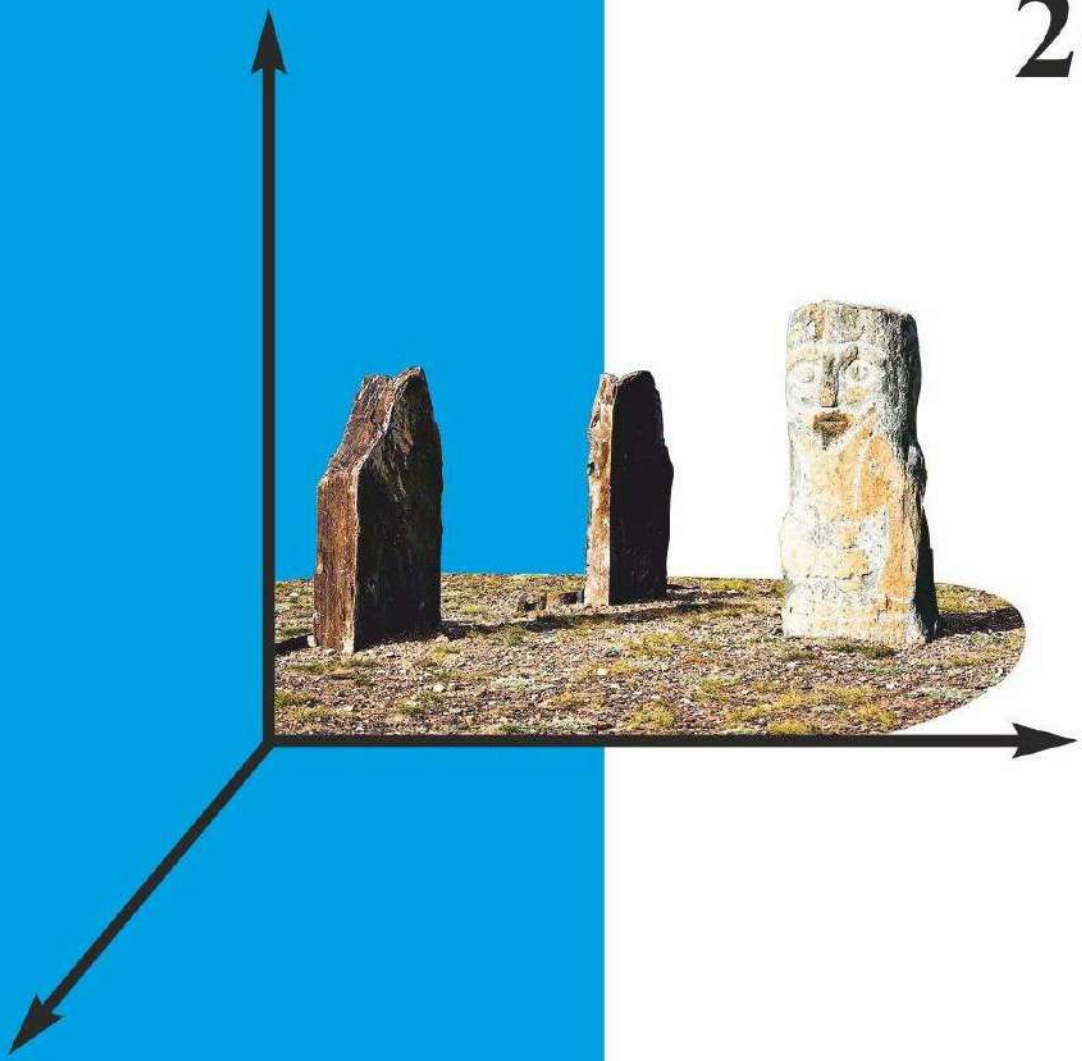
Model Theory and Algebra 2024



НОВОСИБИРСК
2024

Novosibirsk State Technical University

Model Theory and Algebra 2024

Collection of papers

edited by M. Shahryari and S. V. Sudoplatov

Novosibirsk
2024

UDC 512
M78

M78 **Model Theory and Algebra 2024**: Collection of papers / Edited by M. Shahryari, S. V. Sudoplatov. – Novosibirsk: NSTU Publisher, 2024. – 198 pp.

ISBN 978-5-7782-5285-1

The papers in this book are devoted to some problems of model theory and algebra.

UDC 512

ISBN 978-5-7782-5285-1

INTRODUCTION

Model Theory and Algebra 2024

The 16th International Summer School-Conference "Problems Allied to Model Theory and Universal Algebra" was held on 08–13 of July 2024 at Sobolev Institute of Mathematics and Novosibirsk State Technical University NETI. The School was organized by Algebra and Mathematical Logic Department of Novosibirsk State Technical University (NSTU NETI) and Sobolev Institute of Mathematics of Siberian Branch of Russian Academy of Sciences (IM SB RAS). The School was supported by Grant of International Mathematical Center in Akademgorodok. The school-conference included both online and in-person talks. At the school-conference, there were participants from Russia, Kazakhstan, Uzbekistan, Algeria, Canada, France, Hungary, Oman, Poland. They made 43 talks. Within the school-conference, the discussions on actual problems on Model Theory, Algebra and related subjects were held. Information about the conference is posted on the conference website https://erlagol.ru.

The Organizing Committee
of the School-Conference

Programme of 16th International Summer School-Conference "Problems Allied to Model Theory and Universal Algebra"

July 8, Monday

Chairperson S.V. Sudoplatov

8:55 – 9:00 Opening Ceremony

9:00 – 9:50 A.E. Mironov (Novosibirsk, Russia), BirkhoffTs algebraic conjecture on integrable billiards

10:00 – 10:50 M. Shahryari (Muscat, Oman), On conjugately separability of nilpotent subgroups and equational domains

11:00 – 11:30 G. Czédli (Szeged, Hungary), From Maltsev conditions to a duality theorem (online)

11:30 – 12:10 Coffee break

12:10 – 13:00 N.Kh. Kasymov (Tashkent, Uzbekistan), Computably separable algorithmic representations of universal algebras with finiteness conditions (online)

Chairperson B.Sh. Kulpeshov

15:00 – 15:50 B.P. Poizat (Lyon, France), Parameters in Algebraically Closed Fields (online)

15:50 – 16:30 Coffee break

16:30 – 17:00 A.A. Iwanow (Gliwice, Poland), Generic groups and the weak amalgamation property (online)

17:00 – 17:30 M.I. Bekenov (Astana, Kazakhstan), On model companions of some theories

17:30 – 18:00 N.D. Markhabatov (Astana, Kazakhstan), On approximations of pseudofinite theories

18:00 – 18:30 D.V. Solomatin (Omsk, Russia), Structure of semigroups admitting generalized outerplanar Cayley graphs (online)

July 9, Tuesday

Chairperson V.V. Verbovskiy

9:00 – 9:50 A.I. Stukachev (Novosibirsk, Russia), Structures on signatures of structures

10:00 – 10:50 N.L. Polyakov (Moscow, Russia), Ultrafilter extensions of infinitary functions: universal algebraic aspects

10:50 – 11:30 Coffee break

11:30 – 12:20 I.B. Kozhukhov (Moscow, Russia), Finiteness conditions in acts over semigroups

12:20 – 13:00 A.A. Stepanova, E.L. Efremov, S.G. Chekanov (Vladivostok, Russia), Pseudofinite polygons over Abelian groups

Chairperson M. Shahryari

15:00 – 15:40 E.V. Vassiliev (Corner Brook, Canada), Small closure in pairs of geometric structures

15:40 – 16:10 V.V. Verbovskiy (Almaty, Kazakhstan), On pure linear orderings of Morley o-rank 1 (joint with A. D. Yershigeshova)

16:10 – 16:30 Coffee break

16:30 – 17:00 I.A. Sakharov (Vladivostok, Russia), On possible degrees of semantic and syntactic rigidity of unars (online)

17:00 – 17:30 V.L. UsolTtsev (Volgograd, Russia), Semimodularity of the class of all congruence Ries algebras of an arbitrary fixed signature

17:30 – 18:00 A.R. Yeshkeyev, I.O. Tungushbayeva (Karaganda, Kazakhstan), Properties of the Jonsson spectrum and its class of model (online)

18:00 – 18:30 A.R. Yeshkeyev, A.K. Koshekova (Karaganda, Kazakhstan), Cosemanticity of Kaiser hulls of definable subsets of the semantic model of a fixed Jonsson theory (online)

18:30 – 19:00 A.R. Yeshkeyev, A.R. Yarullina (Karaganda, Kazakhstan), Jonsson existentially closed unars of expanded signature (online)

19:00 – 19:30 S.M. Amanbekov (Karaganda, Kazakhstan), On semantic Jonsson quasivariety of undirected graphs (online)

July 10, Wednesday

Free day

July 11, Thursday

Chairperson P.S. Kolesnikov

9:00 – 9:50 B.S. Baizhanov (Almaty, Kazakhstan), Expansion of a model of stable theory (online)

10:00 – 10:30 V.N. Zhelyabin (Novosibirsk, Russia), Simple and semisimple finite-dimensional Novikov algebras (online)

10:40 – 11:30 A.S. Zakharov, V.N. Zhelyabin (Novosibirsk, Russia), Simple finite-dimensional Novikov algebras over a field of prime characteristic

11:30 – 12:00 Coffee break

12:00 – 12:40 A.S. Monastyreva (Barnaul, Russia), Zero divisor graphs of a finite ring

Chairperson N.L. Polyakov

15:00 – 15:30 A,V, Kartashova (Volgograd, Russia), On lattices of topologies of commutative unary algebras

15:30 – 16:00 N.A. Shchuchkin (Volgograd, Russia), Ternary quasigroups and their applications in cryptography

16:00 – 16:30 Coffee break

16:30 – 17:00 V.A. Molchanov, R.A. Farakhutdinov (Saratov, Russia), Specific characterization of partially defined graph automata (online)

17:00 – 17:30 G.S. Suleymanova (Abakan, Russia), On centralizers of graph automorphisms of Chevalley algebras and their faithful enveloping algebras (online)

17:30 – 18:00 K. Tahri (Tlemcen, Algeria), Existence and Uniqueness Solution for Biharmonic Kirchhoff Equation with Singular Term (online)

July 12, Friday

Chairperson I.B. Kozhukhov

9:00 – 9:50 P.S. Kolesnikov (Novosibirsk, Russia), Dendriform splitting of varieties and the Dong Lemma

10:00 – 10:50 A.P. Pozhidaev (Novosibirsk, Russia), Pre-Lie Witt doubles

10:50 – 11:30 Coffee break

11:30 – 12:20 F.A. Dudkin (Novosibirsk, Russia), Universal equivalence of generalized Baumslag-Solitaire groups

12:30 – 13:00 H. Alhussein, P.S. Kolesnikov (Novosibirsk, Russia), Hochschild cohomology of the Weyl conformal algebra

Chairperson E.V. Vassiliev

15:00 – 15:30 A.V. Chekhonadskikh (Novosibirsk, Russia), Algebraic aspects of optimization in polynomial synthesis of automatic control systems

15:30 – 16:00 D.Yu. Emelyanov (Novosibirsk, Russia), Algebras of binary formulas for products of graphs

16:00 – 16:30 Coffee break

16:30 – 17:00 I.A. Emelyanenkov (Novosibirsk, Russia), A diagrammatic approach to the study of countable models of complete theories

17:00 – 17:30 S.B. Malyshev (Novosibirsk, Russia), Heritability of pregeometry types by composition relative to the original structures

17:30 – 18:00 A.V. Vaseneva (Novosibirsk, Russia), On ranks of equationality

18:00 – 18:30 A.S. Savin (Novosibirsk, Russia), Some spectra of spherical orderability of finite groups

July 13, Saturday

Chairperson A.A. Stepanova

9:00 – 9:50 B.Sh. Kulpeshov (Almaty, Kazakhstan), S.V. Sudoplatov (Novosibirsk, Russia), Variations of rigidity for ordered and strongly minimal theories

10:00 – 10:30 B.Sh. Kulpeshov (Almaty, Kazakhstan), In.I. Pavlyuk, S.V. Sudoplatov (Novosibirsk, Russia), Pseudo-countably-categorical theories

10:30 – 11:00 Coffee break

11:00 – 11:50 S.V. Sudoplatov (Novosibirsk, Russia), Forty years with Model Theory

11:50 Closing Ceremony

HOCHSCHILD COHOMOLOGY OF THE WEYL CONFORMAL ALGEBRA

H. Alhussein[1)2)], **P.S. Kolesnikov**[3)]

[1)]Novosibirsk State Technical University,
K.Marx avenue 20, Novosibirsk, 630073, Russia;
[2)]Higher School of Economics,
Myasnitskaya street 20, Moscow, 101000, Russia;
[3)]Sobolev Institute of Mathematics,
Acad. Koptyug avenue 4, Novosibirsk, 630090, Russia
e-mail: hassanalhussein2014@gmail.com, pavelsk77@gmail.com

1 Introduction

The notion of a conformal algebra appeared as a formal language for studying the singular part of the operator product expansion (OPE) in 2-dimensional conformal field theory (CFT) in mathematical physics (see, e.g., [9]). From the algebraic point of view, associative (or Lie) conformal algebras may be considered as morphisms from the corresponding operad As (or Lie) into the multicategory of modules over the polynomial algebra $H = \mathbb{C}[\partial]$ [3]. This observation shows us certain similarity between "ordinary" and conformal algebras: the first ones are morphisms form the same operads into the "ordinary" multicategory of linear spaces.

Definition 1. *A conformal algebra is a linear space C equipped with a linear operator $\partial : C \to C$ and a bilinear map $(\cdot_\lambda \cdot)$ from $C \times C$ to the space of polynomials $C[\lambda]$ in a formal variable λ such that*

$$(\partial u_\lambda v) = -\lambda(u_\lambda v), \quad (u_\lambda \partial v) = (\partial + \lambda)(u_\lambda v)$$

for all $u, v \in C$.

For every conformal algebra C, there exists an ordinary algebra $\mathcal{A} = \mathcal{A}(C)$ such that C can be embedded into the space of formal distributions

$\mathcal{A}[[z, z^{-1}]]$ in such a way that ∂u corresponds to the formal derivative $\partial_z u$ and

$$(u_\lambda v) = \operatorname*{Res}_{w=0} u(w)v(z)\exp\{\lambda(w-z)\}$$

for $u, v \in C$, see [10].

A natural universal property defines such an algebra $\mathcal{A}(C)$ in a unique (up to isomorphism) way. A conformal algebra C is said to be associative (or Lie) if so is its *coefficient algebra* $\mathcal{A}(C)$. An important role in the subsequent exposition is played by a subalgebra $\mathcal{A}_+(C)$ called *annihilation* algebra of C.

Example 1. *Let* $C = \mathbb{C}[\partial, x]$ *and*

$$u(\partial, x)_\lambda v(\partial, x) = u(-\lambda, x)v(\partial + \lambda, x + \lambda), \quad u, v \in C.$$

Then C *is an associative conformal algebra denoted* Cend_1*, its coefficient algebra* $\mathcal{A}(C)$ *is a localization of the first Weyl algebra:*

$$\mathcal{A}(\mathrm{Cend}_1) = \mathbb{C}\langle q, t, t^{-1} \mid qt - tq = 1\rangle.$$

Example 2. *The subspace* $x\mathbb{C}[\partial, x]$ *of* Cend_1 *is obviously a conformal subalgebra denoted* $\mathrm{Cend}_{x,1}$ *in [5]. We will shortly denote it by* $U(2)$*.*

Example 3. *An associative conformal algebra* C *with respect to the new bilinear operation*

$$[u_\lambda v] = (u_\lambda v) - (v_{-\partial-\lambda} u), \quad u, v \in C,$$

is a Lie conformal algebra denoted $C^{(-)}$*, its coefficient algebra is just the commutator Lie algebra of* $\mathcal{A}(C)$*.*

In particular, if $C = U(2)$ then the subspace $V = \mathbb{C}[\partial]x \subset C$ is a conformal subalgebra of $C^{(-)}$ since

$$[x_\lambda x] = x(x + \lambda) - x(x - \partial - \lambda) = \partial x + 2\lambda x.$$

This V is known as the Virasoro (Lie) conformal algebra, its coefficient algebra coincides with the Lie algebra of derivations of $\mathbb{C}[t, t^{-1}]$. The Virasoro conformal algebra V is the only exceptional simple finite Lie conformal algebra according to the classification in [7].

Thus, $V \subset U(2)^{(-)}$ and, moreover, $U(2)$ is generated by the elements of V as an associative conformal algebra. Hence, $U(2)$ is an associative enveloping conformal algebra of the Virasoro conformal algebra.

For every Lie conformal algebra L one can construct a series of universal enveloping associative conformal algebras corresponding to different associative locality functions on the generators [12].

For example, consider the Virasoro conformal algebra V described above. It is generated by a single element x. One may fix a natural number N and construct the associative conformal algebra $U(N)$ generated by the element x such that $\deg(x_\lambda x) < N$, and the commutation relations of V hold. Obviously, $U(1) = 0$; the algebra $U(2)$ is exactly the Weyl conformal algebra.

The next universal associative envelope $U(3)$ plays a special role in the representation theory of the Virasoro Lie conformal algebra V. Namely, let M be a finite irreducible module over V (all such modules were described in [6]). Then M is also a module over the associative conformal algebra $U(3)$. This is why $U(2)$ and $U(3)$ are emphasized among other universal envelopes: $U(2)$ is the minimal one which contains V, $U(3)$ is the minimal one with the universal property for finite irreducible representations. The subject of this note is to describe conformal cohomologies of $U(2)$ and $U(3)$ with coefficients in appropriate finite irreducible V-modules.

2 Conformal cohomologies

The starting point for studying cohomologies of conformal algebras is the paper [4] where the notions of basic and reduced complexes for (Lie or associative) conformal algebras with coefficients in a conformal (bi-)module were stated.

As in the case of ordinary algebras, the first cohomology group of the reduced conformal complex describes outer derivations of an algebra, the second cohomology group is in one-to-one correspondence with classes of equivalent extensions. In particular, the Virasoro Lie conformal algebra has 1-dimensional 2nd cohomology group with scalar coefficients which corresponds to the well-known central extension of the Witt algebra known as the ("ordinary") Virasoro algebra.

It was shown in [11] that the second Hochschild cohomology groups denoted $\mathrm{H}^2(U(2), M)$ are zero for every conformal (bi-)module M, but for higher Hochschild cohomologies the direct computation becomes too complicated. In contrast to the "ordinary" Hochschild cohomology, if C is an infinite associative conformal algebra then one cannot reduce the computation of $\mathrm{H}^n(C, M)$ to $\mathrm{H}^{n-1}(C, \mathrm{Chom}(C, M))$ since the space $\mathrm{Chom}(C, M)$ of conformal homomorphisms is not in general a conformal module over C.

A powerful technique for computing Hochschild cohomologies of associative algebras is the Morse matching method described, for example, in [8]. Given an associative algebra defined by generators and relations, one may apply the Morse matching method to compute the differential map in Anick resolution for this algebra. Since the Anick resolution is much smaller than,

for example, the bar resolution, the computation of cohomologies becomes easier.

It is discussed in [2] how to adjust this technique to conformal algebras in order to calculate conformal Hochschild cohomologies with coefficients in a trivial module. In [1] we applied the same Morse matching method for calculation of conformal Hochschild cohomologies with coefficients in a non-trivial module. In particular, $\mathrm{H}^n(U(2), M) = 0$ for every $n > 1$ and for every finite left $U(2)$-module M.

This result shows a difference between homological properties of Lie conformal algebras and their universal enveloping associative conformal algebras. Indeed, there exist finite modules over the Virasoro conformal algebra V with non-trivial higher cohomologies. However, these modules do not correspond to representations of $U(2)$ due to the locality restriction. This is why we are interested in the next universal envelope in the series: every finite irreducible module over V is also a module over $U(3)$.

3 Main results

Let $V = \mathbb{C}[\partial]x$ be the Virasoro conformal algebra as above. Then the space $\mathbb{C}[\partial]u$ can be considerded as a conformal module over V relative to the operation

$$x_\lambda u = (\partial + \alpha + \Delta\lambda)u,$$

where $\alpha, \Delta \in \mathbb{C}$ are fixed scalars. Such a module is denoted $M_{\alpha,\Delta}$. If $\Delta \neq 0$ then this is an irreducible V-module, and it was shown in [6] that all finite irreducible Virasoro conformal modules are in the form of $M_{\alpha,\Delta}$.

Every $M_{\alpha,\Delta}$ is also a left module over $U(3)$. The annihilation algebra of $U(3)$ is generated by infinite set $\{x(n) \mid n \in \mathbb{Z}_+\}$ relative to the following defining relations:

$$x(n)x(m) - 3x(n-1)x(m+1) + 3x(n-2)x(m+2) \\ - x(n-3)x(m+3) = 0, \quad n \geq 3,\ m \geq 0,$$

$$x(n)x(m) - x(m)x(n) = (n-m)x(n+m-1), \quad n > m \geq 0.$$

The Gröbner–Shirshov basis of these relations includes rewriting rules with principal parts $x(1)x(0)$ and $x(n)x(m)$, $n \geq 2$. Hence, the Anick resolution is spanned by n-chains of the form $[x(j_1)|\dots|x(j_n)|x(j_{n+1})]$ and $[x(j_1)|\dots|x(j_n)|1|0]$, where $j_1, \dots, j_n \geq 2$. The Anick resolution allows us to deduce the following statement.

Theorem 1. For the conformal module $M_{(\alpha,\Delta)}$ with $\Delta \neq 0$, we have

$$\dim_{\Bbbk} \mathrm{H}^1(U(3), M_{(\alpha,\Delta)}) = \begin{cases} 2, & \Delta = 1, \alpha = 0 \\ 0, & \text{otherwise.} \end{cases}$$

This statement is about the first cohomology group so it may be checked independently by the definition. However, for higher cohomology groups the straightforward computation is not possible so we need specific methods for computing $\mathrm{H}^n(U(3), M_{(\alpha,\Delta)})$. The same Anick resolution for $U(3)$ computed by means of the Morse matching method gives us

Theorem 2. For all $\alpha \neq 0$, $\Delta \in \mathbb{C}$ we have $\mathrm{H}^n(U(3), M_{(\alpha,\Delta)} = 0$ for $n \geq 2$.

It remains to consider the case $\alpha = 0$. In this way, we obtain

Theorem 3. For the conformal module $M_{(0,\Delta)}$, $\Delta \neq 0$, over $U(3)$, we have

$$\dim_{\Bbbk} \mathrm{H}^2(U(3), M_{(0,\Delta)}) = \begin{cases} 1, & \Delta = 1 \\ 0, & \Delta \neq 1. \end{cases}$$

The same methods may be applied for computing the remaining cohomologies with coefficients in finite irreducible ($\Delta \neq 0$) modules.

Theorem 4. For $n \geq 3$, the cohomology groups $\mathrm{H}^n(U(3), M_{(0,\Delta)})$, $\Delta \neq 0$, are trivial.

These results show that the difference between cohomologies of the Virasoro Lie conformal algebra V and its universal envelope $U(3)$ still holds: as it was shown in [4], for every n there exists $\Delta \neq 0$ such that $\mathrm{H}^n(V, M_{0,\Delta})$ is nonzero.

In order to extend these results from irreducible to arbitrary finite module over $U(3)$, we need cohomologies with coefficients in $M_{0,0}$.

Theorem 5. For the conformal module $M_{(0,0)}$, we have

$$\dim_{\Bbbk} \mathrm{H}^n(U(3), M_{(0,0)}) = \begin{cases} 1 & n = 1; \\ 2 & n = 2; \\ 1 & n = 3; \\ 0 & n \geq 4. \end{cases}$$

The standard reasoning coming from the long exact sequence leads us to the following conclusion.

Corollary. Let M be a finite module over $U(3)$. Then $\mathrm{H}^n(U(3), M) = 0$ for all $n \geq 4$.

Acknowledgments

The work was supported by Russian Science Foundation, project 23-21-00504.

[1] H. Alhussein, P. Kolesnikov, Hochschild cohomology of the Weyl conformal algebra with coefficients in finite modules. J. Math. Phys. 64, no.4, Paper No. 041701, 16 pp (2023).

[2] H. Alhussein, P.S. Kolesnikov, V.A. Lopatkin, Morse matching method for conformal cohomologies, arxiv.org/pdf/2204.10837.

