a finite non-trivial width. Here we study strongly minimal partial orderings having an infinite non-trivial width.

Recall [2] that an infinite structure $\mathcal{M}$ is said to be *minimal* if for any formula $\varphi(x, \overline{a})$ of the language of $\mathcal{M}$, with parameters $\overline{a}$, either $\varphi(\mathcal{M}, \overline{a})$ or $\neg\varphi(\mathcal{M}, \overline{a})$ is finite. A theory T without finite models is said to be *strongly minimal* if any model $\mathcal{M} \models T$ is minimal. Models of a strongly minimal theory are said to be *strongly minimal*, too.

Recall that a *partial order* on a set is a binary relation $<$ satisfying:

Asymmetry $\forall x \forall y[x < y \rightarrow \neg(y < x)]$;

Transitivity $\forall x \forall y \forall z[(x < y \wedge y < z) \rightarrow x < z]$.

A set equipped with a partial order on it is said to be a *partially ordered set* or *partial ordering*.

Let $\mathcal{M} = \langle M, < \rangle$ be an infinite partial ordering. Assuming that $\mathcal{M}$ is strongly minimal we have only finite $\leq$-chains and the lengths of these chains are bounded, since unbounded lengths imply existence of structures $\mathcal{N} \equiv \mathcal{M}$ with infinite chains $\{a_i \mid i \in \mathbb{Z}\}$, $a_i < a_j$ for $i < j$, that violate the strong minimality by any formula $x < a_i$. Thus, the *height* $h(\mathcal{M})$, that is the supremum of lengths of $\leq$-chains in $\mathcal{M}$, must be finite for a strongly minimal structure $\mathcal{M}$. Therefore, further we consider here only infinite partial orderings with finite $\leq$-chains.

Also, since $\mathcal{M}$ is infinite, it has an infinite *width* $w(\mathcal{M})$ that is the supremum of cardinalities of $\leq$-antichains.

We say a connected component is *trivial* if it is a chain. We say a trivial connected component is an *n-component* if it is a chain of length n, where $1 \leq n < \omega$. We say a 1-component is a *singleton*.

The value $w(\mathcal{M})$ is witnessed by both trivial connected components and collections of maximal antichains in non-trivial connected components. Indeed, let $\mathcal{M}$ consist of both $\bigsqcup_{i \in I} \mathcal{A}_i$ and $\bigsqcup_{j \in J} \mathcal{B}_j$, where each $\mathcal{A}_i$ is a trivial connected component, and each $\mathcal{B}_j$ is a non-trivial connected component. Then obviously $w(\mathcal{M}) = w_0(\mathcal{M}) + w_1(\mathcal{M})$, where $w_0(\mathcal{M})$ is the width of trivial part $\bigsqcup_{i \in I} \mathcal{A}_i$ (trivial width) and $w_1(\mathcal{M})$ is the width of non-trivial part $\bigsqcup_{j \in J} \mathcal{B}_j$ (non-trivial width).

The following theorem describes strongly minimal partial orderings with finite non-trivial width:

Theorem 1. [1] An infinite partial ordering $\mathcal{M} = \langle M, < \rangle$ with finite non-trivial width is strongly minimal iff $\mathcal{M}$ has infinitely many singletons and additionally can have only finitely many finite connected components which are not singletons.

Recall that an element a of a partial ordering $\mathcal{M}$ is said to be *minimal* if there is no element in $\mathcal{M}$ that is less than a. Also, an element a of a partial ordering $\mathcal{M}$ is said to be *maximal* if there is no element in $\mathcal{M}$ that is greater than a. Observe that any singleton of a partial ordering is both maximal and minimal element of the ordering. Also, any maximal (minimal) element of a non-trivial connected component of a partial ordering is not minimal (maximal).

Example 1. Let $\mathcal{M} = \langle M, < \rangle$ be a partial ordering consisting of exactly one infinite non-trivial connected component of height two having exactly one maximal element. Then, obviously, $\mathcal{M}$ contains infinitely many minimal elements. Then $\mathcal{M}$ is a strongly minimal structure having an infinite non-trivial width.

We say that an element a of a partial ordering $\mathcal{M}$ has *up-degree* (*down-degree*) m for some $m \in \omega$ if there exist exactly m elements of $\mathcal{M}$ being an immediate successor (predecessor) of a. If there are infinitely many elements of $\mathcal{M}$ being an immediate successor (predecessor) of a then we say a has infinite up-degree (down-degree). Obviously, a has both up-degree 0 and down-degree 0 iff a is a singleton.

The following theorem is a criterion for strong minimality of an infinite partial ordering of height two having an infinite non-trivial width.

Theorem 2. Let $\mathcal{M} = \langle M, < \rangle$ be an infinite partial ordering of height two having an infinite non-trivial width. Then $\mathcal{M}$ is strongly minimal iff the following holds:

(1) $\mathcal{M}$ contains exactly one non-trivial connected component of height two having both an infinite set of maximal (minimal) elements and a non-empty finite set of minimal (maximal) elements;

(2) If $\mathcal{M}$ contains exactly m minimal (maximal) elements of infinite up-degree (down-degree) for some $1 \leq m < \omega$ then almost all maximal (minimal) elements have down-degree (up-degree) m;

(3) $\mathcal{M}$ contains only finitely many finite connected components of height at most two.

Recall that a first-order theory is said to be *totally categorical* if it has exactly one model in each infinite power.

Corollary 1. Any strongly minimal partial ordering of height two with an infinite non-trivial width is totally categorical.

Acknowledgements. *The authors were supported by Science Committee of Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. BR20281002).*

References

[1] Kulpeshov B.Sh., Pavlyuk In.I., Sudoplatov S.V., *Pseudo-strongly-minimal structures and theories, Lobachevskii Journal of Mathematics, 45*(12), (2024), 6515–6525.

[2] Baldwin J.T., Lachlan A.H., *On strongly minimal sets, The Journal of Symbolic Logic, 36*(1), (1971), 79–96.

On K_T-normal Jonsson theories

AIBAT YESHKEYEV AND INDIRA TUNGUSHBAYEVA

Karaganda Buketov University

E-mail: yeshkeyev a@buketov.edu.kz, tungushbayeva_i_1@buketov.edu.kz

Abstract

We study the specific subclass of inductive theories in a countable first-order language L, namely, Jonsson theories [1]. A theory T is called Jonsson, if it has an infinite model, is inductive, admits AP and JEP. T.G. Mustafin introduced the notion of semantic model of a Jonsson theory, which plays a role of the semantic invariant of the theory [2]. A.R. Yeshkeyev proposed a new concept of the semantic invariant for a Jonsson theory, which is called the Kaiser class:

Definition. Let T be an L-theory. A class K_T of L-structures is called a Kaiser class of T if

$$K_T = \{M \mid M \in Mod(T) \text{ and } Th_{\forall\exists}(M) \text{ is a Jonsson theory}\}.$$

The following definition provides an equivalence relation, which allows us to compare L-theories by their Kaiser classes:

Definition. Let T_1 and T_2 be Jonsson L-theories. T_1 and T_2 are called K_T-equivalent ($T_1 \widetilde{\bowtie} T_2$), if $K_{T_1} = K_{T_2}$.

The following definition was introduced by A.R. Yeshkeyev.

Definition. Let T be a Jonsson theory. T is called K_T-normal, if for any model $M \in K_T$, C_{M^0} is an existentially closed submodel of C_T.

The result of this research is the following criterion of normality of a Jonsson theory.

Theorem 1. *Let T be a Jonsson theory. The following conditions are equivalent:*

1. *T is K_T-normal;*
2. *for any model M of K_T, $M^0 \bowtie T$;*
3. *K_T^0 is an $\exists$-complete theory;*
4. *$K_T = \{M \mid M$ is $\forall$-elementary equivalent to N, where $N \in E_T\}$, where E_T is the class of all existentially closed models of T;*
5. *$K_T^0 = T \cup \Sigma(T)$, where $\Sigma(T)$ is a set of all existential L-sentences that are consistent with T;*
6. *$T \widetilde{\bowtie} T \cup \Sigma(T)$, where $\Sigma(T)$ is as in (5);*
7. *for any Jonsson theory $T' \supseteq T$, T and T' are cosemantic.*

Corollary 2. *Any $\exists$-complete Jonsson theory is K_T-normal.*

Acknowledgements. *This research has been funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP23489523)*

References

[1] Barwise, J., *Teoriya modelei: spravochnaia kniga po matematicheskoi logike. Chast 1 [Model theory: Handbook of mathematical logic. Part 1]*, *Izdatelstvo Nauka*, Moscow, 1982 [in Russian].

[2] Yeshkeyev, A.R., *Teorii i ih modeli. Tom 1: monografiia [Theories and their models. Volume 2]*, *Izdatelstvo Karagandinskogo universiteta*, Karaganda, 2024 [in Russian].

Countable categoricity of hybrids

Mussina N.M., Amanbekov S.M.

Karaganda Buketov university, Karaganda, Kazakhstan

E-mail: mussinanazerke@gmail.com, amanbekovsmath@gmail.com

Abstract

We work within the framework of studying Jonsson theories [1]. Let T be a Jonsson L-theory, and $\mathfrak{C}_T$ be a semantic model of the theory T. The center of a Jonsson theory T is defined as the elementary theory of the semantic model of this theory: $T^* = Th(\mathfrak{C}_T)$.

The following definition gives us important notion of Jonsson spectrum, the details of this one can extract from [1].

Definition 1. [1] Let K be a class of L-structures. The Jonsson spectrum of K, denoted $JSp(K)$, is defined as the set of all theories satisfying the following conditions:

$JSp(K)$=$\{T|T$ is a Jonsson theory and $\forall A \in K, A \models T\}$.

The following definition is an essential generalization of the concept of a Jonsson set.

Definition 2. [2] A set X is called an almost Jonsson if it satisfies the following conditions:

1) X is a definable subset of $\mathfrak{C}_T$;

2) $cl(X) = \mathfrak{M} \in Mod(T)$.

Furthermore, the sets of all $\forall\exists$-sentences in the language that are true in the model $\mathfrak{M}$, denoted by $Th_{\forall\exists}(\mathfrak{M}) = \mathfrak{M}^0 = Fr(X)$, and $\mathfrak{M}^0 \in JSp(\mathfrak{C}_T)$, where $cl(X)$ is the definable closure of the set X in the frame of given above pregeometry.

The concept of cl-normality for a Jonsson theory is defined for a class of theories where any fragment of their semantic models, denoted by $Fr(X)$, belongs to the Jonsson spectrum of the given Jonsson theory's semantic model.

The following definition identifies specific subsets within the semantic model of the given Jonsson theory.

Definition 3. [2] The Jonsson theory T is said to be cl-normal if, for any $X \subseteq \mathfrak{C}_T$ such that $cl(X) = \mathfrak{M} \in Mod(T)$, $Fr(X) = \mathfrak{M}^0 \in JSp(\mathfrak{C}_T)$ and $\mathfrak{C}_{\mathfrak{M}^0} \preceq_{\exists_1} \mathfrak{C}_T$, where $\mathfrak{C}_{\mathfrak{M}^0}$ is a semantic model of $\mathfrak{M}^0$.

And now let us define the concept of the Kaiser class of models for the arbitrary of the Jonsson theory, denoted by K_T [3].

$K_T = \{\mathfrak{A} \in ModT|Th_{\forall\exists}(\mathfrak{A})$ is a Jonsson theory$\}$.

It is clear that $E_T \subseteq K_T$, where E_T denotes the class of existentially closed models of the theory T.

Next, we can consider the binary relation according to the Kaiser classes of two Jonsson theories T_1 and T_2.

Definition 4. [4] Let T_1 and T_2 are Jonsson theories. We say that theories T_1 and T_2 are K_T-equivalent, if K_{T_1}=K_{T_2}.

The Jonsson sets and almost Jonsson sets generate fragments in the case of cl-normality of considered Jonsson theory from models of the Kaiser class of this theory, and these fragments semantic models are existentially closed submodels of semantic model of considered Jonsson theory.

Let us now turn to the notion of the semantic class of the Jonsson complex.

Let L be a countable first-order language, and let T be a cl-normal Jonsson theory in the language L, and let $L_0 \subseteq L$, where L_0 is the set of sentences of language L, with its semantic model denoted by $\mathfrak{C}_T$. K_T is the Kaiser class of the theory T. $N \subseteq K_T$. Let N form a quasivariety in the usual sense. Consider the elementary theory $Th(N)$ of this class N. By adding $\forall\exists$-sentences of language L, denoted as $\forall\exists(L_0)$ which are not contained in $Th(N)$, we can define the following set, denoted by $J\mathbb{T}$, which we will call the Jonsson complex of the class N.

Denotation 1. $J\mathbb{T} = \{\Delta | \Delta = Th(N) \cup \{\varphi_i\}$, where Δ is a Jonsson theory, φ_i denotes either a formula from $\forall\exists(L_0)$, or its negation, $i \in \{0, 1\}$, and $Th(N)$ is elementary theory of class of quasivariety N.

Every theory $\Delta \in J\mathbb{T}$ is associated with a semantic model, denoted $\mathfrak{C}_\Delta$. We now define the set all such models:

Denotation 2. $\mathbb{C}_\mathbb{T} = \{\mathfrak{C}_\Delta | \Delta \in J\mathbb{T}, \mathfrak{C}_\Delta$ is a semantic model of $\Delta\}$.

We will call the set $\mathbb{C}_\mathbb{T}$ semantic class of Jonsson complex $J\mathbb{T}$ if its elementary theory $Th(\mathbb{C}_\mathbb{T})$ is a Jonsson theory.

Now, let us move on to the main results of this abstract.

Let $\mathbb{C}_\mathbb{T}$ be semantic class of Jonsson complex $J\mathbb{T}$. $JSp(\mathbb{C}_\mathbb{T})$ be its Jonsson spectrum.