[3] B. Bakalov, A. D'Andrea, V.G. Kac, Theory of finite pseudoalgebras. Adv. Math. 162, 1–140 (2001).

[4] B. Bakalov, V.G. Kac, A. Voronov, Cohomology of conformal algebras. Comm. Math. Phys. 200, 561–589 (1999).

[5] C. Boyallian, V.G. Kac, J.-I. Liberati, On the classification of subalgebras of Cend_N and gc_N. J. Algebra 260, 32–63 (2003).

[6] S.-J. Cheng, V. G. Kac, Conformal modules. Asian J. Math. 1, 181-193 (1997).

[7] A. D'Andrea, V.G. Kac, Structure theory of finite conformal algebras. Sel. Math., New Ser. 4, 377–418 (1998).

[8] M. Jöllenbeck, V. Welker, Minimal resolutions via algebraic discrete Morse theory. Mem. Am. Math. Soc. 197, no. 923 (2009).

[9] V.G. Kac, Vertex Algebras for Beginners. Univ. Lect. Ser., 10, Am. Math. Soc., Providence, RI (1998).

[10] V.G. Kac, Formal distribution algebras and conformal algebras. In: De Wit, D. et al. (eds.) 12th international congress of mathematical physics (ICMP97), 80–97. Internat. Press, Cambridge, MA (1999).

[11] R.A. Kozlov, Hochshild cohomology of the associative conformal algebra $\mathrm{Cend}_{1,x}$, Algebra and Logic 58, 36–47 (2019).

[12] M. Roitman, Universal enveloping conformal algebras, Sel. Math. New Ser. 6, 319–345 (2000).

FOUR GENERATORS OF AN EQUIVALENCE LATTICE WITH CONSECUTIVE BLOCK COUNTS

Gábor Czédli*

University of Szeged, Bolyai Institute. Szeged, Aradi vértanúk tere 1, HUNGARY 6720, http://www.math.u-szeged.hu/~czedli/

e-mail: czedli@math.u-szeged.hu

Dedicated to my esteemed coauthors, Honorary Professors László Szabó on his seventy-fifth birthday and Lajos Klukovits on his eightieth birthday.

This paper is probably self-contained for those who know the concept of a lattice as an algebraic structure. Our goal is two-fold. First, we present a historical remark on the connection between equivalence lattices and quasiorder lattices. Second, we prove a new theorem, which corresponds to the title of the paper.

1 Introduction and a historical remark

We begin with some notations and well-known definitions. The set of *equivalences* (in other words, *equivalence relations*, that is, reflexive, symmetric, and transitive relations) of a set A will be denoted by $\mathrm{Equ}(A)$. With intersections and the transitive hulls of unions acting as meets and joins, respectively, $\mathrm{Equ}(A)$ is a *lattice*, the *equivalence lattice* of (or over) A; the notation $\mathrm{Equ}(A)$ will stand for this lattice, too. By the canonical bijective correspondence between equivalences and partitions of a set, $\mathrm{Equ}(A)$ is isomorphic to the *partition lattice* $\mathrm{Part}(A)$ of A, which consists of all partitions of A. We will often consider equivalences as partitions. For $X \subseteq Y$, we say that X is a *proper* subset of Y if $X \neq Y$. A *sublattice* or a *complete sublattice* of $\mathrm{Equ}(A)$ is a nonempty subset that is closed with respect to binary joins and meets or to arbitrary joins and meets, respectively. A subset X of $\mathrm{Equ}(A)$ is a *generating set* or a *complete-generating set* of $\mathrm{Equ}(A)$ if there is

*This research was supported by the National Research, Development and Innovation Fund of Hungary, under funding scheme K 138892.

no proper sublattice Y or a proper complete sublattice Y of $\mathrm{Equ}(A)$, respectively, such that $X \subseteq Y$. *Quasiorders* are reflexive and symmetric relations. The quasiorders of a set A form a lattice, the *quasiorder lattice* $\mathrm{Quo}(A)$ of A. Note that $\mathrm{Equ}(A)$ is a complete sublattice of $\mathrm{Quo}(A)$.

In the middle of the seventies, Henrik Strietz proved that for any finite set A with $|A| \geq 3$, $\mathrm{Equ}(A)$ is *four-generated*, that is, it has a four-element generating set; see Strietz [10]–[11]. Since Strietz's work, more than a dozen papers have been devoted to four-element (or small) generating sets of equivalence lattices and quasiorder lattices; for details, see the "References" section here and the bibliographic sections and the survey parts of the papers listed there. Hence, instead of giving another survey, we focus only on the connection between the small generating sets of $\mathrm{Equ}(A)$ and those of $\mathrm{Quo}(A)$. In one direction, we recall an important statement from [9, page 61]; see also Lemma 2.1 of [7], where the original lemma is recalled.

Lemma 1.1 (Kulin's Lemma)**.** *If A is an arbitrary set with at least three elements and S is a complete sublattice of* $\mathrm{Quo}(A)$ *such that* $\mathrm{Equ}(A)$ *is a proper subset of S, then $S = \mathrm{Quo}(A)$.*

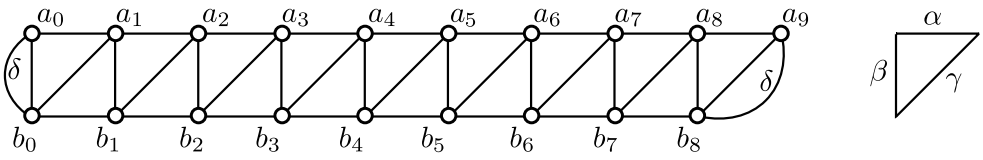


Figure 1: Zádori's construction for $|A| = 19$

In other directions, neither any connection nor the forthcoming Claim 1.4 has been published before. To present such a connection of historical value, let $|A| = 19$; the case of $|A| = 2k + 1 \geq 5$ would be similar. The construction visualized by Figure 1 is taken from Zádori [12].

Claim 1.2 ([12]; exemplifying the odd case of Zádori's construction)**.** *If $|A| = 19$, then* $\mathrm{Equ}(A)$ *has a four-element generating set.*

For later reference, we present Zádori's proof and his generating set.

Proof. For $p, q \in A$, the smallest equivalence collapsing p and q is an atom in $\mathrm{Equ}(A)$; we denote it by $\mathrm{at}(p, q)$. So $(x, y) \in \mathrm{at}(p, q)$ if and only if $x = y$ or $\{x, y\} = \{p, q\}$. Denote the elements of A as follows: $A = \{a_0, a_1, \ldots, a_9, b_0, b_1, \ldots, b_8\}$; see Figure 1. The figure defines a subset $X := \{\alpha, \beta, \gamma, \delta\}$ of the equivalence lattice $\mathrm{Equ}(A)$ as follows. Assume that the horizontal edges, the vertical edges, and the slanted straight edges of the graph are labeled

by α, β, and γ, respectively. To avoid a crowded figure, these labels are not indicated in the figure, but the triangle on the right reminds us of this convention. There are also two δ-labeled edges, which are drawn as curves. For $\epsilon \in X$, the figure defines ϵ as follows; walks of length zero are allowed.

$$\epsilon := \{(x, y) \in A^2 : \text{we can walk from } x \text{ to } y \text{ along } \epsilon\text{-colored edges}\}. \quad (1.1)$$

For example, $\{b_1, a_2\}$ is a block of γ and $\{b_0, \dots, b_8\}$ is a block of α. Let S be the sublattice generated by X. In Figure 2, where A is drawn three times, some equivalences are given by their non-singleton blocks. The meanings of these blocks, with different geometric orientations, line styles, and colors, are defined on the right of the figure. For example, $\rho_0 = \mathrm{at}(a_0, b_0)$ and $\lambda'_1 = \mathrm{at}(a_9, a_8) \vee \mathrm{at}(a_8, a_7) \vee \mathrm{at}(b_8, b_7)$. We can easily show that, in this order, ρ_0, ρ'_0, ρ''_0, ρ_1, ρ'_1, ρ''_1, ρ_2, ρ'_2, ρ''_2, ρ_3, ρ'_3, ρ''_3, ρ_4, ... belong to S, since each of them is expressible from the generators and the earlier ones. Indeed, $\rho_0 = \beta \wedge \delta$ and, for $i = 0, 1, 2, \dots$, we have that $\rho'_i = (\rho_i \vee \gamma) \wedge \alpha$, $\rho''_i = (\rho'_i \vee \beta) \wedge \gamma$, and $\rho_{i+1} = \big(((\rho''_i \vee \beta) \wedge \alpha) \vee \rho''_i\big) \wedge \beta$. The increasing sequences $(\rho_0, \rho_1, \rho_2, \dots)$, $(\rho'_0, \rho'_1, \rho'_2, \dots)$, and $(\rho''_0, \rho''_1, \rho''_2, \dots)$ are *right-going* in the sense that when the subscript increases by 1, the subscripted equivalence obtains a new "edge" on the right of the earlier edges. By interchanging the role of β and γ, we obtain three increasing "left-going" sequences $(\lambda_0, \lambda_1, \lambda_2, \dots)$, $(\lambda'_0, \lambda'_1, \lambda'_2, \dots)$, and $(\lambda''_0, \lambda''_1, \lambda''_2, \dots)$. Where a right-going sequence "reaches" the appropriate left-going one, the meet of the two sequences yields an atom of $\mathrm{Equ}(A)$. Namely, for $i \in \{0, 1, \dots, 8\}$, $\mathrm{at}(a_i, b_i) = \rho_i \wedge \lambda''_{8-i} \in S$, $\mathrm{at}(a_{i+1}, b_i) = \rho''_i \wedge \lambda_{8-i} \in S$, and $\mathrm{at}(a_i, a_{i+1}) = \rho'_i \wedge \lambda'_{8-i} \in S$. Furthermore, for $i \in \{0, \dots, 7\}$, $\mathrm{at}(b_i, b_{i+1}) = \big(\mathrm{at}(a_{i+1}, b_i) \vee \mathrm{at}(a_{i+1}, b_{i+1})\big) \wedge \alpha \in S$. Hence, for every edge (x, y) of the graph, $\mathrm{at}(x, y) \in S$. Therefore, the following lemma implies easily that X generates $\mathrm{Equ}(A)$. □

Lemma 1.3. *If* $3 \leq n \in \mathbb{N}^+ = \{1, 2, 3, \dots\}$, $A = \{a_0, a_1, \dots, a_{n-1}\}$, *and* $|A| = n$, *then* $\{\mathrm{at}(a_{i-1}, a_i) : i \in \{1, \dots, n-1\}\} \cup \{\mathrm{at}(a_{n-1}, a_0)\}$ *generates* $\mathrm{Equ}(A)$.

In some form, this easy lemma occurs in several papers; see, e.g., [3, Lemma 2.2] and [8, Lemma 2.5].

In 1995, the author visited Ivan Chajda at Palacký University in Olomouc. The research plan looked easy: by orienting the edges of the graph in Figure 1 in some way, we should find a small generating set of $\mathrm{Quo}(A)$. Our first construction was soon developed into a more sophisticated one, and so the first construction does not occur [1]. However, we need the first

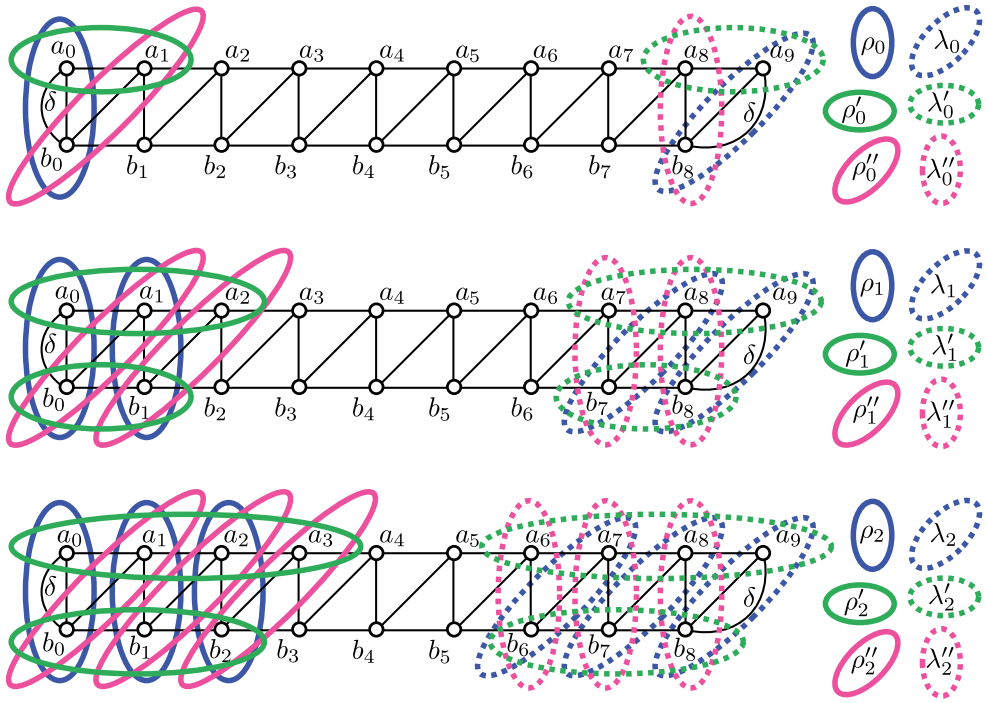


Figure 2: Right-going and left-going sequences

construction[1] here even though [1] contains a stronger result and we have an even stronger one nowadays.

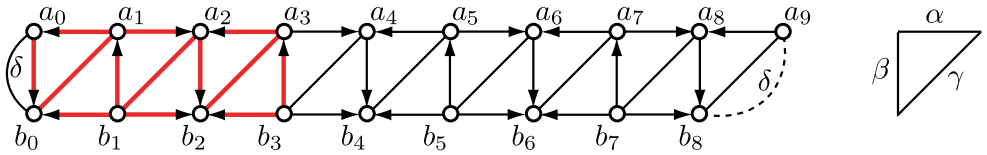


Figure 3: Generating a quasiorder lattice

Let $A = \{a_0, a_1, \ldots, a_9, b_0, b_1, \ldots, b_8\}$ be the 19-element set drawn in Figure 3, which is quite similar to Figure 1. Some edges are directed by arrowheads, some others are not. The figure defines a set $Y_0 = \{\alpha, \beta, \gamma, \delta\}$ of quasiorders of A by (1.1) with the only modification that we cannot walk along a directed edge in the opposite direction. Along an undirected edge, we can walk in both directions. At present, it makes no difference whether an edge is red and thick or not. For example, $(a_3, a_2), (a_3, a_4) \in \alpha$, $(a_3, b_2), (b_2, a_3) \in \gamma$, but $(b_4, a_4) \notin \beta$ and $(a_2, a_3), (a_3, a_7) \notin \alpha$. For $\epsilon \in Y_0$,

[1] Its exact details have been lost but the idea of Claim 1.4 is the same.

denote $\epsilon^{-1} = \{(y,x) : (x,y) \in \epsilon\} \in \mathrm{Quo}(A)$ the *inverse* of ϵ. Note that γ and δ are equivalences, and so $\gamma^{-1} = \gamma$ and $\delta^{-1} = \delta$. Let $Y := Y_0 \cup \{\epsilon^{-1} : \epsilon \in Y_0\} = \{\alpha, \alpha^{-1}, \beta, \beta^{-1}, \gamma, \delta\}$.

Claim 1.4. *The six-element set Y generates* $\mathrm{Quo}(A)$.

Outline of the proof. For $x, y \in A$, $\mathrm{qu}(x,y)$ denotes the smallest quasiorder containing (x,y). Let S stand for the sublattice generated by Y. Since $f\colon \mathrm{Quo}(A) \to \mathrm{Quo}(A)$ defined by $\mu \mapsto \mu^{-1}$ is an automorphism of $\mathrm{Quo}(A)$ and Y is f-closed, S is also closed with respect to forming inverses. In particular, whenever $\mathrm{qu}(x,y)$ is in S, then so is $\mathrm{qu}(y,x)$; this fact will be used without further explanation. Let us compute; each containment "$\in S$" below follows from the earlier ones and $Y \subseteq S$:

$$\mathrm{qu}(a_0,b_0) = \beta \wedge \delta \in S, \tag{1.2}$$
$$\mathrm{qu}(a_1,b_0) = (\alpha \vee \mathrm{qu}(a_0,b_0)) \wedge \gamma \in S, \text{ by (1.2)}, \tag{1.3}$$
$$\mathrm{qu}(a_1,a_0) = \alpha \wedge (\mathrm{qu}(a_1,b_0) \vee \mathrm{qu}(b_0,a_0)) \in S \text{ by (1.3) and (1.2)}, \tag{1.4}$$
$$\mathrm{qu}(b_1,a_1) = (\alpha \vee \mathrm{qu}(b_0,a_1)) \wedge \beta \in S \text{ by (1.3)}, \tag{1.5}$$
$$\mathrm{qu}(b_1,b_0) = \alpha \wedge (\mathrm{qu}(b_1,a_1) \vee \mathrm{qu}(a_1,b_0)) \in S \text{ by (1.5) and (1.3)}, \tag{1.6}$$
$$\mathrm{qu}(b_1,a_2) = \gamma \wedge (\mathrm{qu}(b_1,a_1) \vee \alpha) \in S \text{ by (1.5)}, \tag{1.7}$$
$$\mathrm{qu}(a_1,a_2) = \alpha \wedge (\mathrm{qu}(a_1,b_1) \vee \mathrm{qu}(b_1,a_2)) \in S \text{ by (1.5) and (1.7)}, \tag{1.8}$$
$$\mathrm{qu}(a_2,b_2) = \beta \wedge (\mathrm{qu}(a_2,b_1) \vee \alpha) \in S \text{ by (1.7)}, \tag{1.9}$$
$$\mathrm{qu}(b_1,b_2) = \alpha \wedge (\mathrm{qu}(b_1,a_2) \vee \mathrm{qu}(a_2,b_2)) \in S \text{ by (1.7) and (1.9)}, \tag{1.10}$$
$$\mathrm{qu}(a_3,b_2) = \gamma \wedge (\alpha \vee \mathrm{qu}(a_2,b_2)) \in S \text{ by (1.9)}, \tag{1.11}$$
$$\mathrm{qu}(a_3,a_2) = \alpha \wedge (\mathrm{qu}(a_3,b_2) \vee \mathrm{qu}(b_2,a_2)) \in S \text{ by (1.11) and (1.9)}, \tag{1.12}$$
$$\mathrm{qu}(b_3,a_3) = \beta \wedge (\alpha \vee \mathrm{qu}(b_2,a_3)) \in S \text{ by (1.11)}, \tag{1.13}$$
$$\mathrm{qu}(b_3,b_2) = \alpha \wedge (\mathrm{qu}(b_3,a_3) \vee \mathrm{qu}(a_3,b_2)) \in S \text{ by (1.13) and (1.11)}, \tag{1.14}$$

and so on. Computations (1.2)–(1.14) and the fact that S is closed with respect to forming inverses show that for each thick and red edge (x,y) of the graph, $\mathrm{qu}(x,y)$ and $\mathrm{qu}(y,x)$ are in S. The figure and (1.2)–(1.14) also show how we can proceed further to the right. Hence, $\mathrm{qu}(x,y)$ and $\mathrm{qu}(y,x)$ are in S for every edge (x,y) of the graph. Thus, the straightforward counterpart of Lemma 1.3 for quasiorder lattices completes the proof of Claim 1.4. □

In the proof above, δ was needed only in the first step, (1.2). This step and the whole proof still work if we omit the dashed curve in Figure 3 and replace δ by the equivalence $\mathrm{at}(a_0,b_0)$. Now we do not need a left-going sequence of quasiorders. Hence, and this was a surprise in 1995, we do not need the figure to end on the right. So A can be $\{a_i : i \in \mathbb{N}_0\} \cup \{b_i : i \in \mathbb{N}_0\}$,

where $\mathbb{N}_0 = \{0, 1, 2, \dots\}$; this was the moment when an *infinite base set* came into the picture.

Infinite base sets required new techniques, first for quasiorder lattices, see [1]. The new techniques were soon adapted to infinite equivalence lattices; see, e.g., [2]. Later, it appeared that these techniques are useful for finite equivalence lattices; see [3] and [8]. Due to the results of these two papers, a connection with cryptography has been discovered; see [3] and, mainly, [4]. This connection and many earlier results on four-element generating sets motivate Section 2, where a new four-element generating set is constructed. To summarize our historical remark: In some sense, most papers mentioned so far and the present one grew from the unpublished proof of Claim 1.4.

Finally, to conclude this section, note that we can obtain a four-element generating set of $\mathrm{Quo}(A)$ for $|A| = 19$, that is, a stronger result, as follows. (However, this argument does not show how to step from the class of finite equivalence and quasiorder lattices to that of the infinite ones.) Going after [7] and using Figure 1, add a new δ-curve, a directed one, from a_1 to a_2. That is, we change δ to $\delta \vee \mathrm{qu}(a_1, a_2)$. By the proof of Claim 1.2, we obtain all members of $\mathrm{Equ}(A)$ from $X := \{\alpha, \beta, \gamma, \delta\}$. Thus, X generates $\mathrm{Quo}(A)$ by (Kulin's) Lemma 1.1.

2 A new four-element generating set with a special property

The *block count* of an equivalence $\mu \in \mathrm{Equ}(A)$ is the number $\mathrm{blnum}(\mu)$ of blocks of (the partition corresponding to) μ. We say that $X = \{\mu_1, \mu_2, \mu_3, \mu_4\}$ is a *four-element generating set of* $\mathrm{Equ}(A)$ *with consecutive block counts* if X generates $\mathrm{Equ}(A)$ and $\mathrm{blnum}(\mu_{1+i}) = \mathrm{blnum}(\mu_1) + i$ for $i \in \{1, 2, 3\}$. We are going to prove the following theorem.

Theorem 2.1. *If the number of elements of a finite set A is six or it is at least eight, then* $\mathrm{Equ}(A)$ *has a four-element generating set with consecutive block counts.*

Similar properties (namely, "same block counts" and "the difference between the block counts ≤ 2") have been studied in [5] and [6]; the property we consider in this section is more difficult to fulfill. Despite some similarities with [5] and [6] in the approach, the present paper remains self-contained.

Remark 2.2. We know that if $|A| < 6$, then $\mathrm{Equ}(A)$ has no four-element generating set with consecutive block counts; we guess the same for $|A| = 7$.

A pair (μ, ν) of elements of $\mathrm{Equ}(A)$ is *complementary* if $\mu \vee \nu = \mathbf{1}_A$, the top element of $\mathrm{Equ}(A)$, and $\mu \wedge \nu = \mathbf{0}_A$, the bottom element of $\mathrm{Equ}(A)$.

Definition 2.3 ([5])**.** A 7-tuple $\mathbf{A} = (A; \alpha, \beta, \gamma, \delta; u, v)$ is called an *eligible system* if A is a nonempty set, $\{\alpha, \beta, \gamma, \delta\}$ is a generating set of $\mathrm{Equ}(A)$, and the pairs (α, δ), $\bigl(\beta, \gamma \vee \mathrm{at}(u, v)\bigr)$, and $\bigl(\beta \vee \mathrm{at}(u, v), \gamma\bigr)$ are complementary.

For $\rho \subseteq (A')^2$, $\overline{\mathrm{eq}}'(\rho)$ will denote the smallest equivalence of A' that includes ρ. For distinct elements $x, y \in A'$, let $\mathrm{at}'(x, y) := \overline{\mathrm{eq}}'(\{(x, y)\})$. The lattice operations in $\mathrm{Equ}(A')$ will be denoted by $\vee'$ and $\wedge'$.

Lemma 2.4. *Let* $\mathbf{A}$ *be an eligible system with components denoted as in Definition 2.3. Assume that* $u', v' \notin A$ *and* $u' \neq v'$*. Let* $A' := A \cup \{u', v'\}$*,* $\alpha' := \overline{\mathrm{eq}}'(\alpha) \vee' \mathrm{at}'(u, u')$*,* $\beta' := \overline{\mathrm{eq}}'(\beta) \vee' \mathrm{at}'(u, v')$*,* $\gamma' := \overline{\mathrm{eq}}'(\gamma) \vee' \mathrm{at}'(v, v')$*,* $\delta' := \overline{\mathrm{eq}}'(\delta) \vee' \mathrm{at}'(u', v')$*. Then* $\mathbf{A}' := (A'; \alpha', \beta', \gamma', \delta'; u', v')$ *is an eligible system, too. Furthermore, if* $\Phi := \{\alpha, \beta, \gamma, \delta\}$ *is of consecutive block counts, then so is* $\Phi' := \{\alpha', \beta', \gamma', \delta'\}$*.*

Proof. The situation is visualized in Figure 4, where the blocks of some elements, all important elements from our perspective, are drawn. The three blocks drawn by solid lines are blocks of some members of $\Phi \subseteq \mathrm{Equ}(A)$. The seven blocks drawn in non-solid line styles (dotted and various kinds of dashed) are blocks of the equivalences belonging to $\Phi' \subseteq \mathrm{Equ}(A')$. The figure uses different line styles or distinct colors for the blocks of different equivalences, but we use the same color for $\epsilon \in \Phi$ and ϵ'. Note that the geometrically large blocks on the left could be singletons and, on the other hand, $u/\alpha := \{x : (x, u) \in \alpha\}$ and v/γ can be but need not be disjoint. Not all blocks of all ϵ and ϵ' are drawn for $\epsilon \in \Phi$. However, for any $x \in A$ and $\epsilon \in \Phi$, if the block x/ϵ is not drawn, then $x/\epsilon = x/\epsilon'$. The last sentence of Lemma 2.4 follows from the trivial fact that $\mathrm{blnum}(\epsilon') = 1 + \mathrm{blnum}(\epsilon)$ holds for every $\epsilon \in \Phi$. Applying a lemma from [5] twice (in a "twisted way" and in a "straight way"), we could derive the rest of Lemma 2.4 from [5]. To keep the paper self-contained, we give a different and direct proof.

The existence of an $x \in u/\beta \wedge v/\gamma$ would violate the conjunction of $\beta \wedge (\gamma \vee \mathrm{at}(u, v)) = \mathbf{0}_A$ and $\gamma \wedge (\beta \vee \mathrm{at}(u, v)) = \mathbf{0}_A$ —call them the *meet conditions* for β and γ— and $u \neq v$. Thus, u/β and v/γ are disjoint.

By the two paragraphs above, Figure 4 faithfully represents the situation and contains all the details the proof needs. Hence, it is straightforward to verify that the three pairs in Definition 2.3 for $\mathrm{Equ}(A')$ are complementary. Let S and E denote the sublattice generated by Φ' in $\mathrm{Equ}(A')$ and the sublattice $\{\mu \in \mathrm{Equ}(A') : \text{ both } u'/\mu \text{ and } v'/\mu \text{ are singletons}\}$. Then $f \colon \mathrm{Equ}(A) \to E$ defined by $\mu \mapsto \overline{\mathrm{eq}}'(\mu)$ is a lattice isomorphism.

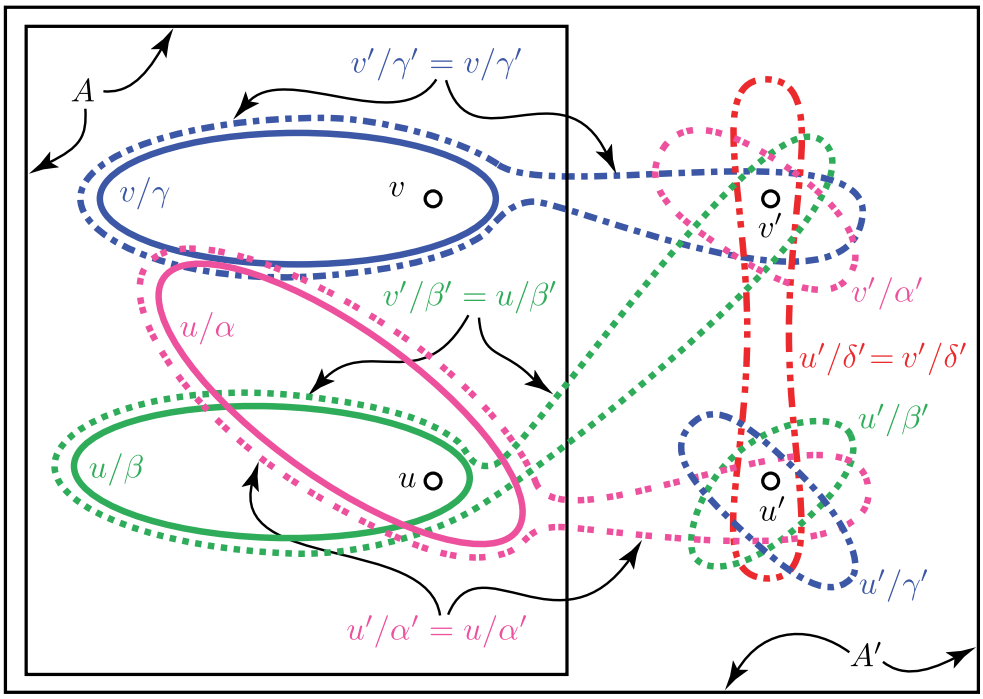


Figure 4: Illustrating the proof of Lemma 2.4

Observe that $\{u'\}$ is a singleton block of $\beta' \vee' \gamma'$. Furthermore, $\{v'\}$ is a singleton block of both α' and $\delta' \wedge' (\beta' \vee' \gamma')$. Thus $\{v'\}$ is a singleton block of $\alpha' \vee' \big(\delta' \wedge' (\beta' \vee' \gamma')\big)$. Therefore, with

$$\kappa := (\beta' \vee' \gamma') \wedge' \Big(\alpha' \vee' \big(\delta' \wedge' (\beta' \vee' \gamma')\big)\Big),$$

$|u'/\kappa| = |v'/\kappa| = 1$. Using the fact that $\epsilon \subseteq \epsilon'$ for all $\epsilon \in X$, the join condition $\beta \vee \mathrm{at}(u, v) \vee \gamma = \mathbf{1}_A$ for β and γ, and $(u, v) \in \beta' \vee' \gamma'$, we obtain that $A^2 \subseteq \beta' \vee' \gamma'$. By the previous two "$\subseteq$" inclusions, $\delta \subseteq \delta' \wedge' (\beta' \vee' \gamma')$. Using this fact, $\alpha \subseteq \alpha'$, and the join condition for the complementary pair (α, δ), we obtain that $A^2 \subseteq \kappa$. Combining this with $|u'/\kappa| = |v'/\kappa| = 1$, we have that $f(\mathbf{1}_A) = \kappa \in S$. Thus, for all $\epsilon \in \Phi$, $f(\epsilon) = f(\mathbf{1}_A) \wedge \epsilon' \in S$, whereby $f(\Phi) \subseteq S$. Since Φ generates $\mathrm{Equ}(A)$ and $f\colon \mathrm{Equ}(A) \to E$ is an isomorphism, we obtain that $E \subseteq S$. In particular, $\mathrm{at}'(u, v) = f(\mathrm{at}(u, v)) \in S$. As the following equalities are clear by the figure, we obtain further

elements of S as follows:

$$\begin{aligned}
\mathrm{at}'(v,v') &= (\mathrm{at}'(u,v) \vee' \beta') \wedge' \gamma' \in S, && (2.1)\\
\mathrm{at}'(v',u) &= (\mathrm{at}'(u,v) \vee \mathrm{at}'(v,v')) \wedge' \beta' \in S, &&\\
\mathrm{at}'(v',u') &= (\mathrm{at}'(v',u) \vee' \alpha') \wedge' \delta' \in S, \text{ and} && (2.2)\\
\mathrm{at}'(u',u) &= \alpha' \wedge' (\mathrm{at}'(u',v') \vee' \mathrm{at}'(v',u)) \in S. && (2.3)
\end{aligned}$$

Finally, since $E \subseteq S$ and we have (2.1), (2.2), and (2.3), Lemma 1.3 implies that $S = \mathrm{Equ}(A')$. This completes the proof of Lemma 2.4. □

Lemma 2.5. *With* $A = \{1, 2, \ldots, 6\}$,

$$\begin{aligned}
\alpha &:= \mathrm{eq}(12;3;45;6), && (2.4)\\
\beta &:= \mathrm{eq}(1;2;34;5;6), && (2.5)\\
\gamma &:= \mathrm{eq}(13;24;56), \ \textit{and} && (2.6)\\
\delta &:= \mathrm{eq}(146;235), && (2.7)
\end{aligned}$$

$\mathbf{A} = (A; \alpha, \beta, \gamma, \delta; 4, 6)$ *is an eligible system with consecutive block counts.*

Proof. Let $\Phi := \{\alpha, \beta, \gamma, \delta\}$, and let S stand for the sublattice generated by S. The labels above the equality signs will indicate which members of S imply that the equivalences on the left of these equality signs belong to S.

$$\begin{aligned}
\mathrm{eq}(12;345;6) &\overset{(2.4)(2.5)}{=} \mathrm{eq}(12;3;45;6) \vee \mathrm{eq}(1;2;34;5;6), && (2.8)\\
\mathrm{eq}(1234;56) &\overset{(2.5)(2.6)}{=} \mathrm{eq}(1;2;34;5;6) \vee \mathrm{eq}(13;24;56), && (2.9)\\
\mathrm{eq}(12;3;4;5;6) &\overset{(2.4)(2.9)}{=} \mathrm{eq}(12;3;45;6) \wedge \mathrm{eq}(1234;56), && (2.10)\\
\mathrm{eq}(1;2;35;4;6) &\overset{(2.7)(2.8)}{=} \mathrm{eq}(146;235) \wedge \mathrm{eq}(12;345;6), && (2.11)\\
\mathrm{eq}(14;23;5;6) &\overset{(2.7)(2.9)}{=} \mathrm{eq}(146;235) \wedge \mathrm{eq}(1234;56), && (2.12)\\
\mathrm{eq}(1;2;345;6) &\overset{(2.5)(2.11)}{=} \mathrm{eq}(1;2;34;5;6) \vee \mathrm{eq}(1;2;35;4;6), && (2.13)\\
\mathrm{eq}(1356;24) &\overset{(2.6)(2.11)}{=} \mathrm{eq}(13;24;56) \vee \mathrm{eq}(1;2;35;4;6), && (2.14)\\
\mathrm{eq}(14;235;6) &\overset{(2.11)(2.12)}{=} \mathrm{eq}(1;2;35;4;6) \vee \mathrm{eq}(14;23;5;6), && (2.15)\\
\mathrm{eq}(1;2;3;45;6) &\overset{(2.4)(2.13)}{=} \mathrm{eq}(12;3;45;6) \wedge \mathrm{eq}(1;2;345;6), && (2.16)\\
\mathrm{eq}(16;2;35;4) &\overset{(2.7)(2.14)}{=} \mathrm{eq}(146;235) \wedge \mathrm{eq}(1356;24), && (2.17)\\
\mathrm{eq}(13;2456) &\overset{(2.6)(2.16)}{=} \mathrm{eq}(13;24;56) \vee \mathrm{eq}(1;2;3;45;6), && (2.18)\\
\mathrm{eq}(126;35;4) &\overset{(2.10)(2.17)}{=} \mathrm{eq}(12;3;4;5;6) \vee \mathrm{eq}(16;2;35;4), && (2.19)
\end{aligned}$$

$$\mathrm{eq}(145;23;6) \overset{(2.12)\text{–}(2.16)}{=} \mathrm{eq}(14;23;5;6) \vee \mathrm{eq}(1;2;3;45;6), \tag{2.20}$$

$$\mathrm{eq}(15;2;3;4;6) \overset{(2.14)\text{–}(2.20)}{=} \mathrm{eq}(1356;24) \wedge \mathrm{eq}(145;23;6), \tag{2.21}$$

$$\mathrm{eq}(1;26;3;4;5) \overset{(2.18)\text{–}(2.19)}{=} \mathrm{eq}(13;2456) \wedge \mathrm{eq}(126;35;4), \tag{2.22}$$

$$\mathrm{eq}(135;2;4;6) \overset{(2.11)\text{–}(2.21)}{=} \mathrm{eq}(1;2;35;4;6) \vee \mathrm{eq}(15;2;3;4;6), \tag{2.23}$$

$$\mathrm{eq}(14;2356) \overset{(2.15)\text{–}(2.22)}{=} \mathrm{eq}(14;235;6) \vee \mathrm{eq}(1;26;3;4;5), \tag{2.24}$$

$$\mathrm{eq}(13;2;4;5;6) \overset{(2.6)\text{–}(2.23)}{=} \mathrm{eq}(13;24;56) \wedge \mathrm{eq}(135;2;4;6), \tag{2.25}$$

$$\mathrm{eq}(1;2;3;4;56) \overset{(2.6)\text{–}(2.24)}{=} \mathrm{eq}(13;24;56) \wedge \mathrm{eq}(14;2356). \tag{2.26}$$

In particular, $\mathrm{at}(1,2) \in S$ by (2.10), $\mathrm{at}(2,6) \in S$ by (2.22), $\mathrm{at}(6,5) \in S$ by (2.26), $\mathrm{at}(5,4) \in S$ by (2.16), $\mathrm{at}(4,3) \in S$ by (2.5), and $\mathrm{at}(3,1) \in S$ by (2.25). Hence, Φ is a generating set by Lemma 1.3. Clearly, Φ is of consecutive block counts. It is easy to check that the pairs in Definition 2.3 are complementary. Thus, $\mathbf{A}$ is an eligible system, proving Lemma 2.5. □

The author has created a program package called "equ2024p", available from his website http://tinyurl.com/g-czedli/. This program package can also "prove" that Φ generates $\mathrm{Equ}(A)$, but verifying the programs is much more difficult than verifying the proofs of Lemmas 2.5 and (the next) 2.6.

Lemma 2.6. *With* $A = \{1, 2, \ldots, 9\}$,

$$\alpha := \mathrm{eq}(158;2;3;47;69), \tag{2.27}$$

$$\beta := \mathrm{eq}(1;23;4;56;78;9), \tag{2.28}$$

$$\gamma := \mathrm{eq}(135;268;4;79), \text{ and} \tag{2.29}$$

$$\delta := \mathrm{eq}(16;257;3489), \tag{2.30}$$

$\mathbf{A} = (A; \alpha, \beta, \gamma, \delta; 1, 4)$ *is an eligible system with consecutive block counts.*

The proof of this lemma is similar to but more than three times longer than the previous proof. As the reader would hardly enjoy such an amount of technicalities, the proof goes into the Appendix of the extended version of the paper; it is available at https://arxiv.org/abs/2410.15328 or https://doi.org/10.48550/arXiv.2410.15328.

Now, we are in the position to prove our theorem.

Proof of Theorem 2.1. Combine Lemmas 2.4, 2.5, and 2.6. □

References

[1] I. Chajda, G. Czédli, How to generate the involution lattice of quasiorders? Studia Sci. Math. Hungar., **32** (1996), 415–427.

[2] G. Czédli, Four-generated large equivalence lattices, Acta Sci. Math. (Szeged), **62** (1996), 47–69.

[3] G. Czédli, Four-generated direct powers of partition lattices and authentication, Publicationes Mathematicae (Debrecen), **99** (2021), 447–472. https://doi.org/10.5486/PMD.2021.9024

[4] G. Czédli, Generating Boolean lattices by few elements and exchanging session keys, Novi Sad Journal of Mathematics, https://doi.org/10.30755/NSJOM.16637 (online first)

[5] G. Czédli, A pair of four-element horizontal generating sets of a partition lattice, preprint.

[6] G. Czédli, Four-element generating sets with block count widths at most two in partition lattices, preprint.

[7] G. Czédli, J. Kulin, A concise approach to small generating sets of lattices of quasiorders and transitive relations, Acta Sci. Math. (Szeged), **83** (2017), 3–12. https://dx.doi.org/10.14232/actasm-016-056-2

[8] G. Czédli, L. Oluoch, Four-element generating sets of partition lattices and their direct products, Acta Sci. Math. (Szeged), **86** (2020), 405–448. https://doi.org/10.14232/actasm-020-126-7

[9] J. Kulin, Quasiorder lattices are five-generated. Discussiones Mathematicae — General Algebra and Applications, **36** (2016), 59–70. https://dx.doi.org/10.7151/dmgaa.1248

[10] H. Strietz: Finite partition lattices are four-generated. In: Proc. Lattice Theory Conf. Ulm, 1975, pp. 257–259.

[11] H. Strietz, Über Erzeugendenmengen endlicher Partitionenverbände, Studia Sci. Math. Hungar., **12** (1977), 1–17. (German)

[12] L. Zádori, Generation of finite partition lattices. In: Lectures in universal algebra. (Proc. Colloq. Szeged, 1983) Colloq. Math. Soc. János Bolyai, Vol. 43. Amsterdam: North-Holland, 1986, pp. 573–586.

АЛГЕБРЫ БИНАРНЫХ ИЗОЛИРУЮЩИХ ФОРМУЛ ДЛЯ ДЕКАРТОВЫХ ПРОИЗВЕДЕНИЙ ГРАФОВ

Д.Ю. Емельянов*

Новосибирский государственный технический университет,
просп. Карла Маркса, 20, Новосибирск, 630073;
ИМ СО РАН, проспект ак. Коптюга, 4, 630090, Новосибирск, Россия
e-mail: dima-pavlyk@mail.ru

В работе более обширно описаны алгебры для декартовых произведений графов. Начало исследования и остальные произведения рассмотрены в монографии [1].

Определение 1. *Декартово произведение* или *прямое произведение* $G \times H$ графов G и H — это граф, такой, что множество вершин графа $G \times H$ — это прямое произведение $V(G) \times V(H)$, а любые две вершины (u, u') и (v, v') смежны в $G \times H$ тогда и только тогда, когда либо $u = v$ и u' смежна с v' в H, либо $u' = v'$ и u смежна с v в G.

В монографии [1] рассмотрены операции умножения графов на ребро. В этой работе мы далее будем исследовать декартово произведение правильных многоугольников между собой. Начнем с квадрата (четырехугольника), поскольку умножение на симплекс приводит к алгебраическому поглощению, характерному для симплексов [2].

Вспомним, как будут выглядеть алгебры для многоугольников.

Алгебра графа квадрата $\mathfrak{Q}$ и алгебра для пятиугольника $\mathfrak{P}$ с множеством меток $\rho_{\nu(p)} = \{0, 1, 2\}$ задается следующей таблицей:

$*$	0	1	2
0	$\{0\}$	$\{1\}$	$\{2\}$
1	$\{1\}$	$\{0, 2\}$	$\{1\}$
2	$\{2\}$	$\{1\}$	$\{0, 2\}$

*Работа выполнена при финансовой поддержке Российского научного фонда, проект № 24-21-00096.

Алгебра графа шестиугольника и алгебра семиугольника будут иметь множество меток $\rho_{\nu(p)} = \{0, 1, 2, 3\}$ и задаваться следующей таблицей:

$*$	0	1	2	3
0	$\{0\}$	$\{1\}$	$\{2\}$	$\{3\}$
1	$\{1\}$	$\{0, 2\}$	$\{1, 3\}$	$\{0, 2\}$
2	$\{2\}$	$\{1, 3\}$	$\{0, 2\}$	$\{1, 3\}$
3	$\{3\}$	$\{0, 2\}$	$\{1, 3\}$	$\{0, 2\}$

С каждым увеличением диаметра графа увеличивается и количество меток алгебры. Интересно отметить, что диаметр графа одинаковый для двух рядомстоящих графов с четным количеством вершин и нечетным. Например, диаметр для квадрата и пятиугольника одинаковый, далее для шестиугольника и семиугольника и так далее. Такая же зависимость диаметра графа наблюдается и в производных от них структурах.

Начнем с умножения квадрата на квадрат, постепенно увеличивая количество углов.

Алгебра для декартового произведения графа квадрата на граф квадрата $\mathfrak{QQ}$ с метками $\rho_{\nu(p)} = \{0, 1, 2, 3, 4\}$ задается следующей таблицей:

$*$	0	1	2	3	4
0	$\{0\}$	$\{1\}$	$\{2\}$	$\{3\}$	$\{4\}$
1	$\{1\}$	$\{0, 2\}$	$\{1, 3\}$	$\{0, 2, 4\}$	$\{1, 3\}$
2	$\{2\}$	$\{1, 3\}$	$\{0, 2, 4\}$	$\{1, 3\}$	$\{0, 2, 4\}$
3	$\{3\}$	$\{0, 2, 4\}$	$\{1, 3\}$	$\{0, 2, 4\}$	$\{1, 3\}$
4	$\{4\}$	$\{1, 3\}$	$\{0, 2, 4\}$	$\{1, 3\}$	$\{0, 2, 4\}$

Алгебра для декартового произведения графа квадрата на граф пятиугольника изоморфна $\mathfrak{QQ}$

Алгебра для декартового произведения графа квадрата на граф шестиугольника $\mathfrak{QH}$ с метками $\rho_{\nu(p)} = \{0, 1, 2, 3, 4, 5\}$ задается следующей таблицей:

$*$	0	1	2	3	4	5
0	$\{0\}$	$\{1\}$	$\{2\}$	$\{3\}$	$\{4\}$	$\{5\}$
1	$\{1\}$	$\{0, 2\}$	$\{1, 3\}$	$\{0, 2, 4\}$	$\{1, 3, 5\}$	$\{0, 2, 4\}$
2	$\{2\}$	$\{1, 3\}$	$\{0, 2, 4\}$	$\{1, 3, 5\}$	$\{0, 2, 4\}$	$\{1, 3, 5\}$
3	$\{3\}$	$\{0, 2, 4\}$	$\{1, 3, 5\}$	$\{0, 2, 4\}$	$\{1, 3, 5\}$	$\{0, 2, 4\}$
4	$\{4\}$	$\{1, 3, 5\}$	$\{0, 2, 4\}$	$\{1, 3, 5\}$	$\{0, 2, 4\}$	$\{1, 3, 5\}$
5	$\{5\}$	$\{0, 2, 4\}$	$\{1, 3, 5\}$	$\{0, 2, 4\}$	$\{1, 3, 5\}$	$\{0, 2, 4\}$

Алгебра для декартового произведения графа квадрата на граф семиугольника равна $\mathfrak{QH}$.

Алгебра для декартового произведения графа квадрата на граф восьмиугольника $\mathfrak{QO}$ с метками $\rho_{\nu(p)} = \{0, 1, 2, 3, 4, 5, 6\}$ задается следующей таблицей:

$*$	0	1	2	3	4	5	6
0	$\{0\}$	$\{1\}$	$\{2\}$	$\{3\}$	$\{4\}$	$\{5\}$	$\{6\}$
1	$\{1\}$	$\{0, 2\}$	$\{1, 3\}$	$\{0, 2, 4\}$	$\{1, 3, 5\}$	$\{0, 2, 4, 6\}$	$\{1, 3, 5\}$
2	$\{2\}$	$\{1, 3\}$	$\{0, 2, 4\}$	$\{1, 3, 5\}$	$\{0, 2, 4, 6\}$	$\{1, 3, 5\}$	$\{0, 2, 4\}$
3	$\{3\}$	$\{0, 2, 4\}$	$\{1, 3, 5\}$	$\{0, 2, 4, 6\}$	$\{1, 3, 5\}$	$\{0, 2, 4\}$	$\{1, 3, 5\}$
4	$\{4\}$	$\{1, 3, 5\}$	$\{0, 2, 4, 6\}$	$\{1, 3, 5\}$	$\{0, 2, 4\}$	$\{1, 3, 5\}$	$\{0, 2, 4\}$
5	$\{5\}$	$\{0, 2, 4, 6\}$	$\{1, 3, 5\}$	$\{0, 2, 4\}$	$\{1, 3, 5\}$	$\{0, 2, 4\}$	$\{1, 3, 5\}$
6	$\{6\}$	$\{1, 3, 5\}$	$\{0, 2, 4\}$	$\{1, 3, 5\}$	$\{0, 2, 4\}$	$\{1, 3, 5\}$	$\{0, 2, 4\}$

Алгебра для декартового произведения графа квадрата на граф девятиугольника равна $\mathfrak{QO}$.

Видно, что и тут алгебры идут парами. Это связано с диаметром полученного графа: для данного умножения равные диаметры графов дают равные алгебры. Далее буду описывать алгебры парами.