Further, on this spectrum, we introduce the following relations:

1) equivalence of Jonsson syntactic and semantic similarity,

2) K_T-equivalent, and

3) cosemanticness relations.

It is obvious that all these relations are equivalence relations, so we obtain a factor-set of the Jonsson spectrum of $\mathbb{C}_\mathbb{T}$ with respect to the introduced relations, which we call triple factorization and denote as $JSp(\mathbb{C}_\mathbb{T})_{/\bigtriangleup\limits_K^{SS}}$. $[\dddot{\Delta}]$ is an equivalence class of a theory Δ from $JSp(\mathbb{C}_\mathbb{T})_{/\bigtriangleup\limits_K^{SS}}$.

Theorem 1. Let $[\dddot{\Delta}_1]$ and $[\dddot{\Delta}_2]$ be classes of ω-categorical Jonsson theories. Then their hybrid $H([\dddot{\Delta}_1], [\dddot{\Delta}_2])$ is also a ω-categorical Jonsson theory.

All definitions that were not given in the abstract can be found in [1].

Acknowledgements. *This research has been funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP22686796 Hybrids of fragments and their small models).*

References

[1] A.R. Yeshkeyev, *Theories and their models: a monograph in 2 volumes*, *KBU Publishing House, Karaganda*, 2024.

[2] A.R. Yeshkeyev, O.I. Ulbrikht, M.T. Omarova, Double factorization of the Jonsson spectrum, Bulletin of the Karaganda University. Mathematics Series, 116(4) (2024), 185–196. https://doi.org/10.31489/2024M4/185-196

[3] A.R. Yeshkeyev, M.T. Kassymetova, N.M. Mussina, Normal Jonsson theories and their Kaiser classes, Bulletin of the Karaganda University. Mathematics Series, 117(1) (2025), 199–210. https://doi.org/10.31489/2025M1/199-210

[4] A.R. Yeshkeyev, I.O. Tungushbayeva, M.T. Kassymetova, On the Kaiser Class of a Jonsson Theory, Symmetry. – Basel, 17(6), (2025), 870(1-25). https://doi.org/10.3390/sym17060870

ON JONSSON SPECTRUM OF UNARS IN EXPANDED SIGNATURE

Yeshkeyev A.R., Yarullina A.R., Kassymetova M.T.

Karaganda Buketov University, Karaganda, Kazakhstan

E-mail: aibat.kz@gmail.com, linka14221@mail.ru, mairushaasd@mail.ru

Abstract

Let K be a class of models of fixed signature σ.

Definition 1. [1] *A set $JSp(K)$ of Jonsson theories of signature σ, where $JSp(K) = \{\Delta \mid \Delta$ is a Jonsson theory and $K \subseteq Mod(\Delta)\}$, is called the Jonsson spectrum for class K.*

Definition 2. [2] *Let T be a Jonsson theory. A class of models $K_T \subseteq Mod(T)$ such that $K_T = \{\mathfrak{A} \mid \mathfrak{A} \in Mod(T)$ and $Th_{\forall\exists}(\mathfrak{A})$ is a Jonsson theory $\}$ is called a Kaiser class of the theory T.*

Definition 3. [2] *Let T_1 and T_2 be Jonsson theories of the considered language L. T_1 and T_2 are called K_T-equivalent if $K_{T_1} = K_{T_2}$.*

Definition 4. [1] *Let T_1 and T_2 be Jonsson theories, $\mathfrak{C}_{T_1}$ and $\mathfrak{C}_{T_2}$ be their semantic models, respectively. T_1 and T_2 are said to be cosemantic Jonsson theories (denoted by $T_1 \bowtie T_2$), if $\mathfrak{C}_{T_1} = \mathfrak{C}_{T_2}$.*

We can consider the cosemanticness relation on $JSp(K)$ and get a factor-set, denoted as $JSp(K)_{/\bowtie}$. We introduce the K_T-equivalent relation on the factor-set and obtain its double factorization denoted as $JSp(K)_{/\underset{K_T}{\bowtie}}$.

Let T be a *cl*-normal Jonsson theory [2] in the countable first-order language L, $L_0 \subset L$, where L_0 is the set of all sentences of language L. Let K_T be the Kaiser class of the theory T and $N \subseteq K_T$. Let N form a quasivariety in the sense of [3]. We consider the elementary theory $Th(N)$ of such class N, by adding to $Th(N)$ such $\forall\exists$ sentences of language L that are not contained in the $Th(N)$. We can consider the set of Jonsson theories $J\mathbb{T}$ defined as follows.

Definition 5. *A set $J\mathbb{T} = \{\Delta \mid \Delta$ is a Jonsson theory, $\Delta = Th(N) \cup \{\varphi^i\}\}$, where $\varphi^i \in \forall\exists(L_0)$ and $\varphi^i \notin Th(N)$, $i = 0$ or $i = 1$ (i.e. it is a formula or its negation), $Th(N)$ is an elementary theory of class of quasivariety N, $\forall\exists(L_0)$ is a set of all $\forall\exists$ sentences of first-order language L.*

A set of Jonsson theories $J\mathbb{T}$ is called a Jonsson complex of the class N. Let us consider the set of semantic models of Δ and denote it as $\mathbb{C}_{\mathbb{T}}$.

Denotation 1. *A set $\mathbb{C}_{\mathbb{T}} = \{\mathfrak{C}_\Delta \mid \Delta \in J\mathbb{T}, \mathfrak{C}_\Delta$ is a semantic model of $\Delta\}$.*

We will call the set $\mathbb{C}_{\mathbb{T}}$ semantic class of Jonsson complex $J\mathbb{T}$ if its elementary theory $Th(\mathbb{C}_{\mathbb{T}})$ is a Jonsson theory.

Further we consider first-order language L of the signature $\sigma =< f >$, where f is a unary functional symbol and expand it by symbols of new constant c and unary predicate P^1. Let $\sigma'' = \sigma \cup \sigma'$, where $\sigma =< f >$, $\sigma' = (P^1, c)$. We consider a theory $\overline{T}_\forall$ in the new expanded signature σ'' as follows: [4] $\overline{T}_\forall = T_\forall \cup Th_\forall(\mathfrak{C}_{T_\forall}, a)_{a \in P^1(\mathfrak{C}_{T_\forall}) \cup P^1(c)} \cup \{P^1, \subseteq\} \cup P^1(c)$. Here P^1 is a new unary predicate symbol, $\{P^1, \subseteq\}$ is an infinite set of sentences such that

in the semantic model $\mathfrak{C}_{T_\forall}$ the predicate P^1 distinguishes existentially closed submodel of $\mathfrak{C}_{T_\forall}$, i.e. $P^1(\mathfrak{C}_{T_\forall}) = \mathfrak{M}, \mathfrak{M} \in K_{T_\forall}$, $Th_{\forall\exists}(\mathfrak{M})$ is a Jonsson theory, $K_{T_\forall}$ is a Kaiser class of theory $T_\forall$.

We consider a theory $\overline{T}_\nabla$ in the new expanded signature σ'' as follows: [4] $\overline{T}_\nabla = T_\nabla \cup Th_\nabla(\mathfrak{C}_{T_\nabla}, a)_{a \in P^1(\mathfrak{C}_{T_\nabla}) \cup P^1(c)} \cup \{P^1, \subseteq\} \cup P^1(c)$.

Here $\{P^1, \subseteq\}$ is an infinite set of sentences such that in the semantic model $\mathfrak{C}_{T_\nabla}$ of T_∇: $P^1(\mathfrak{C}_{T_\nabla}) = \mathfrak{M}, \mathfrak{M} \in K_{T_\nabla}$, $Th_{\forall\exists}(\mathfrak{M})$ is a Jonsson theory, K_{T_∇} is a a Kaiser class of theory T_∇. We denote the center of $\overline{T}_\nabla$ as follows: $\overline{T}^*_\nabla = Th(\overline{\mathfrak{C}}_{T_\nabla})$

Denotation 2. *A set $J\overline{\mathbb{T}} = \{\overline{\Delta} \mid \overline{\Delta}$ is a Jonsson primitive of unars, $\overline{\Delta} = Th(\overline{N}) \cup \{\varphi^i\}\}$, where $\varphi^i \in \forall\exists(\overline{L}_0)$ and $\varphi^i \notin Th(\overline{N})$, $i = 0$ or $i = 1$ (i.e. it is a formula or its negation), $Th(\overline{N})$ is an elementary theory of class of quasivariety of unars $\overline{N}$ in the new expanded signature σ'', $\forall\exists(\overline{L}_0)$ is a set of all $\forall\exists$ sentences of first-order language $\overline{L}$ of the signature σ''.*

Definition 6. *A set $\mathbb{C}_{\overline{\mathbb{T}}} = \{\overline{\mathfrak{C}}_\Delta \mid \Delta \in J\overline{\mathbb{T}}, \overline{\mathfrak{C}}_\Delta$ is a semantic model of $\overline{\Delta}\}$ is called a semantic class of Jonsson complex $J\overline{\mathbb{T}}$ in a signature σ'' if its elementary theory $Th(\mathbb{C}_{\overline{\mathbb{T}}})$ is a Jonsson theory.*

Definition 7. *A set $JSp(\mathbb{C}_{\overline{\mathbb{T}}})$ of Jonsson theories of signature σ'', where $JSp(\mathbb{C}_{\overline{\mathbb{T}}}) = \{\overline{T}_\nabla \mid \overline{T}_\nabla$ is a Jonsson primitive of unars and $\mathbb{C}_{\overline{\mathbb{T}}} \subseteq Mod(\overline{T}_\nabla)\}$, is called the Jonsson spectrum for class $\mathbb{C}_{\overline{\mathbb{T}}}$, where $\mathbb{C}_{\overline{\mathbb{T}}}$ is a semantic class of Jonsson complex $J\overline{\mathbb{T}}$ in a signature σ''.*

We introduce the double factorization on the set $JSp(\mathbb{C}_{\overline{\mathbb{T}}})$ and obtain such disjoint equivalence classes $[\overline{\overline{T}}_\nabla] \in JSp(\mathbb{C}_{\overline{\mathbb{T}}})_{/\underset{K_T}{\bowtie}}$. $[\overline{\overline{T}}_\nabla]$ is an equivalence class of Jonsson primitives of unars in the new expanded signature, containing theories that have coinciding centers, semantic models and Kaiser classes, as well as the class of models of such theories is equal to or contains semantic class $\mathbb{C}_{\overline{\mathbb{T}}}$ of Jonsson complex $J\overline{\mathbb{T}}$. Let $[\overline{\overline{T}}_\nabla]^*$ be the center of $[\overline{\overline{T}}_\nabla]$.

Theorem 1. *Let $[\overline{\overline{T}}_\nabla]$ be a double factorization class as defined above, and let $[\overline{\overline{T}}_\nabla]^*$ be its center. Then, $[\overline{\overline{T}}_\nabla]_\forall = [\overline{\overline{T}}_\nabla]^*_\forall$.*

All undefined concepts can be found in [1, 2, 5, 6].

Acknowledgements. *This research is funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP23489523)*

References

[1] Yeshkeyev A.R. Teorii i ikh modeli. Tom 2 / Monografiia v 2 tomakh. Karaganda: Izdetelstvo KarU im. akademika E.A. Buketova, 2024 — 297 p. [in Russian].

[2] Yeshkeyev A.R., Tungushbayeva I.O., Kassymetova M.T. On the Kaiser Class of a Jonsson Theory // Symmetry. – Basel, 2025. – Vol. 17, I. 6. – P. 870(1-25)

[3] Malcev, A.I. (1970). *Algebraicheskie sistemy [Algebraic systems].* Moscow: Izdatelstvo Nauka [in Russian]

[4] Yeshkeyev, A.R., Yarullina, A.R., Kassymetova M.T. (2024). Jonsson existentially closed unars of expanded signature. Bulletin of Abai KazNPU - Mathematical and Physical Sciences, Vol. 87, No. 3, 2024, pp. 1-17.

[5] Yeshkeyev A.R. Teorii i ikh modeli. Tom 1 / Monografiia v 2 tomakh. Karaganda: Izdetelstvo KarU im. akademika E.A. Buketova, 2024 — 282 p. [in Russian].

[6] Yeshkeyev, A.R., & Ulbrikht, O.I., Omarova M.T. Double factorization of the Jonsson spectrum. Bulletin of the Karaganda University-Mathematics, 2024, No. 4(116), P. 185-196.

J-o-Minimality and Learnability: A Study of connection between Jonsson theory and VC-Dimension

A.R.Yeshkeyev, A.K.Issayeva, N.V.Popova

Karaganda Buketov university, Karaganda, Kazakhstan

E-mail: isaevaaiga@gmail.com

Abstract

This paper explores Jonsson theories within the framework of model-theoretic logic, focusing on properties such as J-o-minimality and the presence of the JNIP (Jonsson Non-Independence Property). Special attention is given to the relationship between JNIP formulas and VC-dimension, establishing a connection between logical structures and the concept of Probably Approximately Correct (PAC) learning. The main result shows that a formula is JNIP if and only if the corresponding family of sets is a VC-class.

Definition 1. [A.R. Yeshkeyev] Let τ be some given pregeometry in C_T with a closure operator $cl : P(C_T) \to P(C_T)$. A Jonsson theory T is called normal in pregeometry τ (cl-normal), if, for each almost Jonsson subset $X \subseteq C_T$, $C_{Fr(X)}$ is an existentially closed submodel of C_T.

Definition 2.[A.R. Yeshkeyev] Let T be a Jonsson theory. A class K_T of L-structures is called a Kaiser class of T if

$$K_T = \{M \mid M \in Mod(T) \text{ and } Th_{\forall\exists}(M) \text{ is a Jonsson theory}\}.$$

Let T perfect normal complete theory for $\exists$-sentences.