Алгебра для декартового произведения графа квадрата на граф десятиугольника и граф одиннадцатиугольника $\mathfrak{QO}$ с метками $\rho_{\nu(p)} = \{0, 1, 2, 3, 4, 5, 6, 7\}$ задается следующей таблицей:

$*$	0	1	2	3	4	5	6	7
0	$\{0\}$	$\{1\}$	$\{2\}$	$\{3\}$	$\{4\}$	$\{5\}$	$\{6\}$	$\{7\}$
1	$\{1\}$	$\{0, 2\}$	$\{1, 3\}$	$\{0, 2, 4\}$	$\{1, 3, 5\}$	$\{0, 2, 4, 6\}$	$\{1, 3, 5, 7\}$	$\{0, 2, 4, 6\}$
2	$\{2\}$	$\{1, 3\}$	$\{0, 2, 4\}$	$\{1, 3, 5\}$	$\{0, 2, 4, 6\}$	$\{1, 3, 5, 7\}$	$\{0, 2, 4, 6\}$	$\{1, 3, 5\}$
3	$\{3\}$	$\{0, 2, 4\}$	$\{1, 3, 5\}$	$\{0, 2, 4, 6\}$	$\{1, 3, 5, 7\}$	$\{0, 2, 4, 6\}$	$\{1, 3, 5\}$	$\{0, 2, 4, 6\}$
4	$\{4\}$	$\{1, 3, 5\}$	$\{0, 2, 4, 6\}$	$\{1, 3, 5, 7\}$	$\{0, 2, 4, 6\}$	$\{1, 3, 5\}$	$\{0, 2, 4, 6\}$	$\{1, 3, 5\}$
5	$\{5\}$	$\{0, 2, 4, 6\}$	$\{1, 3, 5, 7\}$	$\{0, 2, 4, 6\}$	$\{1, 3, 5\}$	$\{0, 2, 4, 6\}$	$\{1, 3, 5\}$	$\{0, 2, 4, 6\}$
6	$\{6\}$	$\{1, 3, 5, 7\}$	$\{0, 2, 4, 6\}$	$\{1, 3, 5\}$	$\{0, 2, 4, 6\}$	$\{1, 3, 5\}$	$\{0, 2, 4, 6\}$	$\{1, 3, 5\}$
7	$\{7\}$	$\{0, 2, 4, 6\}$	$\{1, 3, 5\}$	$\{0, 2, 4, 6\}$	$\{1, 3, 5\}$	$\{0, 2, 4, 6\}$	$\{1, 3, 5\}$	$\{0, 2, 4, 6\}$

Алгебра для декартового произведения графа квадрата на граф двенадцатиугольника и граф тринадцатиугольника $\mathfrak{QOod}$ с метками $\rho_{\nu(p)} = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ задается следующей таблицей:

*	0	1	2	3	4	5	6	7	8
0	{0}	{1}	{2}	{3}	{4}	{5}	{6}	{7}	{8}
1	{1}	{0, 2}	{1, 3}	{ 0, 2, 4 }	{ 1, 3, 5 }	{ 0, 2, 4, 6 }	{ 1, 3, 5, 7 }	{ 0, 2, 4, 6, 8 }	{ 1, 3, 5, 7 }
2	{2}	{1, 3}	{ 0, 2, 4 }	{ 1, 3, 5 }	{ 0, 2, 4, 6 }	{ 1, 3, 5, 7 }	{ 0, 2, 4, 6, 8 }	{ 1, 3, 5, 7 }	{ 0, 2, 4, 6 }
3	{3}	{ 0, 2, 4 }	{ 1, 3, 5 }	{ 0, 2, 4, 6 }	{ 1, 3, 5, 7 }	{ 0, 2, 4, 6, 8 }	{ 1, 3, 5, 7 }	{ 0, 2, 4, 6 }	{ 1, 3, 5, 7 }
4	{4}	{ 1, 3, 5 }	{ 0, 2, 4, 6 }	{ 1, 3, 5, 7 }	{ 0, 2, 4, 6, 8 }	{ 1, 3, 5, 7 }	{ 0, 2, 4, 6 }	{ 1, 3, 5, 7 }	{ 0, 2, 4, 6 }
5	{5}	{ 0, 2, 4, 6 }	{ 1, 3, 5, 7 }	{ 0, 2, 4, 6, 8 }	{ 1, 3, 5, 7 }	{ 0, 2, 4, 6 }	{ 1, 3, 5, 7 }	{ 0, 2, 4, 6 }	{ 1, 3, 5, 7 }
6	{6}	{ 1, 3, 5, 7 }	{ 0, 2, 4, 6, 8 }	{ 1, 3, 5, 7 }	{ 0, 2, 4, 6 }	{ 1, 3, 5, 7 }	{ 0, 2, 4, 6 }	{ 1, 3, 5, 7 }	{ 0, 2, 4, 6 }
7	{7}	{ 0, 2, 4, 6, 8 }	{ 1, 3, 5, 7 }	{ 0, 2, 4, 6 }	{ 1, 3, 5, 7 }	{ 0, 2, 4, 6 }	{ 1, 3, 5, 7 }	{ 0, 2, 4, 6 }	{ 1, 3, 5, 7 }
8	{8}	{ 1, 3, 5, 7 }	{ 0, 2, 4, 6 }	{ 1, 3, 5, 7 }	{ 0, 2, 4, 6 }	{ 1, 3, 5, 7 }	{ 0, 2, 4, 6 }	{ 1, 3, 5, 7 }	{ 0, 2, 4, 6 }

Алгебра для декартового произведения графа квадрата на граф четырнадцатиугольника и граф пятнадцатиугольника $\mathfrak{QT}$ с метками $\rho_{\nu(p)} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ задается следующей таблицей:

*	0	1	2	3	4	5	6	7	8	9
0	{0}	{1}	{2}	{3}	{4}	{5}	{6}	{7}	{8}	{9}
1	{1}	{0, 2}	{1, 3}	{0, 2, 4}	{1, 3, 5}	{0, 2, 4, 6}	{1, 3, 5, 7}	{0, 2, 4, 6, 8}	{1, 3, 5, 7, 9}	{0, 2, 4, 6, 8}
2	{2}	{1, 3}	{0, 2, 4}	{1, 3, 5}	{0, 2, 4, 6}	{1, 3, 5, 7}	{0, 2, 4, 6, 8}	{1, 3, 5, 7, 9}	{0, 2, 4, 6, 8}	{1, 3, 5, 7}
3	{3}	{0, 2, 4}	{1, 3, 5}	{0, 2, 4, 6}	{1, 3, 5, 7}	{0, 2, 4, 6, 8}	{1, 3, 5, 7, 9}	{0, 2, 4, 6, 8}	{1, 3, 5, 7}	{0, 2, 4, 6, 8}
4	{4}	{1, 3, 5}	{0, 2, 4, 6}	{1, 3, 5, 7}	{0, 2, 4, 6, 8}	{1, 3, 5, 7, 9}	{0, 2, 4, 6, 8}	{1, 3, 5, 7}	{0, 2, 4, 6, 8}	{1, 3, 5, 7}
5	{5}	{0, 2, 4, 6}	{1, 3, 5, 7}	{0, 2, 4, 6, 8}	{1, 3, 5, 7, 9}	{0, 2, 4, 6, 8}	{1, 3, 5, 7}	{0, 2, 4, 6, 8}	{1, 3, 5, 7}	{0, 2, 4, 6, 8}
6	{6}	{1, 3, 5, 7}	{0, 2, 4, 6, 8}	{1, 3, 5, 7, 9}	{0, 2, 4, 6, 8}	{1, 3, 5, 7}	{0, 2, 4, 6, 8}	{1, 3, 5, 7}	{0, 2, 4, 6, 8}	{1, 3, 5, 7}
7	{7}	{0, 2, 4, 6, 8}	{1, 3, 5, 7, 9}	{0, 2, 4, 6, 8}	{1, 3, 5, 7}	{0, 2, 4, 6, 8}	{1, 3, 5, 7}	{0, 2, 4, 6, 8}	{1, 3, 5, 7}	{0, 2, 4, 6, 8}
8	{8}	{1, 3, 5, 7, 9}	{0, 2, 4, 6, 8}	{1, 3, 5, 7}	{0, 2, 4, 6, 8}	{1, 3, 5, 7}	{0, 2, 4, 6, 8}	{1, 3, 5, 7}	{0, 2, 4, 6, 8}	{1, 3, 5, 7}
9	{9}	{0, 2, 4, 6, 8}	{1, 3, 5, 7}	{0, 2, 4, 6, 8}	{1, 3, 5, 7}	{0, 2, 4, 6, 8}	{1, 3, 5, 7}	{0, 2, 4, 6, 8}	{1, 3, 5, 7}	{0, 2, 4, 6, 8}

Опишем полученные алгебры в общем виде. Алгебру для декартового произведения квадрата на граф многоугольника с диаметром графа n

обозначим через $\mathfrak{QT}_n$. Она будет иметь метки $\rho_{\nu(p)} = \{0, 1, 2, 3, 4, 5, 6, \ldots, n\}$ и задаваться следующей таблицей Кэли:

$\cdot$	0	1	2	3	4	...	n
0	$\{0\}$	$\{1\}$	$\{2\}$	$\{3\}$	$\{4\}$	$\{\ldots\}$	$\{n\}$
1	$\{1\}$	$\{0,2\}$	$\{1,3\}$	$\{0,2,4\}$	$\{1,3,5\}$	$\{\ldots\}$	$\{F(n)\}$
2	$\{2\}$	$\{1,3\}$	$\{0,2,4\}$	$\{1,3,5\}$	$\{0,2,4,6\}$	$\{\ldots\}$	$\{F(n)\}$
3	$\{3\}$	$\{0,2,4\}$	$\{1,3,5\}$	$\{0,2,4,6\}$	$\{F(4+3)\}$	$\{\ldots\}$	$\{F(n)\}$
4	$\{4\}$	$\{1,3,5\}$	$\{0,2,4,6\}$	$\{F(4+3)\}$	$\{F(4+4)\}$	$\{\ldots\}$	$\{F(n)\}$
...	...	...	...	...	...	...	...
n	$\{m\}$	$\{F(\mathrm{n})\}$	$\{F(\mathrm{n})\}$	$\{F(\mathrm{n})\}$	$\{F(\mathrm{n})\}$	...	$\{F(n)\}$

где $F(x)$ — функция, которая возвращает метки в зависимости от четности x: если x четная, то получаем все четные метки, начиная с нуля до x, а если нечетная, то получаем все нечетные метки до x, где $x \leq n$.

Далее приведем диаметры графов и метки для алгебр перемножения квадрата. Используя их, можно получить таблицу, подставив значения в предыдущую таблицу.

Алгебра для декартового произведения графа квадрата на граф шестнадцатиугольника и граф семнадцатиугольника будет иметь метки $\rho_{\nu(p)} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

Алгебра для декартового произведения графа квадрата на граф восемнадцатиугольника и граф девятнадцатиугольника будет иметь метки $\rho_{\nu(p)} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$.

Алгебра для декартового произведения графа квадрата на граф двадцатиугольника и граф двадцатиодногоугольника будет иметь метки $\rho_{\nu(p)} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$.

Алгебра для произведения графа квадрата на граф девяностоугольника будет иметь 48 меток.

Алгебра для декартового произведения графа пятиугольника на граф четырехугольника и граф пятиугольника $\mathfrak{PT}$ с метками $\rho_{\nu(p)} = \{0, 1, 2, 3, 4\}$ задается следующей таблицей:

$*$	0	1	2	3	4
0	$\{0\}$	$\{1\}$	$\{2\}$	$\{3\}$	$\{4\}$
1	$\{1\}$	$\{0,2\}$	$\{1,3\}$	$\{0,2,4\}$	$\{1,3\}$
2	$\{2\}$	$\{1,3\}$	$\{0,2,4\}$	$\{1,3\}$	$\{0,2\}$
3	$\{3\}$	$\{0,2,4\}$	$\{1,3\}$	$\{0,2\}$	$\{1,3\}$
4	$\{4\}$	$\{1,3\}$	$\{0,2\}$	$\{1,3\}$	$\{0,2\}$

Алгебра для декартового произведения графа пятиугольника на граф шестиугольника и граф семиугольника $\mathfrak{PH}$ с метками $\rho_{\nu(p)} = \{0, 1, 2, 3, 4, 5\}$ задается следующей таблицей:

$*$	0	1	2	3	4	5
0	$\{0\}$	$\{1\}$	$\{2\}$	$\{3\}$	$\{4\}$	$\{5\}$
1	$\{1\}$	$\{0,2\}$	$\{1,3\}$	$\{0,2,4\}$	$\{1,3,5\}$	$\{0,2,4\}$
2	$\{2\}$	$\{1,3\}$	$\{0,2,4\}$	$\{1,3,5\}$	$\{0,2,4\}$	$\{1,3\}$
3	$\{3\}$	$\{0,2,4\}$	$\{1,3,5\}$	$\{0,2,4\}$	$\{1,3\}$	$\{0,2,4\}$
4	$\{4\}$	$\{1,3,5\}$	$\{0,2,4\}$	$\{1,3\}$	$\{0,2,4\}$	$\{1,3\}$
5	$\{5\}$	$\{0,2,4\}$	$\{1,3\}$	$\{0,2,4\}$	$\{1,3\}$	$\{0,2,4\}$

Алгебра для декартового произведения графа пятиугольника на граф восьмиугольника и граф девятиугольника $\mathfrak{PO}$ с метками $\rho_{\nu(p)} = \{0, 1, 2, 3, 4, 5, 6\}$ задается следующей таблицей:

$*$	0	1	2	3	4	5	6
0	$\{0\}$	$\{1\}$	$\{2\}$	$\{3\}$	$\{4\}$	$\{5\}$	$\{6\}$
1	$\{1\}$	$\{0,2\}$	$\{1,3\}$	$\{0,2,4\}$	$\{1,3,5\}$	$\{0,2,4,6\}$	$\{1,3,5\}$
2	$\{2\}$	$\{1,3\}$	$\{0,2,4\}$	$\{1,3,5\}$	$\{0,2,4,6\}$	$\{1,3,5\}$	$\{0,2,4\}$
3	$\{3\}$	$\{0,2,4\}$	$\{1,3,5\}$	$\{0,2,4,6\}$	$\{1,3,5\}$	$\{0,2,4\}$	$\{1,3,5\}$
4	$\{4\}$	$\{1,3,5\}$	$\{0,2,4,6\}$	$\{1,3,5\}$	$\{0,2,4\}$	$\{1,3,5\}$	$\{0,2,4\}$
5	$\{5\}$	$\{0,2,4,6\}$	$\{1,3,5\}$	$\{0,2,4\}$	$\{1,3,5\}$	$\{0,2,4\}$	$\{1,3,5\}$
6	$\{6\}$	$\{1,3,5\}$	$\{0,2,4\}$	$\{1,3,5\}$	$\{0,2,4\}$	$\{1,3,5\}$	$\{0,2,4\}$

Алгебра для декартового произведения графа пятиугольника на граф десятиугольника и граф одиннадцатиугольника $\mathfrak{PD}$ с метками $\rho_{\nu(p)} = \{0, 1, 2, 3, 4, 5, 6, 7\}$ задается следующей таблицей:

$*$	0	1	2	3	4	5	6	7
0	$\{0\}$	$\{1\}$	$\{2\}$	$\{3\}$	$\{4\}$	$\{5\}$	$\{6\}$	$\{7\}$
1	$\{1\}$	$\{0,2\}$	$\{1,3\}$	$\{0,2,4\}$	$\{1,3,5\}$	$\{0,2,4,6\}$	$\{1,3,5,7\}$	$\{0,2,4,6\}$
2	$\{2\}$	$\{1,3\}$	$\{0,2,4\}$	$\{1,3,5\}$	$\{0,2,4,6\}$	$\{1,3,5,7\}$	$\{0,2,4,6\}$	$\{1,3,5\}$
3	$\{3\}$	$\{0,2,4\}$	$\{1,3,5\}$	$\{0,2,4,6\}$	$\{1,3,5,7\}$	$\{0,2,4,6\}$	$\{1,3,5\}$	$\{0,2,4,6\}$
4	$\{4\}$	$\{1,3,5\}$	$\{0,2,4,6\}$	$\{1,3,5,7\}$	$\{0,2,4,6\}$	$\{1,3,5\}$	$\{0,2,4,6\}$	$\{1,3,5\}$
5	$\{5\}$	$\{0,2,4,6\}$	$\{1,3,5,7\}$	$\{0,2,4,6\}$	$\{1,3,5\}$	$\{0,2,4,6\}$	$\{1,3,5\}$	$\{0,2,4,6\}$
6	$\{6\}$	$\{1,3,5,7\}$	$\{0,2,4,6\}$	$\{1,3,5\}$	$\{0,2,4,6\}$	$\{1,3,5\}$	$\{0,2,4,6\}$	$\{1,3,5\}$
7	$\{7\}$	$\{0,2,4,6\}$	$\{1,3,5\}$	$\{0,2,4,6\}$	$\{1,3,5\}$	$\{0,2,4,6\}$	$\{1,3,5\}$	$\{0,2,4,6\}$

Алгебра для декартового произведения графа пятиугольника на граф многоугольника $\mathfrak{Pn}$ с диаметром n изоморфна алгебре $\mathfrak{OT}_n$.

Как видно из таблиц, алгебры с одинаковыми диаметрами графов будут изоморрфны, и они имеют одинаковые метки.

Лемма 2. *Алгебры бинарных изолирующих формул для теории декартового умножения графов многоугольников будут изоморфны, если имеют одинаковые метки.*

Алгебра для декартового произведения графа шестиугольника на граф шестиугольника и граф семиугольника $\mathfrak{HH}$ с метками $\rho_{\nu(p)} = \{0, 1, 2, 3, 4, 5, 6\}$ задается следующей таблицей:

$*$	0	1	2	3	4	5	6
0	$\{0\}$	$\{1\}$	$\{2\}$	$\{3\}$	$\{4\}$	$\{5\}$	$\{6\}$
1	$\{1\}$	$\{0,2\}$	$\{1,3\}$	$\{0,2,4\}$	$\{1,3,5\}$	$\{0,2,4,6\}$	$\{1,3,5\}$
2	$\{2\}$	$\{1,3\}$	$\{0,2,4\}$	$\{1,3,5\}$	$\{0,2,4,6\}$	$\{1,3,5\}$	$\{0,2,4\}$
3	$\{3\}$	$\{0,2,4\}$	$\{1,3,5\}$	$\{0,2,4,6\}$	$\{1,3,5\}$	$\{0,2,4\}$	$\{1,3,5\}$
4	$\{4\}$	$\{1,3,5\}$	$\{0,2,4,6\}$	$\{1,3,5\}$	$\{0,2,4\}$	$\{1,3,5\}$	$\{0,2,4\}$
5	$\{5\}$	$\{0,2,4,6\}$	$\{1,3,5\}$	$\{0,2,4\}$	$\{1,3,5\}$	$\{0,2,4\}$	$\{1,3,5\}$
6	$\{6\}$	$\{1,3,5\}$	$\{0,2,4\}$	$\{1,3,5\}$	$\{0,2,4\}$	$\{1,3,5\}$	$\{0,2,4\}$

Алгебра для декартового произведения графа шестиугольника на граф шестиугольника и граф семиугольника $\mathfrak{HH}$ с метками $\rho_{\nu(p)} = \{0, 1, 2, 3, 4, 5, 6, 7\}$ задается следующей таблицей:

$*$	0	1	2	3	4	5	6	7
0	$\{0\}$	$\{1\}$	$\{2\}$	$\{3\}$	$\{4\}$	$\{5\}$	$\{6\}$	$\{7\}$
1	$\{1\}$	$\{0,2\}$	$\{1,3\}$	$\{0,2,4\}$	$\{1,3,5\}$	$\{0,2,4,6\}$	$\{1,3,5,7\}$	$\{0,2,4,6\}$
2	$\{2\}$	$\{1,3\}$	$\{0,2,4\}$	$\{1,3,5\}$	$\{0,2,4,6\}$	$\{1,3,5,7\}$	$\{0,2,4,6\}$	$\{1,3,5\}$
3	$\{3\}$	$\{0,2,4\}$	$\{1,3,5\}$	$\{0,2,4,6\}$	$\{1,3,5,7\}$	$\{0,2,4,6\}$	$\{1,3,5\}$	$\{0,2,4,6\}$
4	$\{4\}$	$\{1,3,5\}$	$\{0,2,4,6\}$	$\{1,3,5,7\}$	$\{0,2,4,6\}$	$\{1,3,5\}$	$\{0,2,4,6\}$	$\{1,3,5\}$
5	$\{5\}$	$\{0,2,4,6\}$	$\{1,3,5,7\}$	$\{0,2,4,6\}$	$\{1,3,5\}$	$\{0,2,4,6\}$	$\{1,3,5\}$	$\{0,2,4,6\}$
6	$\{6\}$	$\{1,3,5,7\}$	$\{0,2,4,6\}$	$\{1,3,5\}$	$\{0,2,4,6\}$	$\{1,3,5\}$	$\{0,2,4,6\}$	$\{1,3,5\}$
7	$\{7\}$	$\{0,2,4,6\}$	$\{1,3,5\}$	$\{0,2,4,6\}$	$\{1,3,5\}$	$\{0,2,4,6\}$	$\{1,3,5\}$	$\{0,2,4,6\}$

Алгебра для декартового произведения графа шестиугольника на граф многоугольника $\mathfrak{Hn}$ с диаметром n изоморфна алгебре $\mathfrak{QT}_n$.

На основании полученного описания таблиц Кэли для алгебр бинарных изолирующих формул теорий декартовых умножений справедливы следующие теоремы.

Теорема 3. *Если в результате декартового умножения алгебр бинарных изолирующих для n-угольников получается хотя бы один симплекс, то алгебра для результата будет изоморфна алгебре симплексов* [2].

Теорема 4. *Если T — теория декартового произведения графов многоугольников друг на друга, $\mathfrak{B}$ — алгебра бинарных изолирующих формул теории T, то алгебра $\mathfrak{B}$ задается некоторой алгеброй $\mathfrak{QT}_n$.*

Список литературы

[1] D.Yu. Emelyanov, B.Sh. Kulpeshov, S.V. Sudoplatov, Algebras of binary formulas. — Novosibirsk : Edition of NSTU, 2023. 330 p. doi: 10.17212/978-5-7782-5028-4

[2] Д.Ю. Емельянов, Алгебры распределений бинарных изолирующих формул для теорий симплексов // Algebra and Model Theory 11: Collection of papers. Novosibirsk : NSTU Publisher, 2017. — P. 66–74.

ОБ АКСИОМАТИЗИРУЕМОСТИ КЛАССА ПОДПРЯМО НЕРАЗЛОЖИМЫХ ПОЛИГОНОВ НАД ПОЛУГРУППАМИ

И. Б. Кожухов, Д. С. Храмченок*

НИУ МИЭТ, МГУ им. Ломоносова, РАНХиГС
e-mail: kozhuhov_i_b@mail.ru, dmitrii.khramchenok@math.msu.ru

1 Введение

Универсальная алгебра называется *подпрямо неразложимой*, если она не разлагается в нетривиальное подпрямое произведение алгебр. Эти алгебры интересны тем, что согласно теореме Биркгофа [1, теорема 7.3] любая нетривиальная алгебра является подпрямым произведением подпрямо неразложимых алгебр. Класс алгебр называется *аксиоматизируемым*, если он определяется совокупностью аксиом — замкнутых формул логики первого порядка. Полигоном над полугруппой S называется множество X, на котором действует полугруппа S, т.е. определено отображение $X \times S \to X$, $(x, s) \to xs$ такое, что $x(st) = (xs)t$ при $x \in X$, $s, t \in S$. Пусть полугруппа S имеет единицу e, тогда полигон X над S называется *унитарным*, если $xe = x$ для любого $x \in X$. *Нулём* полигона X называется такой элемент θ, что $\theta s = \theta$ при всех $s \in S$. В отличие от колец и полугрупп полигон может иметь более одного нуля. Более того, существуют полигоны любой мощности, состоящие целиком из нулей.

Аксиоматизируемость некоторых классов полигонов изучалась в ряде работ. В [2] были получены необходимые и достаточные условия аксиоматизируемости классов проективных и плоских полигонов над моноидом. В [3, теорема 2] были охарактеризованы абелевы группы, над которыми класс подпрямо неразложимых полигонов аксиоматизируем, а в [4] была получена характеризация коммутативных моноидов с этим свойством.