Definition 3.[A.R. Yeshkeyev] Let T is perfect cl-normal Jonsson theory and $\phi(x, y)$ is a some $\exists$-formula in theory T (with a partition of the free variables). Say that $\phi(x, y)$ has the J-independence property (or JIP) if there are in $M \in K_T$ theory T $(a_i)_{i<\omega}$ and $(b_s)_{s\subseteq\omega}$ such that $\phi(a_i, b_s)$ holds iff $i \in s$. Say that ϕ is $JNIP$ if not. The theory T is $JNIP$ if all formulas are $JNIP$.

Definition 4.[A.R. Yeshkeyev] Jonsson theory T is J-o-minimal theory if T^*-o-minimal.

Definition 5. (Pregeometry in J-o-minimal Theories) [A.R. Yeshkeyev]

Let C_T is cemantic model J-o-minimal theory T. A pregeometry is a closure operator $\mathrm{cl} : \mathcal{P}(C_T^n) \to \mathcal{P}(C_T^n)$ satisfying the following axioms for all sets $A, B \subseteq C_T^n$:

1. Extensivity: $A \subseteq \mathrm{cl}(A)$
2. Idempotence: $\mathrm{cl}(\mathrm{cl}(A)) = \mathrm{cl}(A)$
3. Monotonicity: If $A \subseteq B$, then $\mathrm{cl}(A) \subseteq \mathrm{cl}(B)$
4. Finite character: $a \in \mathrm{cl}(A) \Rightarrow \exists A_0 \subseteq A$ finite such that $a \in \mathrm{cl}(A_0)$
5. Exchange property: If $a \in \mathrm{cl}(A \cup \{b\}) \setminus \mathrm{cl}(A)$, then $b \in \mathrm{cl}(A \cup \{a\})$

Proposition 1. An element $b \in cl(A)$ if there exists a formula $\varphi(x, \bar{a})$ (with parameters from A) such that:

1) $\varphi(x, \bar{a})$ defines a finite set $X \in M, M \in K_T$

2) $b \in X$

Well-known next facts about PAC-learning

Definition 6. Let X be a set and $\mathcal{F} \subseteq P(X)$. The pair $(X, \mathcal{F})$ is called a set system. We say that $A \subseteq X$ is shattered by $\mathcal{F}$ if for every $S \subseteq A$ there is $F \in \mathcal{F}$ such that

$F \bigcap A = S$. A family $\digamma$ is said to be a VC-class on X if there is some $n < \omega$ such that no subset of X of size n is shattered by $\digamma$. In this case the VC-dimension of $\digamma$, denoted by $VC(\digamma)$, is the smallest integer n such that no subset of X of size $n+1$ is shattered by $\digamma$. If no such n exists, we write $VC(F) = \infty$.

Theorem 1. The following are equivalent for a hypothesis class H with domain X:
(1) - H has finite VC dimension.
(2) - H is PAC learnible(PAC stands for Probably Approximately Correct).
Let T perfect normal $\exists$ complete theory for $\exists$-sentences.

Corollary 1. If theory T is J-o-minimal theory, then T has a $JNIP$-formula.

Theorem 2. [Main result] A formula is JNIP iff for some/every $M \in K_T$, the family $\{\phi(M^x, a) \mid a \in M^y\}$ is a VC-class.

Acknowledgements. This research has been funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP23489523)

References

[1] Yeshkeyev A.R. *Theories and their models.*, Karaganda, Kazakhstan: izd. KarU [in Russian], Volume 1,2. (2024).

[2] Vapnik V. N., Chervonenkis A. Ya. On the uniform convergence of relative frequencies of events to their probabilities, Reprint of Theor., Probability Appl., 16 (1971), no. 264–280.

On the perfectness of double factorization and the existentially finite cover property

A. R. Yeshkeyev, G. E. Zhumabekova, A. K. Koshekova

Karaganda Buketov University, Karaganda

E-mail: aibat.kz@gmail.com, galkatai@mail.ru, koshekova1998@mail.ru

Abstract

We study Jonsson theories in a countable first-order language L.

Definition 1. [1] *A theory T is called Jonsson if the following conditions hold for T:*
1. *T has at least one infinite model;*
2. *T is an inductive theory;*
3. *T has the amalgam property (AP);*
4. *T has the joint embedding property (JEP).*

Definition 2. [2] *A set $JSp(K)$ of Jonsson theories of L, where*

$$JSp(K) = \{T \mid T \text{ is a Jonsson theory and } K \subseteq Mod(T)\},$$

is said to be a Jonsson spectrum of K.

Definition 3. [2] *The Jonsson theory is said to be hereditary, if in any of its permissible enrichment, any expansion of it in this enrichment is a Jonsson theory.*

Definition 4. [2] *The Jonsson theory T is said to be perfect if its semantic model C is saturated.*

Let T be a Jonsson theory, $S^J(X)$ be a set of all existential complete n-types over X, consistent with T, for each finite n.

Definition 5. [2]

1) A Jonsson theory T is called J-P-λ-stable if $|S^J_P| \leq \lambda$ for any set A of cardinality $\leq \lambda$.

2) A Jonsson theory T is called J-P-stable if T is J-P-λ stable for some λ.

T.G. Mustafin introduced the notions of syntactic and semantic similarity of theories in the context of studying relationships between complete theories, including those formulated in different languages. To define semantic similarity, he employed the concepts of a pure triple and isomorphism between pure triples.

Building on this framework, A.R. Yeshkeyev later extended these ideas to Jonsson theories, which, in general, are not complete. In particular, he defined the notions of Jonsson syntactic similarity and Jonsson semantic similarity for such theories.

In this work, we focus on special classes of Jonsson theories for which these two similarity relations coincide. We denote this equivalence by $T_1 \overset{SS}{\bowtie} T_2$.

Definition 6. [2] *Let T_1 and T_2 are Jonsson theories. We will say that T_1 and T_2 are J-syntactically similar if there is an bijection $f : E(T_1) \to E(T_2)$ such that*
1. the restriction of f to $E_n(T_1)$ is an isomorphism of the lattices $E_n(T_1)$ and $E_n(T_2), n < \omega$,
2. $f(\exists v_{n+1}\varphi) = \exists \varphi_{n+1} f(\varphi), \varphi \in \exists_{n+1}(T), n < \omega$,
3. $f(v_1 = v_2) = (v_1 = v_2)$

Definition 7. [2] A pure triple $\langle C_T, AutC_T, SubC_T\rangle$ is called J-semantic triple, where C_T is semantic model of T, $AutC_T$ is a group of automorphisms of C_T, $SubC_T$ is the class of all subsets of carriers C_T, which are carriers the corresponding submodels of C_T.

Definition 8. [2] Two Jonson theories T_1 and T_2 are called J-semantically similar if their J semantic triples are isomorphic as pure triples.

Definition 9. [3] Let T be a Jonsson L-theory and $f(\bar{x},\bar{y})$ be an $\exists$-formula of L.

1) If for any arbitrary large n there exists $\bar{a}_1,...,\bar{a}_n$ in some existentially closed model of T, and $\bar{a}_1,...,\bar{a}_n$ satisfies $\neg(\exists x)\curlywedge_{k\leq n} f(\bar{x},\bar{a}_k)$, and for any $l\leq n$ $\neg(\exists x)\curlywedge_{k\leq n, k\neq l} f(\bar{x},\bar{a}_k)$, then $f(\bar{x},\bar{y})$ is said to have e.f.c.p. (existentially finite cover property).

2) A Jonsson theory T has the existentially finite cover property if there exists a formula $f(\bar{x},\bar{y})$ that has the existentially finite cover property.

Definition 10. [4] Let T be a Jonsson theory, C_T be its semantic model, $X\subseteq C_T$. X is called an almost Jonsson set, if the following conditions are hold:
(1) X is an $\exists$-definable set;
(2) $cl(X)=M\in Mod(T)$;
(3) $Th_{\forall\exists}(M)$ is a Jonsson theory, where $Th_{\forall\exists}(M)$ is a set of all universal-existential sentences of the language L that are true in the model M.

Definition 11. [4] A Jonsson theory T is called a normal theory if for any almost Jonsson set $X\subseteq C_T : C_{Fr(X)}\in Mod(T)$ and $C_{Fr(X)}$ is existentially closed submodel of C_T, where $C_{Fr(X)}$ is a semantic model of $Fr(X)$.

Theorem 1. Let T be an $\exists$-complete normal Jonsson theory. Let $JSp(K)_{/\bowtie,\overset{SS}{\bowtie}}$ is a factor-set of the Jonsson spectrum of K, $[\Delta]\in JSp(K)_{/\bowtie,\overset{SS}{\bowtie}}$, $[\Delta]^*$ is a center of $[\Delta]$, $T_1,T_2\in[\Delta]$, $T_1\overset{S}{\bowtie}T_2$. If $[\Delta]^*$ is λ-stable, then $[\Delta]$ is perfect.

Theorem 2. Let T be an $\exists$-complete, normal, hereditary Jonsson theory. Let $JSp(K)_{/\bowtie,\overset{SS}{\bowtie}}$ is a factor-set of the Jonsson spectrum of K, $[\Delta]\in JSp(K)_{/\bowtie,\overset{SS}{\bowtie}}$, $[\bar{\Delta}]=[\Delta]\cup\{P,\subseteq\}$, $[\bar{\Delta}]^*$ is a center of $\bar{\Delta}$. If the class $[\bar{\Delta}]^*$ does not have the existential finite cover property (e.f.c.p.) and is a P-λ-stable class, then the class $[\bar{\Delta}]^*$ is J-P-λ-stable and also does not have the existential finite cover property (e.f.c.p.).

Acknowledgements. The research has been by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP22686827 "The central types of hereditary Jonsson theories").

References

[1] J. Barwise. Teoriya modelei: spravochnaia kniga po matematicheskoi logike. Chast 1 [Model theory: Handbook of mathematical logic. Part 1], Izdatelstvo Nauka, Moscow (1982).

[2] A.R. Yeshkeyev. Theories and their models. Karaganda, Kazakhstan: izd. KarU [in Russian], Volume 1,2. (2024).

[3] G.E. Zhumabekova. Model-theoretic properties of semantic pairs and e.f.c.p. in Jonsson spectrum // Bulletin of the Karaganda University. Mathematics Series. 2023. vol. 4. no.112. P.185–193. https://doi.org/10.31489-/2023m4/185–193.

[4] A.R. Yeshkeyev, O.I. Ulbrikht, & M.T. Omarova. Double factorization of the Jonsson spectrum // Bulletin of the Karaganda University-Mathematics. 2024. 116(4). P. 185–196.

Universal equivalence of pseudofinite abelian groups

Fazyl Zhebey

L.N. Gumilyov Eurasian National University

E-mail: fzhebei@gmail.com

Abstract

This work is devoted to the model-theoretic analysis of pseudofinite abelian groups, with a particular focus on conditions for universal equivalence. A vector of invariants is introduced, where the first coordinate corresponds to the fourth classical invariant, and the subsequent components represent the third invariants computed at various levels of a fixed filtration. It is proved that two pseudofinite abelian groups are universally equivalent if all the entries of this vector (excluding the first) are infinite.

Acknowledgements. *The study was partially supported by the Scientific Committee for Education and Science of the Republic of Kazakhstan (AP19677451)*

References

[1] Mishchenko, A.A., Remeslennikov, V.N., Treier, A.V. (2017). Universal Invariants for Classes of Abelian Groups. *Algebra and Logic*, 56(2), 176–201.

[2] Pavlyuk, I.I., Sudoplatov, S.V. (2019). Ranks of Families of Theories of Abelian Groups. *Izvestiya of Irkutsk State University. Series Mathematics*, 28, 95–112.

ON PSEUDOFINITENESS OF UNCOUNTABLY CATEGORICAL UNAR THEORIES

Adilkhan A. Nuraly and Nurlan D. Markhabatov

L.N. Gumilyov Eurasian National University

E-mail: adilnur001@gmail.com, markhabatov@gmail.com

Abstract

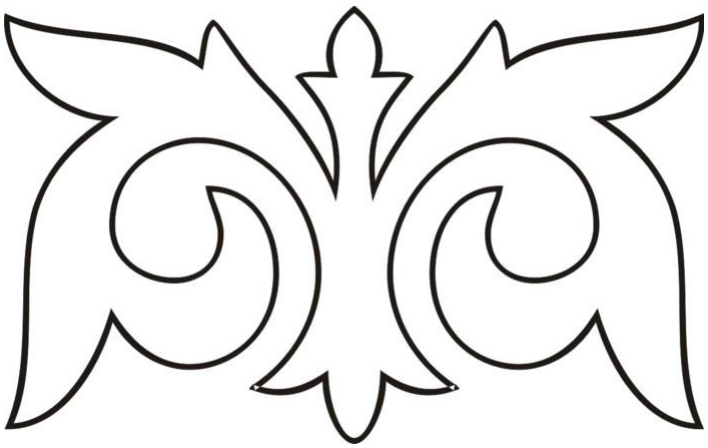
This work concerns unars, i.e., models of a theory with a single unary function. In [1], it was shown that every bounded theory of unars is pseudofinite; moreover, countably categorical unars are smoothly approximable. Various types of approximations and strongly minimal unars were also studied. In the present work, we investigate the pseudofiniteness of unars that are uncountably categorical.

Acknowledgements. *The study was partially supported by the Scientific Committee for Education and Science of the Republic of Kazakhstan (AP19677451)*

References

[1] N.D. Markhabatov, *Approximations of Theories of Unars*, *Bulletin of the Karaganda University. Mathematics Series, No. 3(117), 2025, to appear*

Theories of Computability and Computable Models



HKSS-completeness of the class of Boolean algebras with distinguished subalgebras and atoms

Valeriy Isakov

Novosibirsk State University

E-mail: v.isakov@g.nsu.ru

Abstract

In 2002, D. R. Hirschfeldt, B. Khoussainov, R. A. Shore, and A. M. Slinko [1] proposed an approach for constructing examples of structures with given computability-theoretic properties starting from well-known structures with such properties. In particular, for a given class of structures, the concept of completeness (with respect to degree spectra of nontrivial structures, effective dimensions, expansion by constants, and degree spectra of relations) was introduced. Classes of structures that have such completeness property are called *HKSS–complete*.

It is known that the class of Boolean algebras is not *HKSS*–complete: S. S. Goncharov and V. D. Dzgoev [2] proved that the computable dimension of a computable Boolean algebra $\mathcal{B}$ is either 1 or ∞, which is not true for an *HKSS*–complete class. In 2012, B. Khoussainov and T. Kowalski [3] started systematic investigations of the following problem: how does expanding the language of Boolean algebras affect their computability-theoretic properties?

We will present a result on the *HKSS*–completeness of the class of Boolean algebras with three distinguished subalgebras and distinguished set of atoms.

References

[1] D. Hirschfeldt, B. Khoussainov, R. Shore, A. Slinko, *Degree Spectra and Computable Dimensions in Algebraic Structures*, *Annals of Pure and Applied Logic, 115*(1–3), 71–113, 2002.

[2] S. S. Goncharov, V. D. Dzgoev, *Autostability of models*, *Algebra and Logic, 19*(1), 28–37, 1980.

[3] B. Khoussainov, T. Kowalski, *Computable Isomorphisms of Boolean Algebras with Operators*, *Studia Logica, 100*(3), 481–496, 2012.

On the existence of universal equivalence relations in the Ershov hierarchy

Zh.A. Aset, S.A. Badaev, S.L. Yun, R.E. Zhailybaev

Kazakh-British Technical University, Tole Bi street 59, Almaty, Kazakhstan

E-mail: zh_aset@kbtu.kz, s.badaev@kbtu.kz, s_yun@kbtu.kz, r_zhailybaev@kbtu.kz

Abstract

Denote by $\tilde{\Sigma}_n^{-1}$ ($\tilde{\Pi}_n^{-1}$) the set of all equivalences from the class Σ_n^{-1} (relatively Π_n^{-1}) of the Ershov hierarchy, [1]. Here and furthermore we identify the pairs of numbers with their Cantor index. Elements of the class $\tilde{\Sigma}_1^{-1}$ are well-known in literature as computably enumerable equivalence relations (ceers) and are intensively studied in the last two decades with respect to the following reduction.

Definition 1. For a given equivalences P and Q on ω, we will say that P is *computably reducible* to Q and write $P \leqslant_c Q$ if there is a computable function f such that, for all x, y,

$$P \leqslant_c Q \iff xPy \leftrightarrow f(x)Qf(y).$$

We call an equivalence Q universal in a class $\mathcal{K}$ of equivalences if $Q \in \mathcal{K}$ and $P \leqslant_c Q$ for every $P \in \mathcal{K}$.

Definition 2. (Bazhenov& Kalmurzaev, [2]) Let $X \in \Sigma_n^{-1}$, define the operator

$$M(X) = \{(x,x)|x \in N\} \cup \{(2x, 2x+1), (2x+1, 2x)|x \in X\}$$

Proposition 1. $X \in \Sigma_n^{-1}(\Pi_n^{-1}) \leftrightarrow M(X) \in \tilde{\Sigma}_n^{-1}(\tilde{\Pi}_n^{-1})$.

There is a well-known result from [1] "Theorem of hierarchy". By the above Proposition we are able to formulate and prove the following

Proposition 2. For any $n > 0$, there exists a m-universal equivalence relation $R_n \in (\tilde{\Sigma}_{n+1}^{-1} \cap \tilde{\Pi}_{n+1}^{-1})$.

Proposition 3. For every $n > 0$ the following statements are true:

1. $\tilde{\Sigma}_n^{-1} \subset \tilde{\Sigma}_{n+1}^{-1}$, $\tilde{\Pi}_n^{-1} \subset \tilde{\Pi}_{n+1}^{-1}$,
2. $\tilde{\Sigma}_n^{-1} \cup \tilde{\Pi}_n^{-1} \subset \tilde{\Sigma}_{n+1}^{-1} \cap \tilde{\Pi}_{n+1}^{-1}$,
3. $\tilde{\Sigma}_n^{-1} \setminus \tilde{\Pi}_n^{-1} \neq \emptyset$, $\tilde{\Pi}_n^{-1} \setminus \tilde{\Sigma}_n^{-1} \neq \emptyset$.

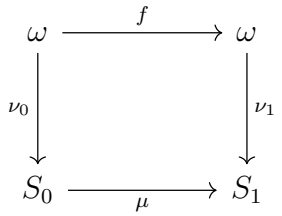
Universal objects play significant role in the study of many fields of the computability theory. We refer to the survey [3] for a history and deep achievements in the study universal ceers. In [4] it was shown that for any $n > 1$, there exists an universal equivalence relation in $\tilde{\Sigma}_n^{-1}$. In [2], this result was extended for all ordinal notations a and for $\tilde{\Pi}_a^{-1}$ equivalences. The latter was shown by means of direct construction. We suggest to use categorial approach to prove the existence of universal equivalences in $\tilde{\Pi}_n^{-1}$. The same approach is applicable to $\tilde{\Pi}_a^{-1}$ for arbitrary ordinal notation a.

Our approach use the following simple observation.

Proposition 4. Every Σ_n^{-1}-computable numbering of $\tilde{\Sigma}_n^{-1}$ induces universal equivalence relation in $\tilde{\Sigma}_n^{-1}$ and every Π_n^{-1}-computable numbering of $\tilde{\Pi}_n^{-1}$ induces universal equivalence relation in $\tilde{\Pi}_n^{-1}$.

We consider a subcategory K_Σ of the category of numbered sets, introduced by Ershov, [5]:

1. $Ob(K_\Sigma) = \{(S, \nu) : S \subseteq \Sigma_n^{-1}$ & ν is Σ_n^{-1}-computable numbering of $S\}$
2. Let $\mathfrak{S}_0, \mathfrak{S}_1 \in Ob(K_\Sigma)$, then mapping $\mu : S_0 \to S_1$ is called morphism ($\mu \in Mor(\mathfrak{S}_0, \mathfrak{S}_1)$) if there is a computable function $f(x)$ s.t. following diagram commutes:



In the similar fashion we define category K_Π, where objects are tuples (S, ν), but $S \subseteq \Pi_n^{-1}$ and ν is computable numbering of S. Morphisms are defined analogous way as in K_Σ.

Proposition 5. $\tilde{\Sigma}_n^{-1}$ is an n-subset of the numbered set (Σ_n^{-1}, α), where α is a principal numbering.

This statement indeed has been proved in [2], Proposition 2.1.

Proposition 6. Categories K_Σ and K_Π are isomorphic.

Corollary 1. There exists a principal numbering of Π_n^{-1}.

Yu.L. Ershov noticed that the family of positive equivalences is r-subset of the family of all c.e. sets under standard numbering, [6]. It might be generalized to common case.

Corollary 2. $\tilde{\Pi}_n^{-1}$ is an n-subset of the numbered set (Π_n^{-1}, α), where α is a principal numbering.

Corollary 3. There exists a principal numbering $\tilde{\alpha}$ of $\tilde{\Pi}_n^{-1}$.

Corollary 4. There is a universal equivalence relation in $\tilde{\Pi}_n^{-1}$, [2].

Acknowledgements. *The work was supported by the Science Committee of the Ministry of Education and Science of the Republic of Kazakhstan (Grant No.AP08856834).*

References

[1] Ershov Yu.L., *A hierarchy of sets. I, Algebra and Logic, 7*, (1968), 25–43.

[2] Bazhenov N.A., Kalmurzaev B.S., *Weakly Precomplete Equivalence Relations in the Ershov Hierarchy, Algebra and Logic, 58(3)*, (2019), 199–213.

[3] Andrews U., Badaev S., Sorbi A., *A survey on universal computably enumerable equivalence relations, Lecture Notes in Computer Science. Computability and Complexity, 10010* (2016), 418–451.

[4] Ng K.M., Yu H., *On the degree structure of equivalence relations under computable reducibility,Notre Dame Journal of Formal Logic, 60(4)*, (2019), 733–761.

[5] Ershov Yu.L., *Theory of Numberings. Nauka, Moscow*, (1977).(in Russian)

[6] Ershov Yu.L., *Positive equivalences, Algebra and Logic, 10*, (1971), 378–394.

Pseudofinite non-computable graphs

I.V. Latkin, A. Kydyrkhankyzy, Zh. A. Sakhanova

D.Serikbayev EKTU, Oskemen, Kazakhstan

E-mail: lativan@yandex.kz, akydyrkhankyzy@gmail.com, zhaiana@bk.ru

Abstract

Definition. Let $G_{\text{fin}}(\lambda)$, for an arbitrary cardinality λ, be a class of all infinite acyclic graphs consisting of λ connected components whose *aggregate diameters are bounded.*

The graphs in $G_{\text{fin}}(1)$ are trees with a single connected component and infinitely many hanging vertices. More generally, graphs in $G_{\text{fin}}(\lambda)$ may contain both finite and infinite components, as long as their diameters remain uniformly bounded.

Let $\Gamma =< V; R >$ is a graph. We define

$D(\Gamma) = \{n > 1 \mid \exists v\,(\deg v = n)\} =$

$= \{n > 1 \mid \exists v\,(\exists u_1, \ldots, u_n)\big[\bigwedge\limits_{i=1}^{n} R(v; u_i) \wedge \bigwedge\limits_{1\le i<j\le n} u_i \neq u_j \wedge (\forall w) \bigwedge\limits_{i=1}^{n} \big(u_i \neq w \to \neg R(v, w)\big)\big]$.

Theorem 1. For any infinite set $A \subseteq \mathbb{N} \setminus \{0, 1\}$, there exists graph $\Gamma_A \in G_{\text{fin}}(\omega)$ such that $D(\Gamma_A) = A$.

Proof. Let A be a set. For each $n \in$ A, let S_n be a star graph with a central vertex v $deg(v) = n$. Then $\Gamma = \amalg_{n\in A} S_n$, it is known that diameter of each S_n equals 2.

Theorem 2. There exist pseudofinite graphs from the class $G_{\text{fin}}(\omega)$ that do not have computable copies (non-constructivizable).

Proof. By Theorem 4 [2], the theory T of any acyclic graph Γ belonging to the class $\mathcal{G}_{fin}(\lambda)$is pseudofinite. That is, every graph in this class is pseudofinite.

Lemma. If the graph Γ is computable, i.e., has a constructive numeration of domain V of Γ, then D(Γ)$\in \sum_2^0$.

Proof. Let Γ is computable, i.e., there exists numeration $\nu : \mathbb{N} \to\!< V; R >$. We have $n \in$ D(Γ), if and only if $n > 1 \wedge (\exists v)\ (\exists u_1, \ldots, u_n)\big[\bigwedge_{i=1}^{n} R(v; u_i) \wedge \bigwedge_{1\le i<j\le n} u_i \neq u_j \wedge (\forall w) \bigwedge_{i=1}^{n} \big(u_i \neq w \to \neg R(v, w)\big)\big]$. Equivalently, when considering the numbers of elements from V, $n \in$ D(Γ) $\Leftrightarrow n > 1 \wedge (\exists k)\ (\exists r_1, \ldots, r_n)\big[\bigwedge_{i=1}^{n} R(\nu k; \nu r_i) \wedge \bigwedge_{1\le i<j\le n} \nu k_i \neq \nu k_j \wedge (\forall s) \bigwedge_{i=1}^{n} \big(\nu k_i \neq \nu s \to \neg R(\nu k, \nu s)\big)\big]$ We recall that $\nu : \mathbb{N} \to\!< v; R >$ is constructivization. This means that there are recursive predicates T_R and $T_=$: $(\forall m, s \in \mathbb{N})[(R(\nu m, \nu s) \Leftrightarrow T_R(m, s))$ and $(\nu m = \nu s \Leftrightarrow T_=(m, s))]$

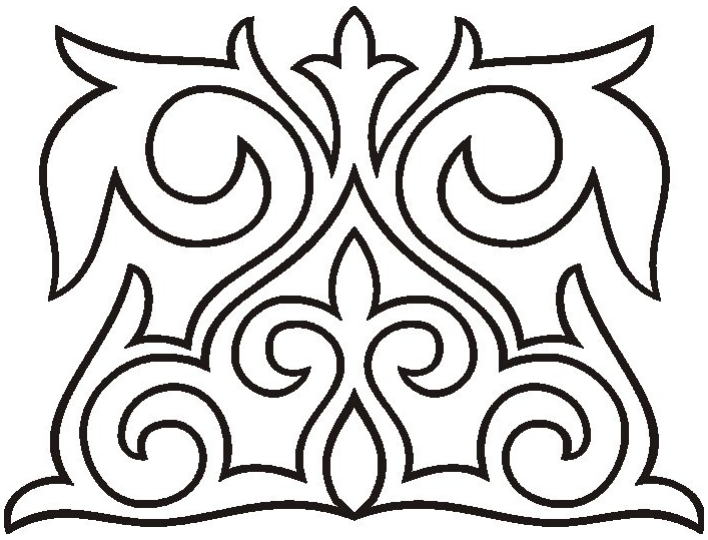
References

[1] Goncharov, S. S.; Ershov, Yu. L. Constructive models. - Novosibirsk: Nauchnaya kniga, 1999. - 345 p.

[2] N. D. Markhabatov, “Approximations of Acyclic Graphs”, Bulletin of Irkutsk State University, Series Mathematics, 40 (2022), 104–111

[3] H.Rogers, "Theory of recursive functions and effective computability", Massachusetts Institute of Technology, 1967.

Algebra



Superposition of three elementary polynomial automorphisms

Kerimbayev R.K. Yuan B.