В настоящей работе мы устанавливаем, что для любой полугруппы S (как конечной, так и бесконечной) и подпрямо неразложимого поли-

*Работа поддержана грантом РНФ №22-11-00052.

гона X над ней имеет место неравенство $|X| \leq 2^{|S^1|}$. Похожее неравенство $|X| \leq 2^{|R|}$ получено для подпрямо неразложимого модуля X над бесконечным ассоциативным кольцом R (в случае аксиоматизируемости класса подпрямо неразложимых модулей). Далее мы устанавливаем, что класс $\mathcal{K}$ подпрямо неразложимых полигонов над полугруппой либо неаксиоматизируем, либо существует натуральное число n такое, что $|X| \leq n$ для любого подпрямо неразложимого полигона X. Рассмотрим следующее условие на полугруппу S:

(1) Существует натуральное число n такое, что $|X| \leq n$ для любого подпрямо неразложимого полигона X.

Это условие равносильно тому, что любой полигон есть подпрямое произведение полигонов с не более, чем n, элементами. В работе [5] было доказано, что полугруппа S, удовлетворяющая условию (1), равномерно локально конечна, т.е. существует функция $f(k)$ натурального аргумента такая, что $|\langle a_1, \ldots, a_k\rangle| \leq f(k)$ для любых $a_1, \ldots, a_k \in S$, где $\langle a_1, \ldots, a_k\rangle$ обозначает подполугруппу, порождённую элементами $a_1, \ldots, a_k$. В теореме 6 из [6] было показано, что для абелевой группы S условие (1) равносильно ограниченности группы S, т.е. $a^n = 1$ для некоторого n и всех $s \in S$. Условие (1) позволяет доказать, что если S — группа (необязательно коммутативная), то класс $\mathcal{K}$ аксиоматизируем в том и только том случае, когда S конечна. Это обобщает упомянутый ранее результат из [3]. Отметим, что для полугрупп, не являющихся группами, данное утверждение верно лишь в одну сторону, а именно, над конечной полугруппой класс $\mathcal{K}$ подпрямо неразложимых полигонов аксиоматизируем (даже конечно аксиоматизируем), но этот класс может быть аксиоматизируем и для некоторых бесконечных полугрупп. Первое утверждение можно доказать на основе теоремы 4.2 из [10] (см. также [13]), а второе получается следующим образом. По теореме 1 из [12] над полурешёткой (т.е. коммутативной полугруппой идемпотентов) подпрямо неразложимые полигоны — это в точности полигоны X такие, что $|X| \leq 2$, а значит, класс $\mathcal{K}$ аксиоматизируем, в то же время полурешётки могут иметь любую мощность.

Основные сведения из универсальной алгебры можно найти в [1], теории полугрупп — в [7], теории групп – в [8], теории полигонов — в [9, 10], математической логики — в [11].

2 Предварительные рассмотрения

Для универсальной алгебры A обозначим через $\mathrm{Con}A$ решётку её конгруэнций. Хорошо известно, что $\mathrm{Con}A$ — полная решётка с наимень-

шим элементом $\Delta = \{(a,a)|a \in A\}$ (*отношение равенства*). Алгебру A назовём *нетривиальной*, если $|A| > 1$, конгруэнция $\rho \in \mathrm{Con}A$ нетривиальна, если $\rho \neq \Delta$. Нетрудно проверить, что нетривиальная алгебра A подпрямо неразложима тогда и только тогда, когда она имеет наименьшую нетривиальную конгруэнцию. О подпрямо неразложимых полигонах над полугруппами можно прочитать в [10, §4.1]. В случае модуля над кольцом существует очевидный изоморфизм решётки конгруэнций и решётки подмодулей, поэтому ненулевой модуль подпрямо неразложим в том и только том случае, если он имеет наименьший ненулевой подмодуль.

Для полугруппы S обозначим через S^1 полугруппу, полученную присоединением к полугруппе S внешним образом единицы: $S^1 = S \cup \{1\}$. Это определение не совпадает с общепринятым, в котором единица присоединяется к S, только если в S нет единицы. Мы же присоединяем единицу $1 \notin S$ в любом случае, даже если в S уже была единица. Полигон X над S можно сделать полигоном над S^1, если положить $x \cdot 1 = x$ для всех $x \in X$. Этот полигон унитарный. Кроме того, как нетрудно проверить, у полигона X_S (над S) и полигона X_{S^1} (над S^1) одни и те же конгруэнции, поэтому X_S подпрямо неразложим, если и только если X_{S^1} подпрямо неразложим.

Аналогичную операцию — присоединение единицы можно проделать для колец. Действительно, пусть R — кольцо. На абелевой группе $\mathbb{Z} \oplus R$ определим умножение по формуле

$$(n,r) \cdot (n',r') = (nn', nr' + n'r + rr'). \tag{2}$$

Если кольцо R конечно, то $nR = 0$ при некотором n, и мы определим умножение на группе $\mathbb{Z}_n \oplus R$ по той же формуле (2). В обоих случаях мы получим кольцо с единицей, которое содержит кольцо R в качестве подкольца. Обозначим полученное кольцо с умножением (2) через R^1. Если кольцо R ассоциативно, то R^1 тоже ассоциативно. Всякий модуль X над кольцом R будет являться модулем над кольцом R^1, если положить $x \cdot (n,r) = nx + xr$ для $x \in X$, $(n,r) \in R^1$. Нетрудно проверить, что у модулей X_R (над R) и X_{R^1} (над R^1) одни и те же подмодули, поэтому X_R подпрямо неразложим, если и только если X_{R^1} подпрямо неразложим.

Полигон X над полугруппой S является *унарной алгеброй*, т.е. алгеброй, все операции которой унарны: для каждого $s \in S$ отображение $\varphi_s : X \to X$, $x \to xs$ и является той самой унарной операцией. Таким образом, полигон является универсальной алгеброй, сигнатуру которой можно отождествить с полугруппой S. Отсюда следует, что в категории

всех полигонов над фиксированной полугруппой существуют прямые произведения и копроизведения. Нетрудно проверить, что *копроизведением* семейства полигонов $\{X_i | i \in I\}$ является их дизъюнктное объединение, т.е. их объединение, если они попарно не пересекаются (если они имеют пересечения, берём попарно не пересекающиеся их изоморфные копии). Копроизведение будем обозначать следующим образом: $\coprod_{i \in I} X_i$.

Со всяким полигоном X можно связать граф, считая X множеством вершин, а пары (x, xs) $(x \in X,\ s \in S)$ — рёбрами. Полигон называется *связным*, если соответствующий граф связен. Очевидно, каждый полигон является копроизведением своих связных подполигонов (*компонент связности*).

3 Полигоны над группами

Пусть G — группа, H — её подгруппа, необязательно нормальная. Через G/H обозначим множество правых смежных классов Hg $(g \in G)$. Оно является полигоном над группой G, если положить $Hg \cdot g' = Hgg'$. Полигон G/H унитарный и *циклический* (т.е. порождается одним элементом). Более того, этот полигон простой (т.е. не имеет подполигонов, отличных от него самого), поэтому он порождается любым своим элементом. Нетрудно показать, что верно и обратное, т.е. любой унитарный циклический полигон над группой G изоморфен полигону G/H для некоторой подгруппы H. Далее, хорошо известно, что при действии группы G с единицей e на множестве X, если действие унитарно (т.е. $xe = x$ при всех $x \in X$), то множество X распадается на попарно не пересекающиеся орбиты. На языке полигонов этот факт и предыдущее утверждение можно сформулировать так: унитарные полигоны над группой G — это в точности полигоны вида $\coprod_{i \in I} G/H_i$, где $\{H_i | i \in I\}$ — семейство подгрупп группы G.

Подпрямо неразложимые полигоны над группой были охарактеризованы в работе [5]. Приведём эту характеризацию.

Теорема 1. *[5, теорема 6]. Нетривиальный полигон X над группой G подпрямо неразложим в том и только том случае, если выполнено одно из следующих условий:*

(i) $X = \{x, \theta\}$ и $xG = \theta G = \{\theta\}$;

(ii) $X \cong G/H$ для некоторой подгруппы H такой, что существует наименьшая подгруппа $H' \supset H$;

(iii) $X \cong G/H \sqcup \{\theta\}$, где θ — нуль, а G/H удовлетворяет требованиям из (ii).

В этой теореме полигон с условием (i) неунитарный, а (ii) и (iii) — унитарные. В условии (ii) полигон связный, а в (iii) несвязный.

4 Ограниченность мощности подпрямо неразложимых объектов

Докажем утверждения об ограниченности сверху мощностей подпрямо неразложимых полигонов, модулей.

Теорема 2. *Для любой полугруппы S и подпрямо неразложимого полигона X над S имеет место неравенство $|X| \leq 2^{|S^1|}$.*

Доказательство. Пусть X подпрямо неразложим, тогда существует ρ — наименьшая нетривиальная конгруэнция на X. Пусть $a \neq b$ — произвольные элементы X, удовлетворяющие условию $a\rho b$. Для произвольного $x \in X$ рассмотрим множество $A_x = \{s \in S^1 \mid xs = a\}$. Определим бинарное отношение $\sim$ следующим образом: $x \sim y \Longleftrightarrow A_x = A_y$. Очевидно, что $\sim$ — отношение эквивалетности. Пусть $x \sim y \in X$ и $t \in S^1$. Тогда $A_{xt} = \{s \in S^1 \mid xts = a\} = \{s \in S^1 \mid ts \in A_x\} = \{s \in S^1 \mid ts \in A_y\} = \{s \in S^1 \mid yts = a\} = A_{yt}$, а значит $xt \sim yt$, то есть $\sim$ — конгруэнция. Заметим, что $1 \in A_a$, но $1 \notin A_b$, то есть $a \nsim b$. Однако любая нетривиальная конгруэнция должна содержать ρ, а значит a и b должны быть эквивалентны, то есть $\sim = \Delta$. Рассмотрим отображение $f : X \mapsto 2^{S^1}$, ставящее каждому $x \in X$ в соответствие A_x. Из доказанного выше следует, что f — инъекция, а значит $|X| \leqslant |2^{S^1}|$.

Теорема 3. *Пусть R — ассоциативное кольцо, X — подпрямо неразложимый правый R-модуль, $\mathfrak{m} = \max\{|R|, \aleph_0\}$. Тогда $|X| \leq 2^{\mathfrak{m}}$.*

Доказательство. Утверждение очевидно при $X = 0$. Далее считаем, что $X \neq 0$. Так как X — подпрямо неразложимый R-модуль, то X как модуль над кольцом R^1 тоже подпрямо неразложим. Очевидно, $|R^1| \leq \mathfrak{m}$. Пусть K — ядро полигона X, т.е. наименьший ненулевой подполигон. Так как любой ненулевой подмодуль модуля X содержит K, то X — существенное расширение полигона K. Следовательно, мы можем считать, что $X \subseteq E(K)$, где $E(K)$ — инъективная оболочка модуля K. Так как K — простой полигон, то $K = aR^1$ для любого ненулевого элемента $a \in K$. Следовательно, $|K| \leq |R^1| \leq \mathfrak{m}$. Рассмотрим K как абелеву группу относительно сложения и вложим её в делимую абелеву группу D, при этом можно считать, что $|D| \leq \mathfrak{m}$. Тогда $E(K) \subseteq \mathrm{Hom}_{\mathbb{Z}}(K, D)$

(см. п. 57.8 в [15]). Отсюда следует, что $|E(K)| \leq |D|^{|K|} \leq \mathfrak{m}^{\mathfrak{m}} = 2^{\mathfrak{m}}$. Таким образом, $|X| \leq 2^{\mathfrak{m}}$. □

Более сильное условие на порядки подпрямо неразложимых полигонов получатся, если потребовать аксиоматизируемость.

Предложение 4. *Пусть S — полугруппа. Если класс $\mathcal{K}$ подпрямо неразложимых полигонов над S аксиоматизируем, то существует натуральное число n такое, что $|X| \leq n$ для любого подпрямо неразложимого полигона $X \in \mathcal{K}$.*

Доказательство. Предположим, что класс $\mathcal{K}$ аксиоматизируем. Если он содержит бесконечный полигон мощности $\mathfrak{p}$, то по теореме Лёвенгейма – Скулема – Тарского (см. [14, следствие 2.1.6]) существуют подпрямо неразложимые полигоны любой мощности $\geq \mathfrak{p}$. Однако, это противоречит теореме 1. Значит, всякий подпрямо неразложимый полигон конечен. Если существуют сколь угодно большие по количеству элементов конечные полигоны из $\mathcal{K}$, то в $\mathcal{K}$ есть бесконечный полигон, что невозможно. □

5 Доказательство конечности группы

Всюду далее G будет обозначать группу с единицей e. Аксиоматизируемость того или иного класса полигонов мы понимаем как наличие совокупности формул логики первого порядка в сигнатуре $\langle \cdot, = \rangle$, определяющей этот класс.

Рассмотрим следующие классы полигонов над группой G:

$\mathcal{K}$ — класс всех подпрямо неразложимых полигонов;

$\mathcal{K}'$ — класс всех унитарных подпрямо неразложимых полигонов;

$\mathcal{K}''$ — класс всех унитарных несвязных подпрямо неразложимых полигонов.

Лемма 5. *Если класс $\mathcal{K}$ аксиоматизируем, то класс $\mathcal{K}'$ также аксиоматизируем.*

Доказательство. Достаточно к формулам, определяющим $\mathcal{K}$, добавить формулу $\forall x \;\; xe = x$.

Чтобы аксиоматизировать класс $\mathcal{K}''$, расширим сигнатуру, добавив константный символ θ. □

Лемма 6. *Если класс $\mathcal{K}'$ аксиоматизируем в сигнатуре $\langle \cdot, = \rangle$, то класс $\mathcal{K}''$ аксиоматизируем в сигнатуре $\langle \cdot, =, \theta \rangle$.*

Доказательство. По теореме 1 несвязные унитарные подпрямо неразложимые полигоны над группой — это в точности такие полигоны из $\mathcal{K}'$, которые имеют нуль и содержат не менее двух элементов. Таким образом, к формулам, определяющим класс $\mathcal{K}'$, достаточно добавить формулу $\exists x\, \exists y\ \ x \neq y$ и совокупность формул $\theta g = \theta$ для всех $g \in G$. $\square$

Согласно предложению 5, если класс подпрямо неразложимых полигонов аксиоматизируем, то $|X| \leq n$ для некоторого натурального числа n и всех $X \in \mathcal{K}$. Пусть $n = \max\{|X| : X \in \mathcal{K}\}$. Для каждого m такого, что $2 \leq m \leq n-1$. Обозначим через $\mathcal{K}''_m$ класс всех полигонов порядка $m+1$ из класса $\mathcal{K}''$. Разобьём класс $\mathcal{K}''_m$ на классы изоморфных друг другу полигонов и обозначим через Γ множество этих классов. Возьмём по одному представителю из каждого такого класса. Получим множество $\{X_\gamma | \gamma \in \Gamma\}$.

Для группы G и натурального числа m рассмотрим неупорядоченные наборы $\overline{g} = (g_1, \ldots, g_m)$ элементов из G. Пусть $\overline{G}$ — множество всех наборов. Введём в рассмотрение формулу

$$\varphi_{\overline{g}} \equiv \exists x \bigwedge_{1 \leq i < j \leq m} x g_i \neq x g_j.$$

Следующая лемма является видоизменением леммы 3 из [3] применительно к нашей ситуации. Мы пишем $A \models \varphi$, если на модели A истинна замкнутая формула φ логики первого поорядка.

Лемма 7. *Пусть G — группа такая, что класс $\mathcal{K}$ всех подпрямо неразложимых полигонов над G, $n = \max\{|X| : X \in \mathcal{K}\}$ и $2 \leq m \leq n-1$. Тогда существует конечное множество наборов $\overline{g}^{(1)}, \ldots, \overline{g}^{(t)} \in \overline{G}$ такое, что во всех полигонах из $\mathcal{K}''_m$ истинна формула*

$$\psi_m \equiv \varphi_{\overline{g}^{(1)}} \vee \ldots \vee \varphi_{\overline{g}^{(t)}}. \tag{3}$$

Доказательство. Для каждого набора $\overline{g}$ пусть $\Gamma_{\overline{g}} = \{\gamma \in \Gamma | X_\gamma \models \varphi_{\overline{g}}\}$ и $\mathcal{D} = \{\Gamma \setminus \Gamma_{\overline{g}} | \overline{g} \in \overline{G}\}$. Далее ситуация разбивается на два случая.

1-й случай: $\mathcal{D}$ — центрированная система, т.е. пересечение любой конечной совокупности элементов из $\mathcal{D}$ непусто. Тогда существует ультрафильтр $\mathcal{U} \supseteq \mathcal{D}$. Пусть $Y = \prod_{\gamma \in \Gamma}^{\mathcal{U}} X_\gamma$ — ультрапроизведение полигонов X_γ по ультрафильтру $\mathcal{U}$. Так как $|X_\gamma| = m+1$ для каждого $\gamma \in \Gamma$, то по теореме Лося [11, §17, теорема 1] $|Y| = m+1$. Так как класс $\mathcal{K}''_m$ аксиоматизируем и каждый входящий в него полигон имеет нуль, то по теореме Лося, лемме 7 и теореме 1 $Y \cong G/H \sqcup \{0\}$, где G/H — подпрямо неразложимый полигон такой, что $|G/H| = m$. Пусть $g_1, \ldots, g_m$ — представители правых смежных классов группы G по подгруппе H. Тогда

$Hg_1, \ldots, Hg_m$ — различные элементы из Y, поэтому на Y истинна формула $\varphi_{\overline{g}}$ для $\overline{g} = (g_1, \ldots, g_n)$. Тогда по теореме Лося $\{\gamma | X_\gamma \models \varphi_{\overline{g}}\} \in \mathcal{U}$, т.е. $\Gamma_{\overline{g}} \in \mathcal{U}$. Но $\Gamma \setminus \Gamma_{\overline{g}} \in \mathcal{D} \subseteq \mathcal{U}$. Это противоречит тому, что $\mathcal{U}$ — фильтр.

2-й случай: $\mathcal{D}$ не является центрированной системой. Тогда

$$(\Gamma \setminus \Gamma_{\overline{g}^{(1)}}) \cap \ldots \cap (\Gamma \setminus \Gamma_{\overline{g}^{(t)}}) = \emptyset$$

при некоторых $\overline{g}^{(1)}, \ldots, \overline{g}^{(t)} \in \overline{G}$. Следовательно,

$$\bigcup_{i=1}^{t} \Gamma_{\overline{g}^{(i)}} = \Gamma. \tag{4}$$

Возьмём любой полигон $X \in \mathcal{K}''_m$. Тогда $X \cong X_\gamma$ при некотором $\gamma \in \Gamma$. Из (4) следует, что $\gamma \in \Gamma_{\overline{g}^{(i)}}$ при некотором $i \leq t$. Поэтому на X_γ истинна формула $\varphi_{\overline{g}^{(i)}}$. Таким образом, на X_γ истинна формула

$$\varphi_{\overline{g}^{(1)}} \vee \ldots \varphi_{\overline{g}^{(t)}}.$$

□

Теперь мы можем доказать конечность группы G, над которой класс $\mathcal{K}$ аксиоматизируем. Доказательство будет во многом следовать доказательству теоремы 2 из [3].

Теорема 8. *Пусть G — группа. Тогда класс $\mathcal{K}$ всех подпрямо неразложимых полигонов над G аксиоматизируем в том и только том случае, если G конечна.*

Доказательство. Мы можем доказывать лишь необходимость, так как доказательство достаточности схематически изложено во введении. Предположим, что группа G бесконечна, а класс $\mathcal{K}$ аксиоматизируем. Приведём это предположение к противоречию.

Согласно предложению 5 все $X \in \mathcal{K}$ конечны и их порядки ограничены сверху одним и тем же натуральным числом. Пусть $n = \max\{|X| : X \in \mathcal{K}\}$.

По лемме 8 на каждом из полигонов $X \in \mathcal{K}''_m$ истинна формула ψ_m (см. (3)). Для каждого m такого, что $2 \leq m \leq n-1$, мы имеем: $\psi_m \equiv \varphi_{\overline{g}^{(1)}} \vee \ldots \varphi_{\overline{g}^{(t_m)}}$. Положим $T_m = \{g_i^{(j)} | i \leq m,\ j \leq t_m\}$ и $T = \bigcup_{m=2}^{m-1} T_m$. Ясно, что T — конечное подмножество группы G. Оно порождает подгруппу $F = \langle T \rangle$, которая конечна по теореме 9 из [5]. Так как группа G бесконечна, то $F \neq G$. Возьмём любое $g \in G \setminus F$. По лемме Цорна существует подгруппа H группы G, максимальная относительно условий $H \supseteq F$ и $H \not\ni g$. Так как H максимальна, то подгруппа

$H' = \langle H, g\rangle$, порождённая группой H и элементом g, содержится в любой подгруппе H_1 такой, что $H_1 \supset H$. Значит, по теореме 6 из [5] полигон G/H подпрямо неразложим. Тогда полигон $X = G/H \sqcup \{0\}$ тоже подпрямо неразложим, причём $m = |G/H| \leq n - 1$.

Равенство $m = 1$ невозможно, так как оно приводит к равенству $G = H$, что противоречит соотношению $g \notin H$. Таким образом, $m \geq 2$.

По лемме 8 на X истинна формула ψ_m, а значит, существует $x \in X$ такое, что элементы $xg_1, \ldots, xg_m$ различны для некоторых $g_1, \ldots, g_m \in T_m$. Так как $m \geq 2$, то $x \neq 0$, поэтому $x \in G/H$, т.е. $x = Ha$ при некотором $a \in G$. Итак, $Hag_1, \ldots, Hag_m$ — различные смежные классы, поэтому $a^{-1}Hag_1, \ldots, a^{-1}Hag_m$ также различны. Так как подгруппа H имеет индекс m, то сопряжённая с ней подгруппа $a^{-1}Ha$ тоже имеет индекс m. Следовательно, $G = \bigcup_{i=1}^{m} a^{-1}Hag_i$. Но тогда также $G = \bigcup_{i=1}^{m} Hag_i$. Так как $g_1, \ldots, g_m \in T_m$, то $g_1, \ldots, g_m \in F$. Следовательно, $G = HaF$. Но $F \subseteq H$, поэтому $G = HaH$. Отсюда $e = h_1ah_2$ при некоторых $h_1, h_2 \in H$. Это означает, что $a \in H$, поэтому $G = H$. Мы снова получили противоречие с тем, что $g \notin H$.Полученное противоречие завершает доказательство теоремы. □

Список литературы

[1] P.M. Cohn, Universal algebra. Harper & Row, 1965, xv + 333 pp. [П. Кон. Универсальная алгебра. М., Мир, 1968, 353 с.]

[2] V. Gould, Axiomatisability problems for S-systems // J. London Math. Soc., 1987, v. 35, pp. 193–201.

[3] A.A. Stepanova, D.O. Ptakhov, Axiomatizability of the class of subdirectly irreducible acts over an Abelian group // Algebra and Logic, 59:5 (2020), 395—403. [А.А. Степанова, Д.О. Птахов, Аксиоматизируемость класса подпрямо неразложимых полигонов над абелевой группой // Алгебра и логика, 59:5 (2020), 582—593.]

[4] A.A. Stepanova, E.L. Efremov, Axiomatizability of the class of subdirectly irreducible S-acts over a commutative monoid // Algebra and Logic, 2024, v. 62, pp. 179—200. [А.А. Степанова, Е.Л. Ефремов. Аксиоматизируемость класса подпрямо неразложимых полигонов над коммутативным моноидом // Алгебра и логика, 62:2 (2023), 266—296.]

[5] I.B. Kozhukhov, A.R. Khaliullina, Semigroups with finitely approximated finite acts // Yakutian Math. J., 2014, v. 21, no. 3(83), pp. 52–57. [И.Б. Кожухов, А.Р. Халиуллина. Полугруппы

с финитно аппроксимируемыми полигонами // Матем. заметки СВФУ, 2014, т. 21, № 3 (83), с. 60–67.]

[6] I.B. Kozhukhov, A.V. Tsarev, Abelian groups with finitely approximated acts // J. Math. Sci., 2021, v. 259, pp. 438–443. [И.Б. Кожухов, А.В. Царёв, Абелевы группы с финитно аппроксимируемыми полигонами // Фундамент. и прикл. матем., 22:5 (2019), 81—89.]