Al Farabi Kazakh National University

E-mail: ker_im@mail.ru, 06littleluck06@gmail.com

Abstract

In 2003, Shestakov-Umirbayev proved that Nagata automorphisms[1] are wild[2]. In 2022, Kerimbayev showed that Nagata automorphisms are algebraic. Using this result, we give another proof of Shestakov-Umirbaev theorem[3]. In 2024, Kerimbayev showed in his work that elementary automorphisms are quadratic. Then, together with Yuan, Kerimbayev showed that the superposition of elementary automorphisms is cubic, which is even algebraic to a higher degree. At the same time, the superposition of two elementary automorphisms may not be algebraic. In this work, we prove the following theorem

Theorem. *The superposition of three elementary automorphisms is algebraic of degree two and degree four is not algebraic.*

Remark. Nagata automorphism is not a superposition of three elementary automorphisms.

Acknowledgements. *This study was funded by the Science Committee of the Ministry of Education and Science of the Republic of Kazakhstan as part of the grant project No. AP19679799 "Development of a modified methodology for assessing spatial growth factors and overcoming differences between regions".*
The second author is supported by Chinese Governmental scholarship (China-Kazakhstan intergovernmental agreement).

References

[1] M. Nagata, *On Automorphism group of k[x,y], Lectures in Mathematics 5, Tokyo* , 1972. https://core.ac.uk/download/pdf/39217134.pdf.

[2] Shestakov, Ivan P., Ualbai U. Umirbaev *The Nagata Automorphism Is Wild, Proceedings of the National Academy of Sciences of the United States of America*, 100, no. 22 (2003): 12561–63. http://www.jstor.org/stable/3147998

[3] Kerimbayev R. K. *One property of Nagata automorphism , Traditional International April Mathematical Conference (The Institute of Mathematics and Mathematical Modelling), Almaty, Kazakhstan.* (2022), P.33.

ALGEBRAIC POLYNOMIAL OF TWO VARIETIES KELLER POLYNOMIALS

Kerimbayev R.K., Kuandykova A.M.

Al Farabi Kazakh National University

E-mail: ker_im@mail.ru, akbota.kuandykova.04@inbox.ru

Abstract

On the way to solving the famous Jacobian problem [1], it is very important to study the algebraic polynomials of Keller polynomials that determine this representation. In the 2020s, Kerimbayev R. K. showed that for Keller polynomials of two varieties, their algebraic polynomial is a finite set [2]. At the same time, this author also showed in 2017 that a two-dimensional surface defined in four-dimensional Euclidean space according to Keller's representation does not have a tangent plane parallel to the coordinate plane [3]. In this work, we show that for a four-dimensional Euclidean space, considering a 16-dimensional Grossman space, the algebraic polynomial of two varieties Keller polynomials consists of only one point.

THEOREM. Let $f(x,y), g(x,y) \in R[x,y]$ for polynomials of

$$f(0,0) = g(0,0) = 0 \; and \; f_x g_y - f_y g_x = 1$$

f_x, f_y, g_x, g_y- mutually independent partial derivatives.

Then $V(f,g) = \{(x,y) \in R^2 \mid f(x,y) = 0 = g(x,y)\}$ the algebraic polynomial of the polynomials f and g consists of only one (0; 0) point, that is

$$\{V(f,g)\} = \{(0;0)\}$$

PROOF

$\Omega = R \oplus R^4 \oplus (R^4 \wedge R^4) \oplus (R^4 \wedge R^4 \wedge R^4) \oplus (R^4 \wedge R^4 \wedge R^4 \wedge R^4)$- We consider a Grossman space of 16 dimensions. For point $(a,b) \in R^2$ let be $f(a,b) = g(a,b) = 0$ $(a,b) \neq (0;0)$. Then in Space R^4, the radius Vector $r(t) = (at, bt, f(at,bt), g(at,bt))$ gives a line connecting the point (0;0;0;0) and the point (a;b;0;0), where $t \in [0;1]$ corresponds to the segment. In short, we denote $f(t) = f(at,bt), g(t) = g(at,bt)$.

Then $f'(t) = f_x(at,bt)\,a + f_y(at,bt)\,b, g(t) = g_x(at,bt)\,a + g_y(at,bt)b$. We get $r'(t) = (a, b, f'(t), g'(t))$.

If we get $f(t), g(t) \in R[t]$, then

$$[f(t), g(t)] = f'(t)\,g(t) - f(t)\,g'(t)$$

by the commutator $(R[t], [\cdot,\cdot])$,The system becomesa Lie algebra.

$$r(t) \wedge r'(t) = (ae_1 + be_2) \wedge ([f,t]\,e_3 + [g,t]\,e_4) + [g(t), f(t)]\,e_3 \wedge e_4$$

Considering that, we get equality

$$r(1) \wedge \ r(t) \wedge r'(t) = [g(t), f(t)] (ae_1 + be_2) \wedge e_3 \wedge e_4$$

Then

$$|r(1) \wedge r(t) \wedge r'(t)| = \sqrt{a^2 + b^2} \ |[g(t), f(t)]|$$

Additionally,

$|r(1) \wedge r(t) \wedge r'(t)| = |r(1)| \cdot |r(t) \wedge r'(t)| = \sqrt{a^2 + b^2} \ |r(t) \wedge r'(t)\ |$

So, $|r(t) \wedge r'(t)| = |[g(t), f(t)]\ |$. When $t = 1$, from this, we can see that. $|r(t) \wedge r'(t)| = 0$. That is, $r(1)$ is parallel to $r'(1)$. This is a contradiction.

So $a = 0$ and $b = 0$. The theorem is proved.

REFERENCES

[1] Van den Essen A. Polynomial Automorphisms and the Jacobian Conjecture.- Birkhauser: Progress in mathematics,2000.

[2] Kerimbaev R.K. Finiteness of Keller manifolds in two variables, Almaty, April 5-8, 2021. Traditional international April mathematical conference in honor of the Day of Science Workers of the Republic of Kazakhstan dedicated to the 75th anniversary of Academician of the National Academy of Sciences of the Republic of Kazakhstan T.Sh.Kalmenova

[3] Kerimbaev R.K. A geometric solution to the Jacobian Problem. Journal of New Theory, 24, 2018. "

MODULARITY PROPERTY OF THE JACOBIAN

Kerimbayev R.K., Spankulova L.S.

Al-Farabi Kazakh National University

E-mail: ker_im@mail.ru

Abstract

The Jacobian is a mapping that corresponds to the polynomials $f_1, f_2, \ldots, f_n \in R[x_1, \ldots, x_n] = K$, the determinant of the matrix of their independent derivatives, and is polylinearly and skew-symmetrically dependent on these polynomials. Then we are given the mapping $J : K \wedge \ldots \wedge K \to K$. We take for this mapping $J(f_1 \wedge \ldots \wedge f_n + g_1 \wedge \ldots \wedge g_n) = J(f_1 \wedge \ldots \wedge f_n) + J(g_1 \wedge \ldots \wedge g_n)$ and continue this mapping for the addition operation. Differential mappings are defined for the spaces $\wedge^n K$ and K. In particular, for the algebra K, a general Lie algebra of the form $W_n = Der(K)$ – Cartan is given. The Lie algebra W_n has a special sub-Lie algebra of the Cartan type $S_n = \{D \in W_n | \ div(D) = 0\}$. It is worth noting that W_n and S_n are simple Lie algebras. For the differential $D \in W_n, D : K \to K$, we define the differential $\widetilde{D} : \wedge^n K \to \wedge^n K$. It is given by the following formula:

$$\widetilde{D}(f_1 \wedge \ldots \wedge f_n) = D(f_1) \wedge \ldots \wedge f_n + \ldots + f_1 \wedge \ldots \wedge D(f_n)$$

Our goal is to find the relationship between the mappings $J, D, \widetilde{D}$ and div. The following theorem holds.

THEOREM [1]
For the mappings $J, \widetilde{D} : \wedge^n K \to \wedge^n K, D : K \to K$ and $div : W_n \to K$, the following formula is true:

$$J \circ \widetilde{D} = D \circ J + div(D) \circ J$$

COROLLARY [1]
In the case of $D \in S_n$

$$J \circ \widetilde{D} = D \circ J$$

the formula surely.

The above theorem shows that in general the Jacobian does not have the modular property. And if we take a differentiation with zero divergence, then by consequence we see that the Jacobian has the modular property. That is, the set of elements $f_1, \ldots, f_n$ consisting of polynomials $f_1 \wedge f_2 \wedge \ldots \wedge f_n$ whose Jacobian is constant is an inner module of the module $\wedge^n K$. This inner module also contains the kernel $kerJ$ of the mapping J. Therefore, for a special Lie algebra S_n, the set of elements $f_1 \wedge f_2 \wedge \ldots \wedge f_n$ of Jacobian

constant polynomials gives a separate inner module. And this module also contains elements consisting of polynomials forming an automorphism. The one-dimensional space $\mathbb{R}$ is invariant for the differential $D : K \to K$. The inner space is Then for Lie algebras W_n or S_n, the space $\mathbb{R}$ has an irreducible inner module: $R = ker\,(D)\,, \forall D \in W_n$. Consider the elements $f_1 \wedge \ldots \wedge f_n$ and $g_1 \wedge \ldots \wedge g_n$. In a module $\wedge^n K$, for elements $f_1 \wedge \ldots \wedge f_n$ and $g_1 \wedge \ldots \wedge g_n$, we say that these two elements are equivalent to each other if $J\,(f_1 \wedge \ldots \wedge f_n) - J(g_1 \wedge \ldots \wedge g_n) \in R$. This relation indeed gives an equivalence relation. Thus, for a module $\wedge^n K$, we obtain the partition $\wedge^n K = A_0 \cup A_1 \cup \ldots \cup A_n \cup \ldots$, where $A_i = \{f_1 \wedge f_2 \wedge \ldots \wedge f_n\}\ J\,(f_1 \wedge f_2 \wedge \ldots \wedge f_n)$- is a polynomial of degree i. Here A_0 is the set of elements $f_1 \wedge f_2 \wedge \ldots \wedge f_n$ whose Jacobian is constant. By implication, it is an inner module. It is homomorphic to the irreducible S_n-module $\mathbb{R}$. This homomorphism is a superposition homomorphism. The module A_0 has an inner module consisting of elements $f_1 \wedge f_2 \wedge \ldots \wedge f_n$ whose Jacobian is zero. Then the factor-module $A_0/A - \infty$ is isomorphic to the irreducible S_n-module $\mathbb{R}$. The module $A - \infty$ is a vertical sum of the module A_0. Thus, the module A_0 has an inner irreducible module bijective to the set $\mathbb{R}$-$\{0\}$. Thus, the elements $f_1 \wedge f_2 \wedge \ldots \wedge f_n$ whose Jacobian is nonzero give automorphisms of the ring K.

REFERENCES

[1]Kerimbaev R.K., Spankulova L.S., Commutative property of Jacobian, Proceedings of the 11th International Asian School-Seminar " Problems of Optimization of Complex Systems", part I, Cholpan-Ata-2015.

THE COMPLEXITY OF THE THREE BY THREE MATRIX ALGEBRA

Kerimbayev R.K., Saparbekova A.S.

Al-Farabi Kazakh National University

E-mail: ker_im@mail.ru, anelyasaparbekova823@gmail.com

Abstract

In 1969, Strassen devised his famous algorithm for two by two matrix algebra. The standard multiplication operation for two by two matrices requires eight multiplications of variables. However, Strassen's algorithm reduces this by one, requiring only seven multiplications. If we decompose the group algebra into ideals, we obtain three ideals. One of these ideals is isomorphic to the two by two matrix algebra. Using the Alder–Strassen theorem [2], we can conclude that the complexity of the two by two matrix algebra cannot be less than seven. Combined with Strassen's algorithm, this shows that the complexity of the two by two matrix algebra is exactly seven. A similar result can be obtained for three by three matrices. It is generally conjectured that the complexity of three by three matrices is equal to nineteen. In this work, by decomposing the group algebra, we show that it has three ideals, one of which is isomorphic to the three by three matrix algebra.

According to the Alder–Strassen theorem, the complexity of the algebra is at least 21. From this result, it immediately follows that the complexity of the three by three matrix algebra is not less than seventeen. However, the structural matrices of the three by three matrix algebra are of order nine, and their linear combinations form block-diagonal matrices corresponding to three by three matrices. If the complexity of the algebra is less than 23, then the rank of the linear combinations of its structural matrices would be less than 22. The ideals of the algebra RA_4 are isomorphic to the algebras R, C, and $M_3(\mathbb{R})$. From this, it follows that the blocks corresponding to R and C have full rank, while the block corresponding to $M_3(\mathbb{R})$ must have rank less than 9. Therefore, this block has a maximum rank of 6. Consequently, six rank-one matrices are sufficient for this block. Therefore, six rank-one matrices are sufficient for this block. As a result, 1+2+6+11=20 rank-one matrices would be enough to compute the product in the algebra. However, this contradicts the Alder–Strassen theorem. Hence, the complexity of the algebra is not less than 23. It follows that the complexity of the algebra $M_3(\mathbb{R})$ is not less than 19. Thus, we have proven the following theorem.

Theorem

The complexity of the 3×3 matrix algebra is not less than nineteen, that is,

$$L(M_3(\mathbb{R})) \geq 19.$$

References

1. Strassen, V. (1969). Gaussian Elimination is not Optimal. *Numerische Mathematik*, 13(4), 354–356.
2. Alder, H., & Strassen, V. On the algorithmic complexity of associative algebras.
3. Alder, H. L., & Strassen, V. (1976). Algebraic Complexity Theory. *Springer Lecture Notes in Computer Science*, Vol. 53.

Automorphisms of free braided nonassociative algebra of rank 2

Riza Mutalip, Altyngul Naurazbekova, Bibinur Duisengalieva

L.N. Gumilyov Eurasian National University, Astana, Kazakhstan

E-mail: mutalipriza@yahoo.com, naurazbekova82@gmail.com, bibinur959@gmail.com

Abstract

It is well known [1, 2, 3, 4] that all automorphisms of the polynomial algebra $K[x_1, x_2]$ and the free associative algebra $K\langle x_1, x_2\rangle$ of rank two over an arbitrary field K are tame. P. Cohn [5] proved that all automorphisms of finitely generated free Lie algebras over an arbitrary field are tame. J. Lewin [6] extended this result to homogeneous Schreier varieties of algebras. Recall that varieties of all nonassociative algebras [7], commutative and anti-commutative algebras [8], Lie algebras [9, 10], and Lie superalgebras [11, 12] are Schreier. Therefor, all automorphisms of finitely generated free nonassociative algebras over an arbitrary field are tame.