[7] A.H. Clifford, G.B. Preston, The algebraic theory of semigroups. Vol. 1 and vol. 2. - Providence, American mathematical Society, 1961 and 1967 (Mathematical Surveys, 7). [А. Клиффорд, Г. Престон. Алгебраическая теория полугрупп: М., Мир, 1972, т. 1, 2, 286 + 432 pp.]

[8] A.G. Kurosh, The theory of groups v. 1,2, Chelsea, N.-Y., 1955. 272 pp.; 308 pp. [А.Г. Курош. Теория групп. Мир, М., 1967, 648 с.]

[9] M. Kilp, U. Knauer, A.V. Mikhalev, Monoids, acts and categories. N.Y. – Berlin, W. de Gruyter, 2000, xvii + 529 pp.

[10] I.B. Kozhukhov, A.V. Mikhalev, Acts over semigroups // J. Math. Sci., 2023, v. 269, pp. 362-401. [И.Б. Кожухов, А.В. Михалёв, Полигоны над полугруппами // Фундамент. и прикл. матем., 23:3 (2020), 141—199.]

[11] Yu.L. Ershov, E.A. Palyutin, Mathematical logic. Revised English translation by Shokurov Vladimir of the preceding. Mir Publishers, Moscow, 1984, 303 pp. - Volume 51 Issue 3 - Elliott Mendelson. [Ю.Л. Ершов, Е.А. Палютин. Математическая логика. М., Наука, 1987, 336 с.]

[12] I.B. Kozhukhov, One characteristical property of semilattices // Commun. Algebra, 1997, v. 25, N 8, pp. 2569–2577.

[13] D.S. Khramchenok, On the axiomatizability of some classes of acts over semigroups // Mosc. Univ. Math. Bull. Univ. Ser. 1. Mat. Mekh., 2024 (in press). [Д.С. Храмченок, Об аксиоматизируемости некоторых классов полигонов над полугруппами // Вестн. Моск. Ун-та. Сер 1. Математика, механика (в печати)]

[14] C.C. Chang, H.J. Keisler, Model theory. Studies in Logic and Foundations of Mathematics, 1973. [Г. Кейслер, Ч.Ч. Чен. Теория моделей. Мир, М., 1977, 614 с.]

[15] C.W. Curtis, I. Reiner, Representation theory of finite groups and associative algebras. AMS, 1966, 689 pp. [Ч. Кэртис, И. Райнер. Теория представлений конечных групп и ассоциативных алгебр. М. Наука, 1969. 668 с.]

ON PSEUDO-STRONGLY-MINIMAL FORMULAE, STRUCTURES AND THEORIES

B.Sh. Kulpeshov, In.I. Pavlyuk, S.V. Sudoplatov*

Institute of Mathematics and Mathematical Modeling,
125, Pushkin street, Almaty, 050010, Kazakhstan;
Kazakh British Technical University,
59, Tole Bi street, Almaty 050000, Kazakhstan;
Novosibirsk State Technical University,
20, K.Marx avenue, Novosibirsk, 630073, Russia;
Sobolev Institute of Mathematics,
4, Acad. Koptyug avenue, Novosibirsk, 630090, Russia
e-mail: kulpesh@mail.ru, pavlyuk@corp.nstu.ru, sudoplat@math.nsc.ru

In a series of papers various approximations of infinite structures by finite ones, i.e. pseudofiniteness are studied [1, 2, 3, 4] including finite approximations of strongly minimal structures [5].

We continue to study possibilities of approximations of theories with respect to given families of theories [6, 7, 8]. At the present paper we consider and describe some possibilities of approximations by strongly minimal structures and theories. Some kinds of approximating formulae in this case are described, too.

For theories of signatures Σ^1 without non-trivial definable n-ary relations, for $n > 1$, we prove a trichotomy theorem according to which each such theory either belongs to the class of theories with finite models, or belongs to the class of strongly minimal theories, or belongs to the class of pseudo-strongly-minimal theories. The last two cases are united by the class of pseudofinite theories. That trichotomy shows that each signature with unary predicates has a pseudo-strongly-minimal theory. It confirms that the class

*The work is partially supported by by Science Committee of Ministry of Science and Higher Education of the Republic of Kazakhstan, Grant No. AP19674850, and was carried out in the framework of the State Contract of the Sobolev Institute of Mathematics, Project No. FWNF-2022-0012.

of pseudo-strongly-minimal theories starts by signatures with at least one n-ary predicate or function, for $n \geq 1$.

1 Pseudo-strongly-minimal formulae and their properties

In this section, we define the notion of pseudo-strongly-minimal formula as an approximating formula [7] of special form, and consider some properties of these formulae.

Throughout we consider complete elementary theories of a signature Σ, where that signature for a family $\mathcal{T}$ of theories is denoted by $\Sigma(\mathcal{T})$.

We denote by $\mathcal{T}_\Sigma$ the family of all complete theories in a signature Σ.

As usual $F(\Sigma)$ collects the set of all formulae of the signature Σ, and $\mathrm{Sent}(\Sigma)$ denotes the set of all sentences of the signature Σ.

Recall [9] that a theory T without finite models is called *strongly minimal* if for any model $\mathcal{M} \models T$ and any its formula $\varphi(x, \overline{a})$, with parameters $\overline{a}$, either $\varphi(\mathcal{M}, \overline{a})$ or $\neg\varphi(\mathcal{M}, \overline{a})$ is finite. Models of a strongly minimal theory are *strongly minimal*, too.

We denote by $\mathcal{T}_\Sigma^{\mathrm{sm}}$ the set of all strongly minimal theories in the signature Σ.

The following definition modifies the definition of pseudo-countably-categorical formula [8].

Definition. For the family $\mathcal{T}_\Sigma^{\mathrm{sm}}$, a formula $\varphi = \varphi(\overline{x})$ is called *pseudo-strongly-minimal*, if φ is satisfied in a model of an accumulation point T of the family $\mathcal{T}_\Sigma^{\mathrm{sm}}$, which is not strongly minimal. Here, following [6], we consider accumulation points for a family $\mathcal{T}$ of theories under neighbourhoods $\mathcal{T}_\varphi = \{T_0 \in \mathcal{T} \mid \varphi \in T_0\}$ for sentences φ.

When considered independently, the formula φ is called *pseudo-strongly-minimal*, if it is pseudo-strongly-minimal with respect to a suitable signature $\Sigma \supseteq \Sigma(\varphi)$.

The set of pseudo-strongly-minimal formulae of the signature Σ is denoted by $\mathrm{PSMF}(\Sigma)$, and the set $\mathrm{PSMF}(\Sigma) \cap \mathrm{Sent}(\Sigma)$ of all pseudo-strongly-minimal sentences of the signature Σ is denoted by $\mathrm{PSMS}(\Sigma)$.

As the following remarks show the behavior of pseudo-strongly minimal formulae is similar to pseudo-countably categorical ones [8].

Remark 1.1. By definition, any pseudo-strongly-minimal formula refers both to strongly minimal theories, and due to approximation there are in-

finitely many such theories, and to theories that are not strongly minimal, but cannot be separated from strongly minimal theories by any sentences.

Since restrictions of strongly minimal theories are strongly minimal, too, it does not depend what a strongly minimal expansion of a strongly minimal structure, satisfying a given pseudo-strongly-minimal formula, is considered.

At the same time the considered signature is essential for approximations of accumulation points. For instance, the formula $x \approx x$ is satisfied in any strongly minimal structure, in particular, in an infinite structure of the empty signature, which can not produce accumulation points, whereas it is pseudo-strongly-minimal for the signature Σ_1 of unary predicate P, where P divides universes of structures into two parts such that one of them is unboundedly finite in models of theories in $\mathcal{T}^{\rm sm}_{\Sigma_1}$. In fact, in such a case, there is unique accumulation point T^* outside $\mathcal{T}^{\rm sm}_{\Sigma_1}$: the theory with infinite and co-infinite predicate P. The formulae $P(x)$, $\neg P(x)$, $\exists x\, P(x)$, $\exists x\, \neg P(x)$ are pseudo-strongly-minimal that is witnessed by T^*, and the formulae $\forall x\, P(x)$ and $\forall x\, \neg P(x)$ are pseudo-strongly-minimal but with respect to a extended signature, for instance, by new unary predicate P'.

We observe for the signature $\Sigma = \{f^{(1)}\}$ that the sentence

$$\varphi^n_f = \forall y \exists^{=n} x f(x) \approx y \wedge \forall x \neg x \approx f(x)$$

belongs to the set $\mathrm{PSMS}(\Sigma)$ since models for φ^n_f can have infinitely many cycles of different lengths.

As any consistent formula of an arbitrary theory in the family $\mathcal{T}^{\rm sm}_{\Sigma}$ has an infinite model then the formulae that are satisfiable only in finite models do not belong to the set $\mathrm{PSMF}(\Sigma)$.

Remark 1.2. By the definition for any signature Σ, the sets $\mathrm{PSMF}(\Sigma)$ and $\mathrm{PSMS}(\Sigma)$ are closed under $\vdash$-deducibility and under sentences ψ, preserving or extending nonempty neighbourhoods $(\mathcal{T}^{\rm sm}_{\Sigma})_{\varphi} = \{T \in \mathcal{T}^{\rm sm}_{\Sigma} \mid \varphi \in T\}$ after replacement of φ by ψ. Thus pseudo-strongly-minimal sentences form equivalence classes with respect to the equality of neighbourhoods, which are divided by the equivalence classes of mutual deducibility.

In view of Remark 1.2 the sets $\mathrm{PSMF}(\Sigma)$ and $\mathrm{PSMS}(\Sigma)$ are supplied by the operations $\vee$ of disjunction and the following proposition holds:

Proposition 1.3. *Structures* $\langle \mathrm{PCCF}(\Sigma); \vee \rangle$ *and* $\langle \mathrm{PCCS}(\Sigma); \vee \rangle$ *are upper semilattices.*

Remark 1.4. Each semilattice in Proposition 1.3 admits the operation $\wedge$ of conjunction only for restrictions to the set of formulae of a fixed theory which is an accumulation point for the class of strongly minimal theories and

these restrictions form distributive lattices. thus pseudo-strongly-minimal formulae are closed under disjunctions and some conjunctions.

Remark 1.5. It is easy to see that consistent quantifier free formulae have strongly minimal models, and, as in Remark 1.1, become pseudo-strongly-minimal. It means that any consistent $\exists$-formula, i.e. a consistent formula of the form $\exists x_1 \dots \exists x_k \varphi$, where φ is a quantifier free formula, is pseudo-strongly-minimal with respect to a suitable signature. For $\forall$-formulae, i.e. formulae of the form $\forall x_1 \dots \forall x_k \varphi$, where φ is quantifier free, that property does not hold, since, for instance, the formula $\forall x \forall y\, x \approx y$ does not have infinite models. This formula shows that some formulae, for example, the formula $\neg\forall x \forall y\, x \approx y$ does not preserve the pseudo-strongly-minimality when hanging a negation. At the same time, as noticed for quantifier free formulae, handing negations for these formulae preserves the pseudo-strongly-minimality.

2 Pseudo-strongly-minimal structures and theories

Definition. An elementary theory T of an infinite structure $\mathcal{M}$ which is not strongly minimal is called *pseudo-strongly-minimal*, if any sentence true in $\mathcal{M}$ has a strongly minimal $\mathcal{N}$. In this case, the models $\mathcal{N}$ are called *approximations* of the model $\mathcal{M}$, and the model $\mathcal{M}$ itself is called *pseudo-strongly-minimal*.

We notice that by the definition any pseudo-strongly-minimal theory T of a signature Σ consists of pseudo-strongly-minimal sentences belonging to theories in the set $\mathcal{T}^{\mathrm{sm}}_{\Sigma}$.

We denote by Σ^1 an arbitrary signature consisting of constant symbols c_i, $i \in I$, as well as 0-ary and unary predicate symbols P_j, $j \in J$.

We argue to show that any theory T of a signature Σ^1 either has only finite models, or it is strongly minimal, or pseudo-strongly-minimal.

Indeed, it is known [10] that formulae of any signature Σ^1 are represented by Boolean combinations of formulae describing numbers of elements in intersections of literas P^{δ} of unary predicates P, belonging of constants to these intersections, equalities and inequalities of constants, and satisfiability and unsatisfiability of zero-ary predicates. Here the structure of the signature Σ^1 is strongly minimal iff each each conjunction of literas $P_i^{\delta_i}(x)$ has finitely many or cofinitely many solutions.

Now we approximate infinite and co-infinite conjunctions of literas increasing their finite cardinalities. For instance, if for all $P_0^{\delta_0}(x) \wedge P_1^{\delta_1}(x)$, $\delta_0, \delta_1 \in \{0, 1\}$, their sets of solutions are infinite, we choose some infinite $P_0^{\delta_0} \cap P_1^{\delta_1}$ and approximate other $P_0^{\delta'_0} \cap P_1^{\delta'_1}$ by finite ones. In general case, we choose some infinite definable part $P_{i_0}^{\delta_0} \cap P_{i_1}^{\delta_1} \cap \ldots \cap P_{i_k}^{\delta_k}$ and, in approximations for other definable parts, either fix cardinalities if these parts are finite in the required structure, or increase their cardinalities, otherwise. Since each approximation is strongly minimal, we have the following:

Theorem 2.1. *Any theory T of a signature Σ^1 is pseudo-strongly-minimal iff T does not have finite models and it is not strongly minimal.*

Recall [1, 2, 3, 4] that an infinite structure $\mathcal{M}$ is said to be *pseudofinite* if any sentence, true in $\mathcal{M}$, has a finite model. If $T = \mathrm{Th}(\mathcal{M})$ for a pseudofinite structure $\mathcal{M}$ then the theory T is said to be *pseudofinite*, too.

Remark 2.2. The construction for the proof of Theorem 2.1 and possibilities for approximations of infinite accumulation points $\mathcal{M}$ in the signatures Σ^1, see [8], give both their approximations by finite structures, and, if $\mathcal{M}$ is not countably categorical, then by countably categorical ones. Hence, any pseudo-strongly-minimal structure of a signature Σ^1 is pseudofinite, too, and it is pseudo-countably categorical, if it has infinitely many 1-types over the empty set.

Thus, for theories of signatures Σ^1, there is a trichotomy according to which each such theory either belongs to the class of theories with finite models, or belongs to the class of strongly minimal theories, or belongs to the class of pseudo-strongly-minimal theories. The last two cases are united by the class of pseudofinite theories.

References

[1] E. Rosen. Some Aspects of Model Theory and Finite Structures // The Bulletin of Symbolic Logic. — 2002. — Vol. 8, No. 3. — P. 380–403.

[2] J. Väänänen. Pseudo-finite model theory // Matematica Contemporanea. — 2003. — Vol. 24. — P. 169–183.

[3] G. Cherlin, E. Hrushovski. Finite Structures with Few Types // Annals of Mathematics Studies, No. 152. — Princeton, Oxford : Princeton University Press, 2003.

[4] H.D. Macpherson, Ch. Steinhorn. Definability in the classes of finite structures // Finite and Algorithmic Model Theory. London

Matheematical Society Lecture Notes series: 379 / eds.: J. Esparza, C. Michaux, Ch. Steinhorn. — Cambridge : Cambridge University Press, 2011.

[5] A. Pillay. Strongly minimal pseudofinite structures // arXiv:1411.5008 [math.LO]. — 2014, 10 p.

[6] S.V. Sudoplatov. Approximations of theories // Siberian Electronic Mathematical Reports. — 2020. — Vol. 17. — P. 715–725.

[7] S.V. Sudoplatov. Approximating formulae // Siberian Electronic Mathematical Reports. — 2024. — Vol. 21, No. 1. — P. 463–480.

[8] B.Sh. Kulpeshov, In.I. Pavlyuk, S.V. Sudoplatov. Pseudo-countably-categorical formulae and theories // Preprint, 2024.

[9] J.T. Baldwin, A.H. Lachlan. On strongly minimal // Journal of Symbolic Logic. — 1971. — Vol. 36, No. 1. — P. 79–96.

[10] Yu.L. Ershov, E.A. Palyutin. Mathematical logic. — Moscow : Fizmatlit, 2011. — 356 p. [in Russian]

НАСЛЕДУЕМОСТЬ ТИПОВ ПРЕДГЕОМЕТРИЙ КОМПОЗИЦИЕЙ ОТНОСИТЕЛЬНО ИСХОДНЫХ СТРУКТУР

С.Б.Малышев*

Новосибирский государственный технический университет,
просп. Карла Маркса, 20, Новосибирск, 630073, Российская Федерация
e-mail: sergei2-mal1@yandex.ru

1 Введение

Предгеометрия и геометрия различных математических структур остаются важными объектами исследований в области математической логики и теории моделей. В 1970-х и 1980-х годах исследователи начали активно изучать предгеометрии и геометрии для классов o-минимальных и ω-стабильных структур. Значительный вклад в развитие этой области внесли работы Б.И. Зильбера [20, 21, 22], Г. Черлина, Л. Харрингтона, А. Лахлана [4] и А. Пилая [16]. В частности, в 1970-х годах Б.И. Зильбер сформулировал гипотезы о несчетно категоричных теориях, среди которых ключевой была гипотеза о возможности классификации таких теорий с точностью до биинтерпретируемости. В 1986 году А. Пилай [16] показал, что если o-минимальная теория является модулярной, то выполняется слабое исключение мнимых чисел. В сильно минимальном случае также известно, что при модулярности выполняется геометрическое исключение мнимых чисел [15].

В последующие годы исследования предгеометрий продолжились. В 1996 году Э. Хрушовский [9] предложил оригинальную конструкцию сильно минимальной структуры, не являющейся локально модулярной и для которой невозможно проинтерпретировать бесконечную группу. Эти работы стали основой для дальнейших исследований, направленных на

*Работа выполнена при финансовой поддержке Российского научного фонда, проект № 24-21-00096.

классификацию и описание предгеометрий различных объектов [1, 2, 3], таких как матроиды Вамоса [14].

Поэтому возникают естественные вопросы о классификации предгеометрий и геометрий для различных значимых классов структур и их теорий.

Современные учёные используют композиции структур, чтобы выявить свойства, которые зависят от наследственных характеристик исходных теорий. Примером может выступать работая [6], в которой устанавливаются условия E-определимой композиции, относительно её исходных структур. Более подробно это изложено в монографии "Алгебры бинарных формул" [7].

В данной работе мы исследуем как предгеометрия, возникающая при композиции двух структур предикатной сигнатуры, наследует виды предгеометрий изначальных структур. Мы устанавливаем, что в случае вырожденности, модулярности и локально конечности предгеометрии графовой сигнатуры, предгеометрия их композиции наследует соответствующие свойства.

2 Предгеометрии. Виды предгеометрий

Из работ [4, 5, 8, 13, 15, 17, 18] и [19] приведём необходимые нам определения.

Определение 1. [15] *Предгеометрией* называется множество S вместе с определённой операцией замыкания $\mathrm{cl} : P(S) \to P(S)$, удовлетворяющей следующим условиям:

1) для любого $X \subseteq S$ выполняется $X \subseteq \mathrm{cl}(X)$;

2) для любого $X \subseteq S$ выполняется $\mathrm{cl}(\mathrm{cl}(X)) = \mathrm{cl}(X)$;

3) для любого $X \subseteq S$ и любых $a, b \in S$ если $a \in \mathrm{cl}(X \cup \{b\}) - \mathrm{cl}(X)$, то $b \in \mathrm{cl}(X \cup \{a\})$;

4) для любого $X \subseteq S$ если $a \in \mathrm{cl}(X)$, то $a \in \mathrm{cl}(Y)$ для некоторого конечного $Y \subseteq X$.

При наличии предгеометрии $\langle S, \mathrm{cl}\rangle$ каждое подмножество $X \subseteq S$ имеет минимальное множество $X' \subseteq X$ такое, что $\mathrm{cl}(X) = \mathrm{cl}(X')$. Это минимальное множество X' называется *базисом* множества X. При этом все базисы равномощны и эта мощность называется *размерностью* множества X в предгеометрии $\langle S, \mathrm{cl}\rangle$, обозначается $\dim(X)$.

По определению имеем $\dim(X) = \dim(\mathrm{cl}(X))$, т.е. размерность сохраняется при переходе к замыканию множества X в предгеометрии $\langle S, \mathrm{cl}\rangle$.

Если $\dim(X) \in \omega$, то множество X называется *конечномерным*.

Определение 2. [15] Множество $X \subseteq S$ называется *замкнутым*, если $X = \mathrm{cl}(X)$.

Определение 3. [15] Предгеометрия $\langle S, \mathrm{cl}\rangle$ называется *тривиальной* или *вырожденной*, если для любого $X \subseteq S$, $\mathrm{cl}(X) = \bigcup\{\mathrm{cl}(\{a\}) \mid a \in X\}$.

Предгеометрия $\langle S, \mathrm{cl}\rangle$ называется *модулярной*, если для любых замкнутых множеств $X_0, Y_0 \subseteq S$, X_0 независимо от Y_0 относительно $X_0 \cap Y_0$, т.е. для любых конечномерных замкнутых множеств $X \subseteq X_0$, $Y \subseteq Y_0$ верно

$$\dim(X) + \dim(Y) - \dim(X \cap Y) = \dim(X \cup Y).$$

Предгеометрия $\langle S, \mathrm{cl}\rangle$ называется *локальной модулярной*, если для любого $a \in S$, предгеометрия $\langle S, \mathrm{cl}_{\{a\}}\rangle$ модулярна, где $\mathrm{cl}_{\{a\}}(X) = \mathrm{cl}(X \cup \{a\})$.

Предгеометрия $\langle S, \mathrm{cl}\rangle$ называется *проективной*, если она модулярная и не тривиальная, и *локально проективной*, если она локально модулярная и не тривиальная.

Предгеометрия $\langle S, \mathrm{cl}\rangle$ называется *локально конечной*, если для любого конечного подмножества $A \subseteq S$, множество $\mathrm{cl}(A)$ конечно.

Определение 4. Пусть S — модель теории T. Тогда оператором *алгебраического замыкания* для модели M называется оператор $\mathrm{acl} : P(M) \to P(M)$ такой, что для любого подмножества $X \subseteq S$, $\mathrm{acl}(X) = \{a \in S \mid$ для некоторой формулы $\phi(x, \bar{y})$ и $\bar{b} \in X$ верно $\models \exists^{<\omega} x \phi(x, \bar{b}) \wedge \phi(a, \bar{b})\}$.

В дальнейшем будут рассматриваться предгеометрии вида $\langle S, \mathrm{acl}\rangle$.

3 Композиции структур

Определение 5. [7] Пусть $\mathcal{M}$ и $\mathcal{N}$ — структуры предикатных сигнатур $\Sigma_{\mathcal{M}}$ и $\Sigma_{\mathcal{N}}$ соответственно. Определим *композицию* $\mathcal{M}[\mathcal{N}]$ структур $\mathcal{M}$ и $\mathcal{N}$ по следующим правилам:

1) $\Sigma_{\mathcal{M}[\mathcal{N}]} = \Sigma_{\mathcal{M}} \bigcup \Sigma_{\mathcal{N}}$

2) $M[N] = M \times N$, где $M[N], M, N$ — носители структур $\mathcal{M}[\mathcal{N}], \mathcal{M}$ и $\mathcal{N}$ соответственно;

3) если $R \in \Sigma_{\mathcal{M}} \backslash \Sigma_{\mathcal{N}}$, $\mu(R) = n$, то $((a_1, b_1), ..., (a_n, b_n)) \in R_{\mathcal{M}[\mathcal{N}]}$ тогда и только тогда, когда $(a_1, ..., a_n) \in R_{\mathcal{M}}$;

4) если $R \in \Sigma_{\mathcal{N}} \backslash \Sigma_{\mathcal{M}}$, $\mu(R) = n$, то $((a_1, b_1), ..., (a_n, b_n)) \in R_{\mathcal{M}[\mathcal{N}]}$ тогда и только тогда, когда $a_1 = ... = a_n$ и $(b_1, ..., b_n) \in R_{\mathcal{N}}$;

5) если $R \in \Sigma_{\mathcal{N}} \bigcap \Sigma_{\mathcal{M}}$, $\mu(R) = n$, то $((a_1, b_1), ..., (a_n, b_n)) \in R_{\mathcal{M}[\mathcal{N}]}$ тогда и только тогда, когда $(a_1, ..., a_n) \in R_{\mathcal{M}}$ или $a_1 = ... = a_n$ и $(b_1, ..., b_n) \in R_{\mathcal{N}}$;

Определение 6. [6] Композиция $\mathcal{M}[\mathcal{N}]$ называется *e-определимой*, если $\mathcal{M}[\mathcal{N}]$ имеет $\emptyset$-определимое отношение эквивалентности E, у которого E-классы являются носителями копий структуры $\mathcal{N}$, образующих $\mathcal{M}[\mathcal{N}]$. Если отношение эквивалентности E фиксировано, то e-определимая композиция называется *E-определимой*.