R. Mutalip, A. Naurazbekova and U. Umirbaev [13] described the automorphism groups of free braided associative algebras in two variables $(K\langle x_1, x_2\rangle, \tau)$ with a diagonal involutive braidings over an arbitrary field of characteristic $\neq 2$. We obtain the similar result for free braided nonassociative algebras.

Acknowledgements. This work was supported by the grant of the Ministry of Science and Higher Education of the Republic of Kazakhstan (project AP23487886).

References

[1] Czerniakiewicz, A.J. (1971,1972). Automorphisms of a free associative algebra of rank 2. I, II. *Trans. Amer. Math. Soc.,* 160, 393–401; 171, 309–315.

[2] Jung, H.W.E. (1942). Uber ganze birationale Transformationen der Ebene. *J. reine angew Math., 184*, 161–174.

[3] van der Kulk, W. (1953). On polynomial rings in two variables. *Nieuw Archief voor Wisk., 1*(3), 33–41.

[4] Makar-Limanov, L.G. (1970). Ob avtomorfizmakh svobodnoi algebry s dvumia obrazuiushchimi [The automorphisms of the free algebra of two generators]. *Funktsional. Anal. i Prilozhen. — Functional Analysis and Applications, 4*(3), 107–108 [in Russian].

[5] Cohn, P.M. (1964). Subalgebras of free associative algebras, *Proc. London Math. Soc., 14*(3), 618–632.

[6] Lewin, J. (1968). On Schreier varities of linear algebras. *Trans. Amer. Math. Soc., 132*, 553–562.

[7] Kurosh, A.G. (1947). Neassotsiativnye svobodnye algebry i svobodnye proizvedeniia algebr [Nonassociative free algebras and free products of algebras]. *Mat. Sb. — Sbornik: Mathimatics, 20*, 239–262 [in Russian].

[8] Shirshov, A.I. (1954). Podalgebry svobodnykh kommutativnykh i svobodnykh antikommutativnykh algebr [Subalgebras of free commutative and free anticommutative algebras]. *Matem. sbornik — Sbornik: Mathimatics, 34*(76), 81–88 [in Russian].

[9] Shirshov, A.I. (1953). Podalgebry svobodnykh lievykh algebr [Subalgebras of free Lie algebras]. *Matem. sbornik — Sbornik: Mathimatics, 33*(75), 441–452 [in Russian].

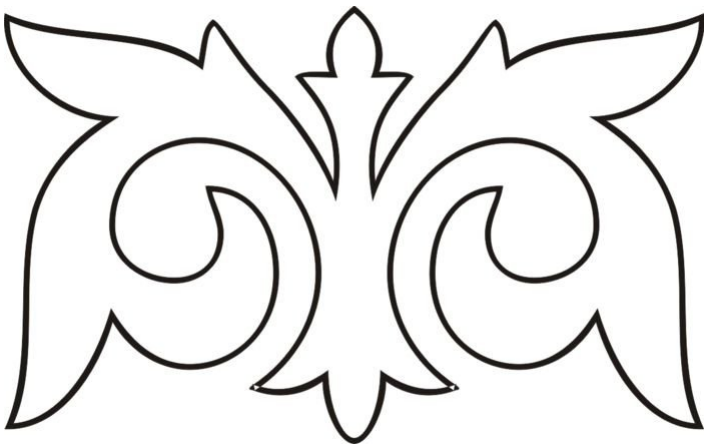
[10] Witt, E. (1956). Die Unterringer der freien Lieschen Rings. *Math. Z., 64*, 195–216.

[11] Mikhalev, A.A. (1985). Podalgebry svobodnykh tsvetnykh superalgebr Li [Subalgebras of free colored Lie superalgebras]. *Mat. Zametki — Matematicheskie Zametki, 37*(5), 653–661 [in Russian].

[12] Shtern, A.S. (1986). Svobodnye superalgebry Li [Free Lie superalgebras]. *Sibirsk. Mat. Zh. — Siberian Math. Journal, 27*(1), 170–174 [in Russian].

[13] Mutalip, R., Naurazbekova, A., Umirbaev, U. (2022). Automorphisms of free braided associative algebras in two variables. *Communications in Algebra, 502*, 848–860

Cryptology



CRYPTOGRAPHIC PROTOCOL OF VERIFIABLY ENCRYPTED SIGNATURE WITH POSSIBILITY OF VERIFICATION AFTER A SPECIFIED TIME

R.M. Ospanov, Ye.N. Seitkulov, B.B. Yergaliyeva,

K.A. Utebayev, S.K. Atanov

L.N.Gumilyov Eurasian National University, Astana, Kazakhstan

Almaty branch of the National Research Nuclear University MEPhI

E-mail: ospanovrm@gmail.com

Abstract

In this paper, we propose a new cryptographic protocol for a verifiably encrypted signature with possibility of verification after a specified time based on the post-quantum cryptographic algorithm for a hash-based digital signature, $TANBA\text{-}SPHINCS^+$.

The protocol describes the interaction of three participants. The first participant is the sender of the signed message (hereinafter referred to as the Sender). The second participant is the recipient of the message who verifies the signature (hereinafter referred to as the Receiver). The third participant is an adjudicator with the ability to encrypt for a specified time (hereinafter referred to as the Adjudicator). The protocol is designed to solve the following problem. Let M be a message. At some point in time T, the Sender wants to send the Receiver a signed message M so that the Receiver can verify the signature no earlier than a future point in time $T + \delta$ specified by the Sender.

Step-by-step description of the protocol.

The formation of a key pair and signature (steps 1 and 2) correspond to the $TANBA\text{-}SPHINCS^+$ post-quantum signature algorithm.

1) The Sender, using some cryptographically strong pseudorandom number generator, obtains the private key $sk = sk_{seed} \parallel sk_{prf} \parallel pk_{seed} \parallel pk_{root}$ and the public key $pk = pk_{seed} \parallel pk_{root}$.

2) Then the Sender forms a signature $\sigma = R \parallel \sigma_{FORS} \parallel \sigma_{HT}$, where

$$R = PRF_{msg}(sk_{prf}, opt, M)$$

is an n-bit randomization string, $PRF_{msg} : \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^* \to \{0,1\}^n$ is a pseudorandom function, opt is some additional random n-bit value, σ_{FORS} is the $FORS$ signature, and σ_{HT} is the hypertree signature defined using R.

3) Next, the Sender requests the Adjudicator for the Adjudicator's public key apk, indicating the time $T + \delta$.

4) Upon receiving the request, the Adjudicator generates the public key apk according to the $ECTLC$ cryptographic protocol and sends it to the Sender.

5) Upon receiving the Adjudicator's public key apk, the Sender generates an encrypted signature $\sigma_{ves} = E_{apk}(R) \parallel \sigma_{FORS} \parallel \sigma_{HT}$, where $E_{apk}(R)$ is the value R from the original signature encrypted with theAdjudicator's public key according to the $ECTLC$ cryptographic protocol.

6) The Sender sends message M with the encrypted signature σ_{ves} to the Recipient.

7) Upon receiving message M with encrypted signature σ_{ves}, the Recipient requests the Adjudicator to provide the Adjudicator's private key ask.

8) Upon receiving the request, the Adjudicator checks the time. If the current time has already reached time $T + \delta$, the Adjudicator generates the private key ask according to the cryptographic protocol $ECTLC$ and sends it to the Recipient. If the current time has not yet reached time $T + \delta$, the Adjudicator rejects the request and sends the Recipient a message that signature verification is not available until the specified time.

9) Upon receiving a refusal from the Adjudicator, the Recipient waits for the specified time, upon reaching which it resends the request to the Adjudicator. Having received the Adjudicator's private key ask, the Recipient calculates $R = D_{ask}(E_{apk}(R))$ - the original value R decrypted using the Adjudicator's private key from the original signature according to the $ECTLC$ cryptographic protocol.

10) Having decrypted the original value R, the Recipient verifies the received signature $\sigma = R \parallel \sigma_{FORS} \parallel \sigma_{HT}$ according to the $TANBA\text{-}SPHINCS^{+}$ post-quantum signature algorithm.

Acknowledgments. *This research was funded by the Ministry of Science and Higher Education of the Republic of Kazakhstan, grant number AP23486901.*

References

[1] Ospanov R.M., Seitkulov Ye.N., Yergaliyeva B.B., Utebayev K.A., and Atanov S.K. 2025. "$TANBA\text{-}SPHINCS^{+}$ - post-quantum cryptographic hash-based digital signature algorithm." Bulletin of Abai KazNPU. Series of Physical and Mathematical Sciences 89 (1). Almaty, Kazakhstan. https://doi.org/10.51889/2959-5894.2025.89.1.020.

[2] Kang, Bao Yuan. "New Types of Verifiably Encrypted Signature Schemes." Advanced Materials Research 490–495 (March 1, 2012): 914–918. https://doi.org/10.4028/www.scientific.net/amr.490-495.914.

[3] Hanser, Christian, Max Rabkin, and Dominique Schröder. "Verifiably Encrypted Signatures: Security Revisited and a New Construction." In Lecture Notes in Computer Science, 146–164, 2015. https://doi.org/10.1007/978-3-319-24174-6_8.

[4] Lu, Xiuhua, Wei Yin, and Pingyuan Zhang. "Lattice-Based Verifiably Encrypted Signature Scheme Without Gaussian Sampling for Privacy Protection in Blockchain." Sustainability 14, no. 21 (October 31, 2022): 14225. https://doi.org/10.3390/su142114225.

[5] Aumasson, et al. "$SPHINCS^{+}$ – Submission to the 3rd round of the NIST post-quantum project." 10 June 2022.

[6] Bernstein, Daniel J., Andreas Hülsing, Stefan Kölbl, Ruben Niederhagen, Joost Rijneveld, Peter Schwabe. "The $SPHINCS^{+}$ Signature Framework." CCS, 23 September 2019.

[7] National Institute of Standards and Technology (2024) Stateless Hash-Based Digital Signature Standard. (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publications (FIPS) NIST FIPS 205. https://doi.org/10.6028/NIST.FIPS.205.

[8] Kiktenko, E., Bulychev, A., Karagodin, P., Pozhar, N., Anufriev, M., Fedorov, A. "$Sphincs^{+}$ postquantum digital signature scheme with streebog hash function." AIP Conference Proceedings. vol. 2241, p. 020014. AIP Publishing LLC, 2020.

[9] Sim, M., Eum, S., Song, G., Kwon, H., Jang, K., Kim, H., Kim, H., Yang, Y., Kim, W., Lee, W.K., et al. "K-$XMSS$ and K-$SPHINCS^{+}$: Hash based signatures with korean cryptography algorithms." Cryptology ePrint Archive, 2022, https://eprint.iacr.org/2022/152.pdf.

[10] Tasmagambetov, Olzhas, Yerzhan Seitkulov, Ruslan Ospanov, and Banu Yergaliyeva. "Fault-tolerant Backup Storage System for Confidential Data in Distributed Servers." TELKOMNIKA (Telecommunication Computing Electronics and Control) 21, no. 5 October, 2023): 1030. https://doi.org/10.12928/telkomnika.v21i5.25305.

Reversible Polynomials

Kerimbayev R.K.

Al-Farabi Kazakh National University

E-mail: ker_im@mail.ru

Abstract

A commutative ring that is a K-algebra over $\mathbb{Q}$, and $K[x]$ is the ring of polynomials in one variable. For a polynomial $f(x) \in K[x]$, if there exists a polynomial $g(x)$ such that $f(x) \cdot g(x) = 1$, then $f(x)^{-1}$ is called the inverse of the polynomial $f(x)$ in the ring $K[x]$, and is given by the polynomial $g(x)$.

Proposition

For the polynomial $f(x)$ to be invertible in the ring $K[x]$, its constant coefficient must be invertible in the ring K, and the remaining coefficients must be nilpotent in the ring K. This is both a necessary and sufficient condition.

The proof of the theorem is given in the book by Atiyah-Macdonald [1].

If for a polynomial $f(x)$, there exists a polynomial $h(x)$ such that

$$f(h(x)) = x = h(f(x)),$$

then the polynomial $f(x)$ is said to be invertible by composition. We denote the inverse as $f^{-1}(x) = h(x)$.

Theorem

For a polynomial $f(x) \in K[x]$ to be invertible by composition, its derivative $f'(x)$ must be invertible in the ring $K[x]$. This is both a necessary and sufficient condition.

Proposition

Let the polynomial $f(x) = x + ax^n \in K[x]$, where $a^m = 0$. Then

$$\begin{aligned} f^{-1}(x) = x - ax^n + \frac{n}{1}\binom{2n-1}{0}a^2x^{2n-1} - \frac{n}{2}\binom{3n-1}{1}a^3x^{3n-2} \\ + \frac{n}{3}\binom{4n-1}{2}a^4x^{4n-3} + (-1)^i\frac{n}{i-1}\binom{in-1}{i-2}a^ix^{in-i+1} + \cdots \\ + (-1)^{m-1}\frac{n}{m-2}\binom{(m-1)n-1}{m-3}a^{m-1}x^{(m-1)(n-1)+1} \end{aligned} \tag{5}$$

The proof of the theorem and the sentence is provided in the work [2]

Cryptosystem

We hide m and $f^{-1}(x)$ where for which $a^m = 0$ and expand the function $f(x) = x + ax^n$.The polynomial $f(x)$ is distributed as the public key. All symbols are numbered with elements from the ring $\mathbb{Z}_{a^m}$. Thus, we encrypt the given word by assigning corresponding numbers to it. This is done using the polynomial $f^{-1}(x)$. The resulting numbers are then replaced back with letters. As a result, we obtain an encrypted word, which is sent to the receiver. The receiver decrypts the numbers of the letters using the polynomial $f(x)$, and then replaces the numbers with the corresponding letters, thereby determining the sent word.