Предложение 1. [12] *Пусть $\mathcal{M}$ и $\mathcal{N}$ — структуры предикатных сигнатур, а $\mathcal{M}[\mathcal{N}]$ их E-определимая композиция. Тогда верны утверждения:*

1) если структура $\mathcal{N}$ конечна, а предгеометрия $\langle \mathcal{M}, \mathrm{acl} \rangle$ обладает одним из свойств — вырожденности, модулярности или локально конечности, то предгеометрия $\langle \mathcal{M}[\mathcal{N}], \mathrm{acl} \rangle$ наследует это свойство.

2) если структура $\mathcal{M}$ конечна, а $\mathcal{N}$ бесконечна, тогда алгебраические замыкания на подмножествах $M[N]$ задаются алгебраическими замыканиями в копиях $\mathcal{N}$.

Теорема 7. [12] *Пусть $\mathcal{M}$ и $\mathcal{N}$ — структуры графовой сигнатуры, а $\mathcal{M}[\mathcal{N}]$ их E-определимая композиция. Тогда верны утверждения:*

1) Если вырождены предгеометрии $\langle \mathcal{M}, \mathrm{acl} \rangle$ и $\langle \mathcal{N}, \mathrm{acl} \rangle$, тогда предгеометрия $\langle \mathcal{M}[\mathcal{N}], \mathrm{acl} \rangle$ вырожденная;

2) Если модулярны предгеометрии $\langle \mathcal{M}, \mathrm{acl} \rangle$ и $\langle \mathcal{N}, \mathrm{acl} \rangle$, тогда предгеометрия $\langle \mathcal{M}[\mathcal{N}], \mathrm{acl} \rangle$ модулярна;

3) Если локально конечны предгеометрии $\langle \mathcal{M}, \mathrm{acl} \rangle$ и $\langle \mathcal{N}, \mathrm{acl} \rangle$, тогда предгеометрия $\langle \mathcal{M}[\mathcal{N}], \mathrm{acl} \rangle$ локально конечная;

Замечание 1. [12] *В общем случае обратные утверждения не верны.*

Это можно заметить, если взять композицию $\mathcal{M}[\mathcal{N}]$. Где структура $\mathcal{M}$ не обладает свойством вырожденности, модулярности или локально конечности. А структура $\mathcal{N}$ состоит из бесконечного числа одинаковых элементов.

Пример 1. [12] Рассмотрим композицию $\mathcal{M}[\mathcal{N}]$, составленную из двух бесконечных кубических структур $\mathcal{M}$ и $\mathcal{N}$. Структура $\mathcal{M}$ будет состоять из бесконечного куба. Структура $\mathcal{N}$ будет состоять из бесконечного числа конечных кубов размера 1.

Более подробно об условиях для типов кубических предгеометрий было написано в статье [11].

При этом предгеометрия композиций этих структур $\langle \mathcal{M}[\mathcal{N}], \mathrm{acl} \rangle$ будет вырожденной.

Эти структуры так же будут являться примером для модулярности. Предгеометрия $\langle \mathcal{M}, \mathrm{acl} \rangle$ не модулярна, а предгеометрии $\langle \mathcal{N}, \mathrm{acl} \rangle$ и $\langle \mathcal{M}[\mathcal{N}], \mathrm{acl} \rangle$ будут модулярными.

Пример 2. [12] Рассмотрим композицию $\mathcal{M}[\mathcal{N}]$, составленную из двух бесконечных структур $\mathcal{M}$ и $\mathcal{N}$. Структура $\mathcal{M}$ будет состоять из бесконечного дерева, у которого степени всех его вершин различны. Структура $\mathcal{N}$, как и в прошлом примере, будет состоять из бесконечного числа конечных кубов размера 1.

Более подробно об условиях для типов кубических предгеометрий было написано в статье [11], об условиях для типов ациклических предгеометрий было написано в статье [10].

При этом предгеометрия композиций этих структур $\langle \mathcal{M}[\mathcal{N}], \mathrm{acl} \rangle$ является локально конечной.

4 Заключение

Установлено, что предгеометрия, порожденная композицией $\mathcal{M}[\mathcal{N}]$ бесконечной структуры $\mathcal{M}$ и конечной структуры $\mathcal{N}$ предикатной сигнатуры, сохраняет свойства вырожденности, модулярности и локальной конечности, присущие структуре $\mathcal{M}$. Для структур графовой сигнатуры установлено, что если предгеометрии обеих исходных структур вырождены, модулярны или локально конечны, то эти свойства сохраняются в предгеометрии их композиции. Однако обратное утверждение в общем случае неверно: предгеометрия композиции может обладать указанными свойствами, даже если исходные структуры их не имеют. Перспективные направления исследований могут включать более детальный анализ других типов структур и их композиций, что позволит углубить понимание наследования свойств предгеометрий.

Список литературы

[1] A. Berenstein, E. Vassiliev, On lovely pairs of geometric structures // Annals of Pure and Applied Logic, 2010, vol. 161, no. 7, pp. 866–878.

[2] A. Berenstein, E. Vassiliev, Weakly one-based geometric theories // J. Symb. Logic, 2012, vol. 77, no. 2, pp. 392–422.

[3] A. Berenstein, E. Vassiliev, Geometric structures with a dense independent subset // Selecta Math., 2016, vol. 22, no. 1, pp. 191–225.

[4] G.L. Cherlin, L. Harrington, A.H. Lachlan, ω-categorical, ω-stable structures // Annals of Pure and Applied Logic, 1986, vol. 28, pp. 103–135.

[5] C.C. Chang, H.J. Keisler, Model theory. Third edition of XLI 697. Studies in Logic and the Foundations of Mathematics, vol. 73. 1990. 650 p.

[6] D.Y. Emelyanov, B.S. Kulpeshov, S.V. Sudoplatov, Algebras of binary formulas for compositions of theories // Algebra and Logic, 2020, vol. 59, no. 4, pp. 295-–312. https://doi.org/10.1007/s10469-020-09602-y

[7] D.Y. Emelyanov, B.S. Kulpeshov, S.V. Sudoplatov, Algebras of binary formulae. Novosibirsk : NSTU, 2023, 330 p.

[8] W. Hodges, Model theory. Encyclopedia of Mathematics and its Applications, 1994, vol. 42, Cambridge University Press, 772 p.

[9] E. Hrushovski, A new strongly minimal set // Annals of Pure and Applied Logic, 1993, vol. 62, pp. 147–166.

[10] S.B. Malyshev, Kinds of pregeometries of acyclic theories // Bulletin of Irkutsk State University. Series Mathematics, 2023, vol. 46, pp. 110—120. https://doi.org/10.26516/1997-7670.2023.46.110

[11] S.B. Malyshev, Kinds of pregeometries of cubic theories // Bulletin of Irkutsk State University. Series Mathematics, 2022, vol. 41, pp. 140—149. https://doi.org/10.26516/1997-7670.2022.41.140

[12] S.B. Malyshev, Heritability of types of pregeometry with respect to compositions of structures // Bulletin of Irkutsk State University. Series Mathematics

[13] N.D. Markhabatov, S.V. Sudoplatov, Topologies, ranks, and closures for families of theories. I // Algebra and Logic, 2021, vol. 59, no. 6, pp. 437–455.

[14] M.M. Mukhopadhyay, E. Vassiliev, On the Vamos matroid, homogeneous pregeometries and dense pairs // Australian Journal of Combinatorics, 2019, vol. 75, no. 1, pp. 158–170.

[15] A. Pillay, Geometric Stability Theory, Oxford, Clarendon Press, 1996. 361 p.

[16] A. Pillay, Some remarks on definable equivalence relations in o-minimal structures // The Journal of Symbolic Logic, 1986, vol. 51, no. 3, pp. 709–714 .

[17] S.V. Sudoplatov, Group polygonometries, Novosibirsk : NSTU, 2013, 302 p.

[18] S.V. Sudoplatov, Models of cubic theories // Bulletin of the Section of Logic, 2014, vol. 43, no. 1–2, pp. 19–34.

[19] S.V. Sudoplatov, Closures and generating sets related to combinations of structures // Bulletin of Irkutsk State University. Series Mathematics, 2016, vol. 16, pp. 131–144.

[20] B.I. Zilber, Uncountably categorical theories : American Mathematical Society. 1993. 117 p.

[21] B.I. Zilber, Strongly minimal countably categorical theories // Sibirsk Matematika Zhurnal, 1980, vol. 21, no. 2, pp. 98–112.

[22] B.I. Zilber, Strongly minimal countably categorical theories II //Sibirsk Matematika Zhurnal, 1984, vol. 25, no. 3, pp. 71–88.

ГРАФ ДЕЛИТЕЛЕЙ НУЛЯ КОНЕЧНОГО КОЛЬЦА

А.С. Монастырева*

Алтайский государственный университет,
пр-т. Ленина, 61, Барнаул, 656049, Россия
e-mail: akuzmina1@yandex.ru

В работе под термином “кольцо” мы будем понимать ассоциативное кольцо.

Идея построения графа делителей нуля впервые была использована в 1986 году в работе [6] для коммутативного кольца. В качестве вершин графа делителей нуля коммутативного кольца автор этой работы И.Бек рассматривал все элементы кольца, причем две различные вершины x и y соединял ребром тогда и только тогда, когда $xy = 0$. Введение понятия графа делителей нуля кольца устанавливает связь между теорией колец и теорией графов. И.Бек занимался, в основном, раскраской графов делителей нуля коммутативных колец.

В 1999 году Д. Андерсон и Ф. Ливингстон в работе [5] несколько изменили способ построения графа делителей нуля. Вершинами графа делителей нуля коммутативного кольца они стали считать все ненулевые делители нуля. По мнению Д. Андерсона и Ф. Ливингстона, такое определение лучше иллюстрирует структуру множества делителей нуля. Действительно, в [5] доказано, что граф делителей нуля коммутативного кольца с единицей, вершинами которого являются лишь ненулевые делители нуля, связен. Если же рассматривать в качестве вершин графа все элементы кольца, то это утверждение становится очевидным, поскольку нуль – вершина, которая является смежной для всех остальных вершин графа. Статья [5] посвящена изучению некоторых взаимосвязей между свойствами коммутативного кольца с единицей и свойствами графа делителей нуля этого кольца.

С 1999 года теория графов делителей нуля коммутативного кольца стала интенсивно развиваться. Кроме того, это понятие было распространено и на некоммутативный случай. Для некоммутативного кольца

*Исследование выполнено за счет гранта Российского научного фонда № 24-21-00155, https://rscf.ru/project/24-21-00155/.

используются два определения графа делителя нуля. Во-первых, введено понятие ориентированного графа делителя нуля. Вершинами такого графа считаются все (односторонние и двусторонние) делители нуля кольца, причем две различные вершины соединяются ориентированным ребром $x \longrightarrow y$ тогда и только тогда, когда $xy = 0$ (см., в частности, работы [3, 19]). Во-вторых, используется определение неориентированного графа делителей нуля, т.е. графа, вершинами которого являются все ненулевые делители нуля кольца (односторонние и двусторонние), причем две различные вершины x, y соединяются ребром тогда и только тогда, когда либо $xy = 0$, либо $yx = 0$ [17]. Понятно, что в коммутативном случае последнее определение графа делителей нуля совпадает с определением, введенным Д. Андерсоном и Ф. Ливингстоном в [5]. В настоящей работе всюду далее рассматриваются только неориентированные графы делителей нуля, то есть используется определение из работы [17]. Было доказано, что диаметр графа делителей нуля ассоциативного конечного кольца не превосходит трех [17].

Одним из направлений исследований в этой области стало описание колец, граф делителей нуля которых удовлетворяет определенному условию. В работах [4, 7] исследуются коммутативные конечные кольца с единицей, графы делителей нуля которых планарны. В [4] приведено, в частности, полное описание конечных коммутативных разложимых колец с единицей, у которых графы делителей нуля планарны, а в [7] составлен полный список коммутативных конечных локальных колец с планарными графами делителей нуля. Некоммутативные кольца и кольца без единицы, имеющие планарные графы делителей нуля, до сих пор описаны не были, поэтому мы поставили задачу завершить описание конечных колец с планарными графами делителей нуля, что и было сделано в работах [25] и [11].

Ранее в [3] исследовались кольца с единицей, ориентированные графы делителей нуля которых эйлеровы. В частности, в этой работе доказано, что любое полупростое конечное кольцо имеет эйлеров ориентированный граф делителей нуля. Также авторы работы [3] доказали, что для любого конечного поля K и любой конечной группы G ориентированный граф делителей нуля группового кольца KG эйлеров. Далее, в [3] доказано, что разложимое конечное кольцо $R = R_1 \oplus \ldots \oplus R_n, n \geq 2$, имеет эйлеров направленный граф делителей нуля в том и только в том случае, когда для любого $i \in \{1, 2, \ldots, n\}$ либо кольцо R_i является полем, либо ориентированный граф делителей нуля кольца R_i эйлеров. Мы поставили аналогичную задачу для неориентированного графа делителей нуля. В работе [10] полностью описаны конечные кольца с

эйлеровыми графами делителей нуля.

Также естественным является вопрос о том, как устроены конечные кольца, графы делителей нуля которых однородные, то есть все вершины графа имеют одну и ту же степень. В литературе часто однородные графы называются *регулярными*. В работе [22] описаны конечные кольца, графы делителей нуля которых являются однородными.

Естественным оказался вопрос описания конечных колец, у которых граф делителей нуля является гамильтоновым. Единственное, в работах удалось описать сначала коммутативные [2], а затем некоммутативные [23] разложимые кольца с гамильтоновыми графами делителей нуля. Однако полного описания конечных колец с таким ограничением на графы делителей нуля получить не удалось. Более того, были построены примеры колец очень больших порядков с гамильтоновыми графами делителей нуля. Поэтому решено было ослабить условие "быть гамильтоновым" с помощью известной теоремы Дирака о том, что любой граф, в котором степень каждой вершины не меньше, чем $n/2$, где n – число вершин в данном графе, причем $n \geq 3$, является гамильтоновым. Впредь мы будем говорить, что граф удовлетворяет *условию Дирака*, если он удовлетворяет условию теоремы Дирака. Изучению свойства конечных колец, графы делителей нуля которых удовлетворяющие условию Дирака, посвящена наша работа [12]. Полного описание конечных колец с таким свойством пока получить не удалось.

Как говорилось выше, решить задачу описания конечных колец с гамильтоновыми графами делителей нуля удалось только для разложимых колец. Поэтому была поставлена задача описания конечных колец с гамильтоновыми графами делителей нуля на языке многообразий. Описание многообразий ассоциативных колец, в которых все конечные кольца имеют гамильтоновы графы делителей нуля, было сделано нами в работе [23].

Нетрудно привести примеры неизоморфных колец, графы делителей нуля которых равны. Например, если A — счетномерная алгебра с нулевым умножением над полем $\mathbb{Z}_p$, а B — счетномерная алгебра с нулевым умножением над полем $\mathbb{Z}_q$, где p, q — это различные простые числа, то $\Gamma(A) \cong \Gamma(B)$, но $A \ncong B$. Другими словами, даже в многообразии колец $var\,\langle xy = 0\rangle$ существуют примеры бесконечных неизоморфных колец, графы делителей нуля которых имеют одинаковое строение. В связи с этим интерес представляет такой вопрос: при каких условиях из равенства графов делителей нуля следует изоморфизм колец? Некоторые результаты, дающие ответ на этот вопрос для коммутативных колец, были получены в работе [2]. Мы решили поставить эту задачу

на языке многообразий: описать многообразия ассоциативных колец, в которых каждое конечное кольцо однозначно определяется своим графом делителей нуля. Другими словами, описать многообразие колец $\mathfrak{M}$, для которого из равенства $\Gamma(R) = \Gamma(S)$ для конечных колец $R, S \in \mathfrak{M}$, следует, что $R \cong S$. Описание таких многообразий было полностью завершено в серии работ: [24], [13] и [20].

Однако скоро стало понятным, что изображение графа делителей нуля даже для колец небольших порядков часто является сложным, а для больших порядков почти невозможным. Возникла необходимость разбить множество вершин графа делителей нуля на классы, причем так, чтобы не нарушалось представление о строении графа делителей нуля в целом. В работах [8, 9] предложили довольно естественный способ решения этой проблемы для коммутативного случая. В статье [16] этот подход был обобщен на некоммутативный случай. Изложим суть этого метода. Введем отношение эквивалентности на множестве $D(R)^*$ следующим образом:

$$\text{для любых } \ x, y \in D(R)^* \ \ x \sim y \Leftrightarrow l(x) \cup r(x) = l(y) \cup r(y).$$

Обозначим через $[x]$ класс эквивалентности элемента $x \in D(R)^*$. Для любых $a \in [x]$, $b \in [y]$, где $x, y \in D(R)^*$, очевидно, что $ab = 0$ или $ba = 0$ тогда и только тогда, когда $xy = 0$ или $yx = 0$. Обозначим через $\Gamma_\sim(R)$ граф, множеством вершин которого является множество $\{[x];\ x \in D(R)^*\}$, причем две вершины $[x]$, $[y]$ (не обязательно различные) будем соединять ребром (или петлей) тогда и только тогда, когда $xy = 0$ или $yx = 0$. Граф $\Gamma_\sim(R)$ будем называть *сжатым графом делителей нуля* кольца R.

В работе [16] был доказан следующий факт: *Пусть R – произвольное кольцо и $x \in D(R)^*$. Если $x^2 = 0$, то $yz = 0$ или $zy = 0$ для любых $y, z \in [x]$; если же $x^2 \neq 0$, то $yz \neq 0$ и $zy \neq 0$ для любых $y, z \in [x]$.*

Из этого факт следует, что в графе $\Gamma_\sim(R)$ все вершины делятся на два типа. Если $x^2 = 0$, то $[x]$ – это вершина с петлей. Если $x^2 \neq 0$, то $[x]$ – это вершина без петли. Зная, сколько элементов содержится в каждом классе $[x]$, мы всегда от сжатого графа делителей нуля можем перейти к обычному графу делителей нуля. Действительно, пусть в вершине $[x]$ содержится n делителей нуля. Тогда при переходе от сжатого графа делителей нуля к обычному графу делителей нуля вершина $[x]$ с петлей перейдет в подграф, изоморфный полному графу K_n. Если вершина $[x]$ была без петли, то она при таком переходе развернется в подграф, изоморфный нуль-графу E_n. Ясно, что сжатый граф делителей нуля конечного ассоциативного кольца также связен и его диаметр не

больше трех. Подчеркнем, что в сжатом графе нильпотентные элементы индекса нильпотентности два выделены петлей.

Отметим, что не всякий связный граф может являться сжатым графом делителей нуля для какого-нибудь кольца. Например, если взять отрезок $[a] - [b]$, где обе вершины имеют петли, то он не является сжатым графом делителей нуля никакого кольца, поскольку вершины $[a]$ и $[b]$ на самом деле можно стянуть в одну вершину с петлей. И таких примеров много, причем не всегда причина в том, что граф не до конца сжат. В работе [16] описаны все связные графы делителей нуля (с петлями) на одной, двух и трех вершинах, которые являются сжатыми графами делителей нуля какого-либо конечного кольца. В статье [15] полностью описаны все связные графы с петлями на четырех вершинах, которые могут реализованы как сжатые графы делителей нуля какого-нибудь конечного кольца. Из 50 неизоморфных связных графов с петлями на четырех вершинах только 8, как оказалось, являются сжатыми графами делителей нуля какого-либо конечного кольца (см. [15]). Описаны полностью конечные кольца, сжатые графы делителей нуля содержат мост, вершины которого не являются висячими [1]. В работах [1, 14] получено описание конечных колец, сжатые графы делителей нуля которых являются полными (возможно, с петлями). Позже были описаны конечные кольца с ациклическими сжатыми графами делителей нуля [21].

Список литературы

[1] A.A. Afanas'ev, A.S. Monastyreva, Compressed and Partially Compressed Zero-Divisor Graphs of Finite Associative Rings // Sib. Math. J. – 2023. – 64(2). – P.281–291.

[2] S. Akbari, A. Mohammadian, On the zero-divisor graph of a commutative ring // J. Algebra. – 2004. – 274. – P.847–855.

[3] S. Akbari, A. Mohammadian, On Zero-Divisor Graphs of Finite Rings // Journal of Algebra. – 2007. – 314. – P.168–184.

[4] S. Akbari, H.R. Maimani, S. Yassemi, When Zero-Divisor Graph is Planar or a Complete r-Partite Graph // Journal of Algebra. – 2003. – 270. – P.169–180.

[5] D.F. Anderson, P.S. Livingston, The Zero-Divisor Graph of a Commutative Ring // Journal of Algebra. – 1999. – 217. – P. 434–447.

[6] I. Beck, Coloring of Commutative Rings // Journal of Algebra. – 1988. – 116. – P. 208–226.

[7] R. Belshoff, J. Chapman, Planar Zero-Divisor Graphs // Journal of Algebra. – 2007. – 316. – P. 471–480.

[8] N. Bloomfield, C. Wickham, Local rings with genus two zero divisor graph // Communication in Algebra. – 2010. – V. 38. – P. 2965–2980.

[9] N. Bloomfield, The zero divisor graphs of commutative local rings of order p^4 and p^3 // Communication in Algebra. – 2013. – V. 41. – P. 765–775.

[10] A.S. Kuzmina, Finite rings with Eulerian zero-divisor graphs // J. of Algebra and Its Appl. – 2012. – 11(3). – P.551–559.

[11] Yu.N. Maltsev, A.S. Kuz'mina, Nilpotent Finite Rings with Planar Zero-Divisor Graphs // Asian-European Journal of Mathematics. – 2008. – Vol. 1. – № 4. – P. 565–574.

[12] Yu.N. Maltsev, A.S. Kuz'mina, On Finite Rings in Which Zero-Divisor Graphs Satisfy the Dirac's condition // Lobach. J. Math. – 2015. – 4(36). – P.376-384.

[13] Yu.N. Maltsev, A.S. Kuz'mina, On varieties of rings whose finite rings are determined by their zero-divisor graphs // Asian-European J. Math. – 2012. – 5(2). – P.101–111.

[14] A.S. Monastyreva, Finite Non-Nilpotent Rings with Complete Compressed Zero-Divisor Graphs // Lobach. J. Math. – 2020. – 41(9). – P.1666–1671.

[15] A.S. Monastyreva, The Compressed Zero-divisor Graphs of Order 4 // J. Alg. Appl. – 2022. – 21(9). – 2250179.

[16] A.S. Monastyreva, E.V. Zhuravlev, Compressed Zero-Divisor Graphs of Finite Associative Rings // Siberian Math. J. – 2020. – V. 61(1). – P.76-–84.

[17] S.P. Redmond, The Zero-Divisor Graph of a Noncommutative Ring // Int. J. Commut. Rings. – 2002. – 1(4). – P.203–211.

[18] N. Smith, Infinite Planar Zero-Divisor Graphs // Communications in Algebra. – 2007. – V. 35. – P.171-180.

[19] T. Wu, On Directed Zero-Divisor Graphs of Finite Rings // Discrete Mathematics. – 2005. – V. 296. – P.73–86.

[20] Е.В. Журавлев, Ю.Н. Мальцев, А.С. Кузьмина, Описание многообразий колец, в которых конечные кольца однозначно задаются своими графами делителей нуля // Известия вузов. Математика. – 2013. – № 6. – С.13-24.

[21] А.С. Монастырева, Конечные кольца с ациклическими сжатыми графами делителей нуля // Сиб. электр. мат. известия. – 2024. – 21. – С. 405–416.