This research was funded by the Science Committee of the Ministry of Education and Science of the Republic of Kazakhstan within the framework of the grant project No. AP19679799.

References

[1] Atiyah, M., Macdonald, I. *Introduction to Commutative Algebra*. Moscow: Mir, 1972.

[2] Kerimbayev, R.K., Akhmetov, Z.A. *Invertible Polynomials*, Bulletin of Al-Farabi Kazakh National University, Series on Mathematics, Mechanics, and Informatics.

LOGICAL ANALYSIS OF THE ADVANCED ENCRYPTION STANDARD (RIJNDAEL) ENCRYPTION ALGORITHM

A.V.KABULOV, M.SAYMANOV, M.A.BERDIMURODOV

Department of Information security, National University of Uzbekistan, Tashkent 100174, Uzbekistan;,
School of Mathematics, New Uzbekistan University, Tashkent 100011, Uzbekistan;,

Department of Modern information and communication, International Islamic Academy of Uzbekistan, Tashkent 100011, Uzbekistan;,

E-mail: islambeksaymanov@gmail.com

Abstract

In this article, the Rijndael algorithm is tested for compliance with general cryptographic requirements and mathematical models are built on different bases for each mapping in the algorithm. Algebraic cryptanalysis of the Advanced Encryption Standard (AES) cryptographic algorithm was carried out based on these established mathematical models. Based on optimized mathematical models, a reduction of new variables in algebraic cryptanalysis was achieved, which made it possible to bring algebraic cryptanalysis to the 6th round. At the same time, we analyzed the algebraic nonlinearity after each round and the number of elementary conjunctions in the equation based on the functions representing each mapping, leading it to a system of equations and specified in different bases. Methods for reducing the number of elementary conjunctions and effectively solving systems of Boolean equations by introducing negation into nonlinear algebraic normal forms are considered. Therefore, this article has developed: optimized mathematical models of modern symmetric encryption algorithms based on algebraic cryptanalysis methods; logical methods for assessing general cryptographic requirements based on created mathematical models of modern symmetric encryption algorithms; algorithms for creating and solving systems of Boolean equations on various bases based on mathematical models of modern symmetric encryption algorithms and assessing their complexity; criteria and algorithms for reducing mappings in the AES symmetric block encryption algorithm to functions on different bases. The article also formulates and discusses in detail such tasks as conducting algebraic cryptanalysis based on the developed optimized mathematical models.

Theorem 1. [2] *The value of the dependence of each bit of the linear mapping MixColumns on the values of the input bits is equal to the values 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5. , 5 , 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5 , 5 , 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5 , 5 , 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5 , 7 , 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5.*

Theorem 2. [2] *The dependence of each bit included in the linear transformation MixColumns on the values of the output bits is equal to the values 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5 , 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 5 , 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11 , 5, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5 , 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5 , 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5.*

Conclusions. Based on the generalized Zhegalkin polynomial and generalized and grouped Zhegalkin polynomial models, the article presents the results of algebraic cryptanalysis based on the evaluation of the encryption algorithms of the modern AES symmetric encryption algorithm for compliance with general cryptographic requirements, etc. According to the analysis, the AES encryption algorithm with a number of rounds of 6 and above turns out to be practically resistant to the method of algebraic cryptanalysis. Therefore, in the article: Mathematical models optimized for mappings to the AES symmetric encryption algorithm are developed and an assessment of general cryptographic requirements is presented. MixColums' study of the AES encryption algorithm presents and proves two statements about bit dependency. Methods and algorithms for optimizing statements of Boolean equations in the form of the Zhegalkin polynomial have been developed. The stages of solving systems of Boolean equations in the form of the Zhegalkin polynomial are given. Software was created that calculates the general cryptographic parameters of mappings in the AES-128 standard and three different models were built, optimized using the software.

References

[1] Courtois, Nicolas T., and Josef Pieprzyk. "Cryptanalysis of Block Ciphers with Overdefined Systems of Equations." Advances in Cryptology – ASIACRYPT 2002, edited by Yuliang Zheng, vol. 2501, Springer, 2002, pp. 267–287. Lecture Notes in Computer Science. https://doi.org/10.1007/3-540-36178-2_19.

[2] Courtois, Nicolas T., et al. Did Filiol Break AES? Cryptology ePrint Archive, Report 2003/022, Feb. 2003. http://eprint.iacr.org/2003/022/

[3] Courtois, N. T., The Inverse S-Box, Non-linear Polynomial Relations and Cryptanalysis of Block Ciphers, AES 4 Conference, Lecture Notes in Computer Science, vol. 3373, Springer, 2005, 170–188.

[4] Courtois, N. T. and Goubin, L., An Algebraic Masking Method to Protect AES Against Power Attacks, Technical Report, Axalto Crypto Research & PRiSM Versailles University, 2005. https://eprint.iacr.org/2005/204

[5] Courtois, N. T. and Pieprzyk, J., eXtended Sparse Linearization (XSL) Attack on AES, Unpublished manuscript, Cryptology ePrint Archive, Report 2002/044. https://eprint.iacr.org/2002/044

The Potential of BAN Logic in the Formal Analysis of Elliptic Curve Cryptography Protocols

B. Tashtai, A.A. Konyrkhanova and Nurlan D. Markhabatov

L.N. Gumilyov Eurasian National University

E-mail: 93bahti93@gmail.com, markhabatov@gmail.com

Abstract

BAN logic (Burrows-Abadi-Needham logic)[1] is a powerful formal framework for reasoning about security, authenticity, and trust within cryptographic protocols. In the realm of elliptic curve cryptography (ECC)-particularly protocols based on X25519 (Diffie-Hellman over Curve25519), Ed25519 (digital signatures), and hybrid constructions such as X3DH used in the Signal Protocol-BAN logic offers a structured method for:

i) Formalizing participants beliefs about key authenticity and freshness;

ii) Identifying implicit assumptions of security, such as trust in public key distribution mechanisms;

iii) Proving that each protocol step conveys sufficient guarantees for confidentiality, authenticity, and integrity;

iv) Detecting potential vulnerabilities such as man-in-the-middle attacks, replay attacks, or key compromise scenarios.

BAN logic is especially relevant for analyzing modern cryptographic schemes that rely on dynamic key generation, such as the Double Ratchet algorithm or OPAQUE, where symmetric and elliptic curve primitives are combined. Thus, BAN logic serves not only as a verification tool but also as an essential methodological component in the secure design and analysis of ECC-based communication protocols.

Acknowledgements. *The study was partially supported by the Scientific Committee for Education and Science of the Republic of Kazakhstan (AP19677451)*

References

[1] Burrows, M., Abad, M., & Needham, R. M. (1989). A Logic of Authentication. Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences, 426(1871), 233–271. http://www.jstor.org/stable/2398342

Machine Learning in Cryptography: Historical Progression, Innovations, and Emerging Directions (1995–2025)

Jubatkanov K. and Tanirbergenov A.Z.

L.N. Gumilyov Eurasian National University

E-mail: kuanysh595@gmail.com

Abstract

Over the past three decades, the incorporation of machine learning (ML) into cryptographic research and practice has changed, demonstrating a dynamic interaction between algorithmic development, theoretical investigation, and practical application. Four significant periods are covered in this thesis: the formative years (1995–2000), the development of neural cryptography (2000–2010), the growth of adversarial and privacy-preserving applications (2010–2020), and the present deep cryptanalytic innovation phase (2020–2025).

1995–2000 – Laying the Theoretical Groundwork When machine learning was still in its early stages in the late 1990s, research focused on compact rule-based models, interpretability, and generalization under noise. Important theoretical developments that would later facilitate ML's integration into cryptographic contexts surfaced, even though cryptographic systems functioned independently of ML at this point.

Statistical query models and noise-tolerant learning algorithms, which offered a framework for handling noisy or poor data—conditions typical in secure communications—are noteworthy innovations from this era. Early research on neural networks, perceptrons, and tree-based learning techniques helped define how machine learning (ML) systems could continue to function in unpredictable or hostile situations.

In addition, integrative models like FLARE (Framework for Learning and Reasoning) foreshadowed future hybrid ML-cryptographic models by attempting to combine logical reasoning and inductive learning. Even though real-world uses In addition, integrative models like FLARE (Framework for Learning and Reasoning) foreshadowed future hybrid ML-cryptographic models by attempting to combine logical reasoning and inductive learning. The theoretical tools created during this time period established the fundamental framework for subsequent advancements in neural cryptography, adaptive encryption, and pattern-based cryptanalysis, despite the fact that there were few practical applications in cryptography. [4], [5]

2000–2010 – The Rise of Neural Cryptography

Significant cooperation between machine learning and cryptography started in the years 2000–2010. The development of neural cryptography, in which academics suggested establishing cryptographic keys using mutual learning processes amongst neural networks, is what most prominently defines this era.

Tree Parity Machines (TPMs), a method for synchronizing two neural networks over a public channel to generate a shared secret key, were first presented in studies by Kinzel, Kanter, and others. These systems were computationally efficient and resistant to passive eavesdropping because they made use of the adaptive, stochastic behavior of neural networks to thwart traditional cryptanalytic attempts.

Simultaneously, cryptographic techniques started utilizing probabilistic and statistical learning models, like the Fisher-Schrödinger framework, to modify encryption parameters

according to the characteristics of the data. Understanding how parity functions, which are important for cryptographic hardness, could withstand learning in the presence of adversarial noise was made possible by research on noise-tolerant learning.

This period, while still exploratory, marked a move toward data-driven cryptographic protocols, paving the way for the following ten years of automation, intelligent key management, and security systems based on hybrid learning. [1], [2], [3]

2010–2020 – Privacy-Preserving Computation and Automated Cryptanalysis

Machine learning developed into a potent instrument for both protecting and breaching cryptographic systems between 2010 and 2020. The broad use of privacy-preserving machine learning (PPML) techniques this decade allowed for the analysis of encrypted data without the need to decrypt it, which was a significant privacy advance in industries like healthcare and finance.

One of the main advances was the incorporation of homomorphic encryption (HE) into statistical machine learning models, which enabled the use of encrypted datasets by algorithms such as Naïve Bayes classifiers and decision trees. The development of open-source tools to facilitate encrypted machine learning pipelines made it possible to implement privacy-preserving analytics in real-world scenarios.

Simultaneously, automatic cryptanalysis was using machine learning more and more. High-accuracy detection of cryptographic methods like RSA, AES, or DES could be achieved by tools trained on built binaries, speeding up malware analysis and reverse engineering. Additionally, deep learning models were utilized for ransomware detection, using adversarial training to improve classifier resistance and learning dynamic file activity patterns to detect threats.

All things considered, this decade demonstrated ML's potential to scale cryptographic analysis, automate vulnerability identification, and protect data privacy—even in hostile or resource-constrained environments. HE's high processing costs and vulnerability to adversarial cases, however, continued to be significant obstacles. [6], [7], [8], [9]

2020–2025 – Deep Integration and Post-Quantum Frontiers

Particularly in light of post-quantum security risks, the current era (2020–2025) marks a significant turning point where machine learning is actively redesigning cryptographic systems rather than merely improving them.

One significant development is the use of transformer-based models in lattice cryptanalysis to tackle challenging issues such as Learning With Errors (LWE), which forms the basis of post-quantum encryption techniques. Transformers and angle embeddings are used by well-known tools like SALSA and SALSA FRESCA to increase the effectiveness and scale of attacks on high-dimensional cryptographic instances, which were previously thought to be computationally impossible.

Concurrently, the combination of hybrid homomorphic encryption and federated learning has produced frameworks such as GuardML, which allow for privacy-preserving machine learning on devices with restricted resources. These systems balance utility, efficiency, and confidentiality by performing secure computations on sensitive data (such as medical information) without ever decrypting it.

Gradient-based adversarial simulations have also emerged at this time, challenging earlier theories regarding the limitations of machine learning in cryptanalysis. These simulations demonstrate how contemporary machine learning algorithms can accurately mimic or even surpass traditional sample-based cryptanalytic techniques.

These developments highlight major ethical issues even as they show how much ML can innovate in the field of cryptography. Dual-use risks—where machine learning techniques intended to improve security could be used to compromise it—emphasize the necessity of international cooperation, responsible governance, and safe design standards. [10], [11], [12], [13], [14] , [15]

In conclusion

Between 1995 and 2025, machine learning in cryptography saw a significant transformation, moving from discrete theoretical advancements to extensive, useful integration across security systems. With the introduction of neural cryptography in the 2000s, privacy-preserving and automated analysis techniques in the 2010s, transformer-based cryptanalysis and post-quantum applications in the current era, and foundational learning models in the late 1990s, each decade has brought a new layer of innovation.

The evolution of cryptographic difficulties from static, rule-based protection to adaptive, intelligent, and data-driven security frameworks is demonstrated by this development, which also shows the growing strength and sophistication of ML tools. In addition to securely analyzing encrypted data, today's systems use machine learning (ML) to reveal minute flaws in algorithms that were previously thought to be impenetrable. But this progress also brings risk and complexity. Every advancement in safe computation has a parallel application in cryptographic attacks due to machine learning's dual-use nature. For the upcoming generation of cryptographic systems, ensuring ethical use, protecting ML pipelines from hostile attacks, and controlling computing efficiency continue to be major concerns.

In the end, the combination of cryptography with machine learning has revolutionary potential for applications in digital governance, healthcare, and finance in addition to information security. To guarantee that this potent nexus is utilized to safeguard rather than jeopardize the integrity of our digital environment going forward, a cooperative, interdisciplinary method is necessary.

References

[1] Kinzel, W., & Kanter, I. (2002). Neural cryptography. *arXiv preprint* arXiv:cond-mat/0208453.

[2] Rosen-Zvi, M., Klein, E., Kanter, I., & Kinzel, W. (2002). Mutual learning in a tree parity machine and its application to cryptography. *arXiv preprint* arXiv:cond-mat/0209234.

[3] Ruttor, A., Kinzel, W., & Kanter, I. (2005). Neural cryptography with queries. *arXiv preprint* arXiv:cond-mat/0411374.

[4] Venkatesan, R. C. (2007). Statistical cryptography using a Fisher-Schrödinger model. *arXiv preprint* arXiv:cond-mat/0701319.

[5] Blum, A., Kalai, A., & Wasserman, H. (2000). Noise-tolerant learning, the parity problem, and the statistical query model. *arXiv preprint* arXiv:cs/0010022.

[6] Aslett, L. J. M., Esperança, P. M., & Holmes, C. C. (2015). Encrypted statistical machine learning: New privacy-preserving methods. *arXiv preprint* arXiv:1508.06845.

[7] Hosfelt, D. D. (2015). Automated detection and classification of cryptographic algorithms in binary programs through machine learning. *arXiv preprint* arXiv:1503.01186.

[8] Aslett, L. J. M., Esperança, P. M., & Holmes, C. C. (2015). A review of homomorphic encryption and software tools for encrypted statistical machine learning. *arXiv preprint* arXiv:1508.06574.

[9] Yang, C.-Y., & Sahita, R. (2020). Towards a resilient machine learning classifier: A case study of ransomware detection. *arXiv preprint* arXiv:2003.06428.

[10] Frimpong, E., Nguyen, K., Budzys, M., Khan, T., & Michalas, A. (2024). GuardML: Efficient privacy-preserving machine learning services through hybrid homomorphic encryption. *arXiv preprint* arXiv:2401.14840.

[11] Wenger, E., Chen, M., Charton, F., & Lauter, K. (2023). SALSA: Attacking lattice cryptography with transformers. *arXiv preprint* arXiv:2207.04785.

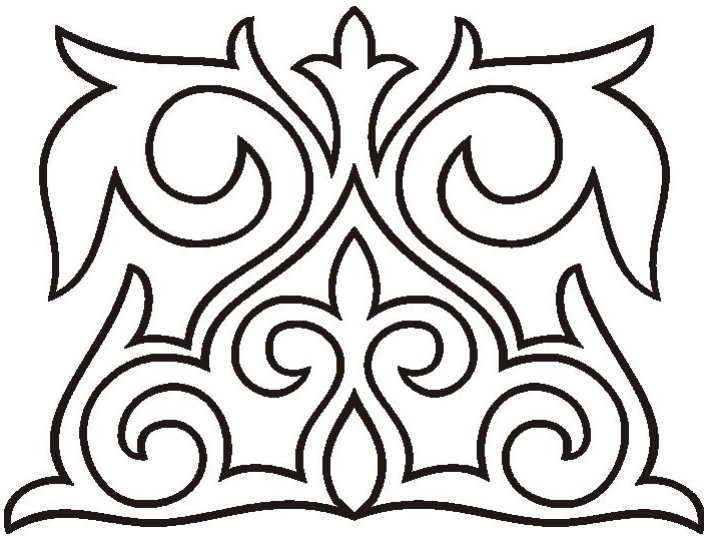
[12] Stevens, S., Wenger, E., Li, C., Nolte, N., Saxena, E., Charton, F., & Lauter, K. (2024). SALSA FRESCA: Angular embeddings and pre-training for ML attacks on learning with errors. *arXiv preprint* arXiv:2402.01082.

[13] Shafran, A., Malach, E., Ristenpart, T., Segev, G., & Tessaro, S. (2024). Is ML-based cryptanalysis inherently limited? Simulating cryptographic adversaries via gradient-based methods. *IACR Cryptology ePrint Archive*, 2024/1126.

[14] Kim, B. D., Vasudevan, V. A., Woo, J., Cohen, A., D'Oliveira, R. G. L., Stahlbuhk, T., & Médard, M. (2023). CRYPTO-MINE: Cryptanalysis via mutual information neural estimation. *arXiv preprint* arXiv:2309.08019.

[15] Shafique, A., Mehmood, A., Alawida, M., Elhadef, M., & Rehman, M. U. (2024). A fusion of machine learning and cryptography for fast data encryption through the encoding of high and moderate plaintext information blocks. *Multimedia Tools and Applications*.

Applied Logic and Artificial Intelligence



Spatiotemporal logic-based modeling of behavioral patterns for autism spectrum disorder detection

Aizat Amirbay, Ayagoz Mukhanova

Department of Information Systems, L. N. Gumilyov Eurasian National University

E-mail: amirbay.aiz@gmail.com

Abstract

This study presents a spatiotemporal logic-based approach for detecting Autism Spectrum Disorder by analyzing structured behavioral patterns. Facial expressions, body posture, and hand movements are quantified using 1639 features extracted from video data via MediaPipe models. These features, including the Mouth Aspect Ratio and movement energy dynamics, provide a formalized representation of behavior suitable for logical reasoning and computational analysis. A hybrid CNN-LSTM model is employed to capture spatial characteristics and temporal dependencies in the data, achieving up to 90% accuracy and an AUC exceeding 0.90. Experimental results reveal distinct behavioral differences between neurotypical children and those with ASD, supporting the model's diagnostic potential. The proposed method bridges deep learning and applied logic, enabling interpretable and scalable ASD screening within intelligent decision support systems.

Assessment of River Surface Water Quality Using an ANFIS Neuro-Fuzzy Model

Elaman Darkhanuly Sarsembinov, La Lira Lvovna

Astana IT University, Astana, Kazakhstan

Eurasian National University, Astana, Kazakhstan

E-mail: elaman.sarsembinov@example.com, la.lira@example.com

Abstract

This study presents the use of an Adaptive Neuro-Fuzzy Inference System (ANFIS) to assess river surface water quality based on key indicators such as dissolved oxygen, BOD_5, ammonia, total phosphorus, and boron. A synthetic dataset was generated to simulate typical pollution and purification scenarios. The ANFIS model was implemented with Gaussian membership functions and trained using supervised learning in PyTorch. The system achieved approximately 90% accuracy after rounding outputs to water quality classes. The model demonstrates strong interpretability and smooth decision boundaries. This approach shows promise for ecological monitoring and can be expanded with real-world data and additional water quality parameters.

APPLICATION OF KNOWLEDGE GRAPHS TO SUPPORT THE EDUCATIONAL PROCESS IN A UNIVERSITY

RAMAZANOVA V. S.

L.N. GUMILYOV EURASIAN NATIONAL UNIVERSITY

E-mail: ramazanovavs@gmail.com

Abstract

The research work is devoted to the integration of multilingual skills from various sources into a single heterogeneous knowledge graph for personalized educational recommendations. The relevance of the topic is due to the insufficient study of methods for combining multilingual data from educational programs, vacancies and online courses (MOOC). [1]

The paper proposes a methodology for integrating semantically similar multilingual skills into a heterogeneous knowledge graph model and develops recommender models based on heterogeneous GNN. The dataset includes information from three subject areas: a catalog of elective disciplines, vacancies and online courses. Three embedding models (Word2Vec, BERT, SBERT) were compared, with SBERT being retrained on skill paraphrases in Kazakh, Russian and English. For integration, embeddings of the retrained SBERT model and hierarchical clustering were used, which improved the separation of mastered and unmastered skills. [2]

To train the GNN, training samples were organized, where the edge weights were normalized as the number of paths between the user's competence and the course by metapaths. Two models based on HGT and HAN layers were proposed to predict continuous edge labels. Experimental results showed the effectiveness of retrained SBERT embeddings and clustering for multilingual skills, as well as the advantage of the HGT-based recommendation model for course selection.

Acknowledgements. This research has been funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP22783030).

References

[1] Ramazanova, M. Sambetbayeva, S. Serikbayeva, Z. Sadirmekova and A. Yerimbetova, (2024) Development of a knowledge graph-based model for recommending MOOCs to supplement university educational programs in line with employer requirements, in IEEE Access, vol. 12, pp. 193313-193331, doi: 10.1109/ACCESS.2024.3519263.

[2] V.S. Ramazanova, A. S. Yerimbetova; M. A. Sambetbaeva; Zh. B. Sadirmekova; S. K. Serikbayeva Enhancing the Quality of Clustering Job Skills Through the Fine-Tuning of the Sentence Transformer Model. // 9th International Conference on Computer Science and Engineering (UBMK), Antalya, Turkiye, 2024, pp. 141-146, doi: 10.1109/UBMK63289.2024.10773449.

Revisiting Engagement Rate Heuristics for TikTok Influence Graphs: A UX-Driven Metric Optimization Approach

Nurzhas Abdikenov

Astana IT University

Dept. of Computer Science and Engineering

Astana 010000, Kazakhstan

E-mail: 242810@astanait.edu.kz

Abstract

The Engagement Rate (ER) is a common metric used to evaluate user influence on social media, but current ER formulas often apply arbitrary weights to interactions like likes, comments, shares, and saves. These weights rarely reflect platform-specific user behavior or effort required to perform each action. This study proposes a revised ER formula tailored to TikTok, where actions such as commenting and sharing involve greater interaction friction than liking or saving. Using a scraped dataset of public TikTok posts from Kazakhstan-based users, the standard ER formulation with the UX-informed variant was compared. A user-user graph was constructed based on hashtag overlap and weighted by average ER, with visual analysis performed in Gephi. While the Louvain community detection algorithm was initially applied, it produced limited interpretability, pointing to the need for additional content-based clustering. The revised ER led to significant shifts in user ranking and centrality, supporting the argument that engagement metrics should be behavior-sensitive and context-aware.

ATP Systems as Tools for Reasoning with Horn Disjunctions in Logic of Computable Structures

Arman K. Musabekov, K. Jetpisov, J.A. Tussupov and Nurlan D. Markhabatov

L.N. Gumilyov Eurasian National University

E-mail: 87710003264a@gmail.com, markhabatov@gmail.com

Abstract

This study explores the capabilities and limitations of modern Automated Theorem Proving (ATP)[1] systems when working with formulas in the form of Horn disjunctions. Special emphasis is placed on Prover9, Vampire, Lean, Coq, and Isabelle as representative tools implementing various proof paradigms, from first-order resolution to dependent type theory. Horn clauses, which play a central role in first-order logic, exhibit desirable properties for automation, such as linear-time satisfiability checking and suitability for logic programming and model checking. This paper analyzes how Horn disjunctions are leveraged in the construction and verification of computable and pseudofinite models. A comparative performance and expressiveness analysis of different ATP systems is provided, with concrete formalization examples. The study also addresses translation techniques for encoding logical assertions into ATP-friendly formats and discusses the potential of Horn-based encodings to optimize proofs in model-theoretic frameworks.

Acknowledgements. *The study was partially supported by the Scientific Committee for Education and Science of the Republic of Kazakhstan (AP19677451)*

References

[1] Sutcliffe, G. (2002). Automated theorem proving: Theory and practice [Review of the book Automated Theorem Proving: Theory and Practice, by M. Newborn]. AI Magazine, 23(1). https://doi.org/10.1609/aimag.v23i1.1617

Application of Machine Learning Techniques for Identifying Heart Disease Risk Factors

Natalya Maxutova, Jamalbek Tussupov

Department of Information Systems, L. N. Gumilyov Eurasian National University

E-mail: natalya.maxutova@gmail.com

Abstract

This study investigates the application of machine learning techniques for identifying risk factors associated with cardiovascular diseases through structured and explainable modeling. Two algorithms were evaluated, XGBoost, known for its rule-based gradient boosting logic on tabular data, and a convolutional neural network (CNN) designed to capture feature interactions in non-linear form. Emphasis is placed on the interpretability and diagnostic reasoning capabilities of the models in relation to critical biomarkers such as cholesterol, ferritin, homocysteine, and AST. Evaluation using MSE, R^2, AIC, and BIC metrics highlights the logical consistency and superior performance of XGBoost in extracting structured insights from clinical features. The CNN model, while initially promising, exhibited overfitting and lower generalization on validation data, underlining the challenges of applying deep models to sparse or structured datasets. The findings emphasize the role of logical model selection and feature-based reasoning in the development of AI-driven diagnostic tools for cardiovascular risk assessment.

Geoinformation approach to solving the problem of geometrically fair division of the Caspian Sea bottom between the Caspian states

Lawrence S.A., Rudenko V.M., Chelyapina O.I.

Russian State University of Tourism and Service

Moscow, Russian

E-mail: lawrencenko@gmail.com

Abstract

Since the Caspian Sea bottom is extremely rich in hydrocarbon resources, there is an urgent problem of dividing the Caspian Sea bottom between the five Caspian states for the development and production of oil and natural gas. In the report, we will give a final solution to this long-standing problem. It should be said right away that, according to the Convention on the Legal Status of the Caspian Sea (Aktau, 2018), the surface and waters of the Caspian are considered common for the ships of all Caspian states, so there is no practical task of dividing the surface of the Caspian. However, we will still find a (conditional) geometrically fair division of the Caspian surface, but not as an end in itself, but as an intermediate result, and the orthogonal projection (i.e. perpendicular to the surface of the sea) of the obtained division of the sea surface onto the sea bottom will give the desired division of the Caspian Sea bottom. The concept of geometric fairness is understood in the sense that a point on the sea surface belongs, for example, to Iran if and only if this point is closest to the coast of Iran. Thus, although the surface of the Caspian Sea plays an auxiliary role, we need an algorithm for a geometrically fair division of the sea surface between the five Caspian states. The report will present such an algorithm using the Voronoi-Thiessen polygon systems. The algorithm is implemented in the QGIS geoinformation system. The resulting division of the Caspian Sea is compared with the officially recognized one to date. It is indicated that although geometric fairness is basic, superstructure factors (such as economic, natural, financial and geopolitical) are no less important. The geoinformation approach proposed in the work can be applied to the division of any geoobjects.

Author Index

Zhailybaev, R.E. – p. 55