[22] Ю.Н. Мальцев, А.С. Кузьмина, Конечные кольца с некоторыми ограничениями на графы делителей нуля // Известия вузов. Математика. – 2014. – 12. – С.48-59.

[23] Ю.Н. Мальцев, А.С. Кузьмина, Описание многообразий колец, в которых все конечные кольца имеют гамильтоновы графы делителей нуля // Алгебра и логика. – 2013. – 52(2). – С.203–218.

[24] А.С. Кузьмина, О некоторых свойствах многообразий колец, в которых конечные кольца однозначно определяются своими графами делителей нуля // Сибирские электронные математические известия. – 2011. – 8. – С.179–190.

[25] А.С. Кузьмина, Описание конечных ненильпотентных колец, имеющих планарные графы делителей нуля // Дискретная математика. – 2009. – Вып. 4. – С.60–75.

PARAMETRES DANS LES CORPS ALGEBRIQUEMENT CLOS

UNE EXEGESE, S'APPUYANT SUR LA THEORIE DES MODELES DES GROUPES ALGEBRIQUES SIMPLES, D'UN RESULTAT DE MONSIEUR ALEKSANDR VASILEVIC BOROVIK, SUIVIE D'UN COMMENTAIRE DE MEME NATURE SUR LE THEOREME DE BOREL-TITS

Bruno Poizat[1]

Les principaux tropes sont l'antonomase,
la catachrèse, la métaphore, la métonymie et la synecdoque.

Abstract. This paper is a study of the influence of the parameters necessary in the definition of a given structure S definable in an algebraically closed field K, principally on the relations between the group of automorphisms of S and the group of automorphisms of K.

It begins by a commentary of a result of A.V. Borovik, which was the source of its inspiration, making explicit its dependence on the famous Theorem of Borel and Tits on abstract isomorphisms between algebraic simple groups, considered from a model-theoretic point of view. It finally leads to a description of the automorphisms of finite order of a simple algebraic group (over an algebraically closed field), and of its superstable groups of automorphisms, based on general arguments from Model Theory; to achieve that, we have to complete a somehow elliptic argument of Altinel, Borovik and Cherlin.

In fact, the Theorem of Borel and Tits is not dependent of the presence of a group structure; it is valid more generally in what we call *autonomous constructible structures,* which are structures S definable in an algebraically closed field K, for which anything which is definable on S in the language of the field K is definable in the language of S. We study significant examples of such structures.

Mots-clés. Groupes algébriques simples, Théorème de Borel-Tits, Théorie de Galois, internité au sens de Hrushovski

Classification des sujets. 03C45, 03C60, 12L12, 20G07

[1] Institut Camille Jordan, Université Claude Bernard, Mathématiques, bâtiment 101, 43, boulevard du 11 novembre 1918, 69622 Villeurbanne cedex, France ; poizat@math.univ-lyon1.fr

0. Introduction

Le but de cet article est d'éclairer les rapports entre les automorphismes d'un corps algébriquement clos K et ceux d'une structure S définissable[2] dans K, quand une copie L du corps de base K est définissable dans S. Nous irons au-delà de la remarque de bon sens qui dit qu'un automorphisme de K qui fixe les paramètres de la définition de S induit un automorphisme de S, et qu'un automorphisme de S fixant les paramètres nécessaires à la définition de L induit un automorphisme de ce dernier. Mais il est clair d'emblée que les paramètres intervenant dans les définitions vont être sur le devant de la scène.

Avant d'entrer dans le vif du sujet, nous commentons le théorème suivant, extrait de BOROVIK 2023, qui a été le déclic à l'origine de la présente étude, tout en me donnant le désir d'affermir la démonstration approximative d'un autre résultat dont Borovik est un co-auteur.

Theorem 3. *Let* K *be an algebraically closed field of characteristic* $p > 0$, *and* K_∞ *the algebraic closure of the prime field* F_p *in* K. *Let* G *be a simple algebraic group over* K, *and* G_∞ *the group of points of* G *over* K_∞. *If* M *is a subgroup of* G *containing* G_∞ *and the structure* (G,M) *has a finite Morley rank, then* $M = G$.

Son énoncé est lacunaire, car G_∞ n'est déterminé que si on précise une façon de définir G dans K (par une formule pour un logicien, par un schéma pour un algébriste) qui ne fait intervenir que des paramètres algébriques. Borovik, citant BOREL 1970, déclare que chaque groupe algébrique simple[3] a une représentation linéaire définie par des équations polynomiales à coefficients entiers ; ce résultat, dont la source est le Théorème de la base entière de CHEVALLEY, est d'après moi implicite dans la classification de THOMAS 1983 des groupes simples de rang de Morley fini localement finis, qu'il a ensuite étendue aux groupes pseudo-localement finis. Rappelons que le travail de Simon Thomas repose sur la classification des groupes simples finis. La question suivante est un prélude aux arguments développés dans le présent article :

Question A. (i) *Peut-on trouver une raison purement modèle-théorique expliquant pourquoi un groupe simple définissable dans un corps algébriquement clos est définissablement isomorphe à un groupe définissable sans paramètres ?*
(ii) *Plus généralement, qu'en est-il des groupes algébriques affines connexes ?*

---

[2] Par définissable, j'entends définissable avec paramètres, sauf si le contraire est précisé ; je ne distingue pas définissable d'interprétable.

[3] Simple a pour nous le sens usuel qu'il a en Théorie des groupes : G n'est pas commutatif et n'a pas de sous-groupe propre normal. Nous qualifions de quasi-simples les groupes algébriques "simples" au sens géométrique : G est connexe, son centre $Z(G)$ est fini, et le quotient $G/Z(G)$ est simple.

La démonstration de Borovik repose sur deux ingrédients :
(i) la version modèle-théorique du Théorème de Borel-Tits exposée dans POIZAT 1988 (voir aussi POIZAT 1987, p. 149, et le Corollaire 3.2 à venir), ayant pour conséquence que tout ce qui est définissable à l'intérieur du groupe simple G au sens du corps K, quand on considère G comme un objet définissable dans K, est définissable (avec paramètres) à partir de la seule loi de groupe de G.
(ii) le théorème de WAGNER 2001 affirmant que si K est un corps infini de rang de Morley fini, dans un langage augmenté, possédant un automorphisme définissable non-trivial, son modèle premier est basé sur K_∞.

Mais, à la fin de son article, Borovik propose deux démonstrations alternatives, demandant une meilleure connaissance de la structure des groupes algébriques simples ; l'une d'elle réduit le problème au cas où $G = SL_2(K)$ ou $PSL_2(K)$, si bien que le Theorem 3 devient alors une conséquence du Théorème 4 de POIZAT 2001, ou de sa généralisation MUSTAFIN-POIZAT 2006, qui décrit les sous-groupes superstables de $SL_2(K)$ et de $PSL_2(K)$; ils n'utilisent pas le Théorème de Wagner, et sont valables en toute caractéristique, si bien que le Theorem 3 est aussi vrai en caractéristique nulle (quand K_∞ est la clôture algébrique du corps des rationnels). Le Théorème de Borel-Tits reste nécessaire à la démonstration, car il faut être sûr que les groupes de racine de G soient définissables dans le groupe G (ou bien il faut le vérifier à la main).

Nous allons voir bientôt que le groupe G_∞ est une restriction élémentaire de G ; mais le Theorem 3 affirme une propriété beaucoup plus forte. Borovik l'utilise sous la forme suivante : si, dans un contexte de rang de Morley fini, G agit sur un ensemble X, et si chaque point de G_∞ normalise un sous-ensemble définissable de X, ou bien commute avec une fonction définissable de X dans X, alors cela a lieu pour tout point de G.

Dans ce qui suit, nous allons interpréter ce résultat en termes de pure Théorie des Modèles ; nous verrons que le seul fait mathématique sur lequel il repose, de même que le Théorème de Borel-Tits et la description des automorphismes des groupes algébriques simples qu'on en tire, est que tout corps infini définissable dans un corps algébriquement clos nu[4] est définissablement isomorphe au corps de base (POIZAT 1987, p. 141) : le reste suit de résultats généraux de Théorie des Modèles. Cela conduit à envisager le Théorème de Borel-Tits dans un cadre plus large, dans lequel il n'est pas essentiel que les structures considérées soient des groupes.

1. Géomètres et Logiciens

Ce qui est frappant dans l'énoncé du Theorem 3, c'est qu'il confronte des notions de Théorie des Modèles ("le rang de Morley fini") à des notions de

[4] Nous voulons dire par là que le langage dans lequel le corps se présente est réduit au pur langage des corps ; pour nous, si rien d'autre n'est spécifié, un "corps de rang de Morley fini" peut être une structure de langage plus étendu.

Géométrie Algébrique ("les points rationnels d'un groupe algébrique") ; son énoncé est une mixture de Géométrie et de Théorie des Modèles.

Les théoriciens des modèles parlent d'un groupe algébrique comme d'un groupe *définissable,* et non pas *défini,* dans un corps algébriquement clos ; ils le voient marchant au milieu du cortège (η θεωρια !) formé par ses restrictions et ses extensions élémentaires ; ils s'immergent volontiers dans un domaine universel très saturé. Un point de vue très proche du leur est celui de WEIL 1948, qui nous apparaît a posteriori comme une étude fine de la Théorie des Modèles des corps algébriquement clos ; elle conforte l'impression que la Théorie des Modèles de la fin du siècle dernier est l'héritière de la Géométrie Algébrique des années cinquante.

Après Weil s'est développée une tendance à introduire les groupes algébriques non pas comme des groupes, mais comme des schémas de groupe, ayant des points rationnels sur n'importe quel anneau intègre A contenant les paramètres nécessaires à sa définition : les points rationnels sur A, eux, forment un groupe[5]. Une possibilité est donnée par les sous-fermés de Zariski de groupes linéaires GL_n, mais ce n'est pas la seule ; à ce propos, il semble que, dans ses premiers travaux, Zil'ber n'a en vue que ces groupes algébriques affines, ce qui n'est pas bien gênant quand on parle de groupes simples[6].

Le théoricien des modèles rejoint le géomètre en considérant les objets définissables dans un corps (nu) algébriquement clos K, associés à une formule φ du langage des corps à paramètres dans K ; ils ont été qualifiés de *constructibles* par Chevalley ; si L est un corps algébriquement clos étendant K, c'en est une extension élémentaire, et la formule φ définit sur L un objet ayant les mêmes propriétés du premier ordre que son ancêtre dont les points sont dans K ; de plus, toute bijection de graphe constructible entre deux objets constructibles dans K s'étend à leurs descendants dans L, ce qui fait que les théoriciens des modèles ont eux-aussi une vision schématique de l'existence.

Si on fixe le schéma, c'est-à-dire la définition, l'extension du corps de base capture bien toutes les extensions élémentaires du groupe. Mais ça ne marche pas dans l'autre sens, d'abord parce que la restriction du corps de base n'est possible que si elle contient les paramètres intervenant dans la définition choisie pour le groupe, et ensuite parce que, si on veut décrire par une restriction du corps toutes les restrictions élémentaires du groupe, il faut considérer toutes ses définitions possibles.

Une autre différence est que les variétés des géomètres sont des objets constructibles très particuliers, pour que leurs points rationnels sur n'importe quel anneau se comportent décemment. Les théoriciens des modèles, eux,

---

[5] Il est piquant de rappeler qu'un algébriste comme Borovik est l'auteur d'une tentative de caractériser la finitude du rang de Morley d'un groupe sans sortir de ce dernier (BOROVIK 1984), qui a été finalisée dans POIZAT 1987.

[6] Car on sait que le quotient d'un groupe algébrique connexe par son centre est affine (POIZAT 1987, p. 147), soit encore linéaire.

manipulent aisément des objets plus généraux, mais doivent payer le prix de n'avoir pour domaine de base que des anneaux qui sont des corps algébriquement clos (ou bien des corps dont ils maîtrisent les propriétés du premier ordre, comme les corps réel-clos).

Ils ont tendance à identifier des objets définissablement isomorphes. Par exemple, le groupe SL_3 est formé des matrices carrées d'ordre 3 dont le déterminant vaut 1 : cette définition est limpide à tout point de vue ; le groupe PSL_3 est défini communément comme étant le quotient de SL_3 par son centre, formé des matrices diagonales associées aux racines cubiques de l'unité. Le théoricien des modèles admet sans états d'âme que $PSL_3(R)$ est le même[7] groupe que $SL_3(R)$, tandis que pour un géomètre il s'agit plutôt des points réels de deux schémas distincts.

Deux objets isomorphes ne sont pas identiques (bien qu'ils aient beaucoup de propriétés en commun !), et il faut se préoccuper de la nature de leur isomorphie avant de les identifier : cette philosophie est à la base du Théorème de Borel-Tits.

Bien que le rang de Morley soit une traduction au niveau constructible de la dimension géométrique, les hypothèses du Theorem 3 sont modèle-théoriques, car le groupe M de l'énoncé n'a a priori rien d'algébrique ; il satisfait cependant une condition de nature géométrique, celle de contenir le groupe G_∞ ; le théoricien des modèles rejoint le géomètre en déterminant G_∞ par le choix nécessaire d'une formule à paramètres algébriques interprétant G dans le corps de base. Quand il énonce cette condition, quel que soit le point-de-vue adopté, l'énoncé du Theorem 3 ne parle pas d'un groupe, mais d'une façon de définir un groupe.

On comprend que cette différence d'approche ne facilite pas la communication entre la Géométrie et la Logique, ce qu'on me permettra d'illustrer par une anecdote. En 1983, à Bombay, j'ai demandé à Jean-Louis Colliot-Thélène s'il était bien connu que le seul corps constructible était le corps de base ; comme je ne savais pas à l'époque que les groupes constructibles étaient constructiblement isomorphes aux groupes algébriques[8], je lui parlais d'un corps dont le groupe additif comme le groupe multiplicatif étaient des groupes algébriques. Il fallut de longues et pénibles explications pour que la lumière se fît : "Ah, tu veux dire un schéma en anneau dont les points rationnels sur un corps algébriquement clos forment un corps !" Gopal Prasad, également présent sur les lieux, fut beaucoup plus pragmatique : "Let us see! What can be the additive group of the field? It is certainly not an abelian variety ... "

---

[7] Il ne l'est pas tout-à-fait : c'est le quotient de $SL_3(R)$ par son sous-groupe réduit à l'unité.

[8] Résultat exposé dans POIZAT 1987, p. 141 ; lui sont associés les noms de Weil, van den Dries et Hrushovski. J'ai reçu à son propos une intéressante lettre d'Alexandre Grothendieck, dont je tiens la copie à la disposition de mes lecteurs.

Le fossé s'est élargi après l'intervention de Grothendieck[9].

2. Une reformulation du Theorem 3

Pour mieux analyser le résultat de Borovik, nous le généralisons très légèrement, et nous en offrons une démonstration qui s'appuie directement sur le Théorème de Wagner, ce qu'évite Borovik qui préfère n'utiliser que la notion de "bon tore" qui en dérive (voir ABC 2008, p. 50).

Notre énoncé distingue la structure (G,M) formée du groupe algébrique G muni de sa loi de groupe, ainsi que d'un prédicat représentant son sous-groupe M, de la structure plus forte (K,G,M) formée du corps de base K et de la relation décrivant M comme sous-groupe de G (lequel est définissable dans K).

Théorème 2.1. *Considérons un groupe algébrique infini* $G(K) = G$ *sur un corps algébriquement clos* K *de caractéristique* p, *où* $G(\ )$ *est une formule du langage des corps à paramètres algébriques, définissant l'ensemble sous-jacent à* G *et sa multiplication, et un sous-groupe* M *de* $G(K)$ *contenant* $G(K_\infty)$, *où* K_∞ *est le corps des nombres algébriques en caractéristique* p.
(i) *Si la structure* (K,G,M) *a un rang de Morley fini, alors* $M = G$.
(ii) *Si* G *est simple et la structure* (G,M) *a un rang de Morley fini, alors* $M = G$.

Démonstration. (i) Comme les paramètres de la formule $G(\ )$ sont algébriques, il existe une puissance non triviale σ de l'automorphisme de Frobenius du corps K, associant x^p à x, qui induit un automorphisme σ^* de G ; l'intersection Γ de toutes les images de M par les puissances de σ^*, positives où négatives, est celle d'un nombre fini d'entre elles, si bien qu'elle est définissable dans (K,G,M). On observe que $G(K_\infty)$ est préservé par σ^*, et inclus dans Γ.

Maintenant on oublie M : la structure (K,G,Γ) n'est rien d'autre qu'un corps enrichi de rang de Morley fini, admettant σ comme automorphisme. D'après le théorème de Wagner rappelé ci-dessous, son modèle premier est porté par K_∞ ; donc $\Gamma = G$.
(ii) Si G est simple, d'après la version modèle-théorique du Théorème de Borel-Tits décrite dans la section suivante, (K,G,M) est de rang de Morley fini si et seulement si (G,M) l'est (Corollaire 4.6). **Fin**

Théorème de Wagner sur les corps (WAGNER 2001)**.** *Soit* K *un corps infini de rang de Morley fini, de langage possiblement enrichi ; alors :*

---

[9] C'est ainsi que j'ai averti un étudiant courageux qui voulait lire le SGA et les EGA comme un préliminaire à toute entreprise de travaux sur les groupes de rang de Morley fini : "Vous verrez que vous aurez du mal à comprendre ce qu'ils appellent une courbe." Olivier Chapuis, qui assistait à l'entretien, a ajouté : "Oh non, la vraie difficulté est de comprendre ce qu'ils appellent un point !"

(i) *le modèle premier de la théorie de* K *est la clôture algébrique modèle-théorique de l'ensemble vide ;*
(ii) K *élimine les imaginaires ;*
(iii) *si de plus la structure enrichie* K *a un automorphisme définissable non trivial, alors son modèle premier est porté par la clôture algébrique algébrique de l'ensemble vide, c'est-à-dire* K_∞ .

Nous appelons *corps de Wagner* un corps (enrichi) satisfaisant (iii) ; sa caractéristique est un nombre premier p , car le corps des invariants de l'automorphisme doit être fini. Observons que son langage ne peut nommer qu'un nombre fini de paramètres, tous algébriques ; on ne sait pas s'il existe des corps de Wagner autres que les corps nus avec un nombre fini de paramètres algébriques nommés.

La problématique sous-jacente au résultat de Borovik se résume à la question suivante : *si* G *est un groupe algébrique, sur un corps* K *algébriquement clos, et* M *est un sous-groupe de* G *, à quelles conditions les structures* (G, M) *ou* (K, G, M) *restent-elles de rang de Morley fini ?*

Par exemple, si la caractéristique de K est p , et si M est un sous-groupe propre divisible du groupe multiplicatif K* contenant sa torsion, (K*,M) est de rang de Morley deux, tandis que le rang de Morley de (K,K*,M) est infini. C'est une conséquence du Théorème de Wagner : comme K* n'a pas de p-éléments, si (K,K*,M) est de rang de Morley fini M est uniquement p-divisible, et l'automorphisme de Frobenius est un automorphisme de (K,K*,M) . D'ailleurs, d'après WAGNER 2003, il est très peu probable qu'on puisse trouver un sous-groupe propre infini M de K* tel que le rang de Morley de (K,K*,M) soit fini.

En caractéristique nulle, BHMPW 2009 ont construit un sous-groupe sans torsion M de K* tel que (K,K*,M) soit de rang de Morley deux, et CAYCEDO-HILS 2015 l'ont fait en incorporant à M de la torsion divisible arbitraire.

Du côté additif, en caractéristique nulle il est clairement impossible d'obtenir un sous-groupe M additif non trivial en gardant (K,K^+,M) de rang de Morley fini. Par contre, BMPZ 2007 ont construit un exemple de rang deux en caractéristique p .

ROCHE 2017 a ajouté des sous-groupes non-algébriques à des variétés abéliennes tout en préservant la finitude du rang.

Comme notre savoir-faire en la matière se limite aux groupe commutatifs, il est tentant de poser la question suivante, à laquelle MUSTAFIN-POIZAT 2007 apporte une réponse positive si $G = SL_2(K)$ ou $PSL_2(K)$.

Question B. *Soit* M *un sous-groupe du groupe algébrique* G *, sur un corps algébriquement clos* K *, tel que* (K,G,M) *soit de rang de Morley fini ; peut-on trouver des sous-groupes* A_1 , ... A_n *de groupes algébriques commutatifs tels que* (K,M) *et* $(K,A_1, \ldots A_n)$ *soient bi-interprétables ?*

Théorème 2.2. *Le Théorème 2.1.(ii) est aussi valable en caractéristique nulle (si* K_∞ *représente la clôture algébrique du corps des rationnels).*

Démonstration. Comme je l'ai dit dans l'introduction, c'est une conséquence de la démonstration alternative de Borovik pour son Theorem 3. **Fin**

3. Le Théorème de Borel-Tits et la théorie des modèles des groupes algébriques simples

Un groupe algébrique infini simple G, sur un corps algébriquement clos K, a des propriétés modèle-théoriques très particulières, qui tiennent aux quatre faits suivants :

(i) G a un sous-groupe de Borel non nilpotent, et en conséquence on peut définir à l'aide de sa seule loi de groupe un corps infini L ; c'est un fait très basique pour un algébriste (voir ABC 2008, p. 118), mais on peut aussi l'obtenir à partir de la pseudo-locale finitude de G (un contre-exemple minimal serait un mauvais groupe).

(ii) Comme nous l'avons dit, ce corps L est isomorphe au corps de base K, par un isomorphisme σ entre K et L qui est définissable dans K ; la construction de σ demande une familiarité minimale avec la Géométrie Algébrique, essentiellement pour montrer que le produit semi-direct de L^+ par L^* est un groupe algébrique affine.

(iii) D'après le premier résultat de Zil'ber sur la Théorie des Modèles du sujet (ZIL'BER 1977), le groupe nu G est ω_1-catégorique, et par conséquent son type générique n'est pas orthogonal à L ; selon un résultat général de Hrushovski sur les groupes simples de rang de Morley fini, G est L-interne, c'est-à-dire paramétrable par des points de L, grâce à l'aide d'un uplet fixé de points de G ; G est alors définissablement dans G (par une formule utilisant des paramètres) isomorphe à un groupe $G_1(L)$ définissable dans L ; en outre le groupe des automorphismes de G qui fixent point-par-point le corps L, qu'on appelle groupe de Galois ou groupe de liaison, est définissable (POIZAT 1987, Ch. 2.f).

(iv) Le groupe G a une copie isomorphe définissable dans K sans paramètres.

Théorème 3.1 (de Borel-Tits, version modèle-théorique). *Soient* G *un groupe algébrique simple sur un corps algébriquement clos* K, L *un corps infini définissable dans* G, *et* σ *un isomorphisme du corps* K *vers le corps* L *définissable dans* K *; alors l'isomorphisme de groupe* σ^* *entre* $G = G(K)$ *et* $G(L)$ *induit par* σ *est définissable dans la structure de groupe nue de* G.

Démonstration. Comme G est L-interne, il est définissablement dans G isomorphe à un groupe $G_1(L)$ définissable dans L. Quand nous revenons dans K en prenant l'image de L par σ^{-1}, nous voyons que $G_1(K)$ est isomorphe à G définissablement dans K, dans lequel tout est définissable ; autrement dit, $G(K)$ est isomorphe à $G_1(K)$ définissablement au sens du corps nu K ; en

appliquant σ, on voit que $G(L)$ est isomorphe à $G_1(L)$ par un isomorphisme définissable dans L ; comme L est définissable dans le groupe G, σ^* est composé d'un isomorphisme de G dans $G_1(L)$ et d'un isomorphisme de $G_1(L)$ dans $G(L)$ qui sont tout deux définissables dans le groupe nu G. **Fin**

Corollaire 3.2. *Si G est un groupe algébrique simple, sur un corps algébriquement clos K, tout sous-ensemble constructible (c'est-à-dire définissable dans K) d'une puissance cartésienne de G est définissable (avec paramètres) dans le groupe nu G.*

Démonstration. Si X est constructible au sens de K, $\sigma^*(X)$ est constructible au sens de L, donc définissable dans G, ainsi que son image réciproque par σ^*. **Fin**

Notes. (i) Etant donné le fossé qui sépare Logique et Géométrie[10], on ne trouve pas dans BOREL-TITS 1973 d'énoncé qui corresponde exactement au théorème ci-dessus ; des géomètres pourront même s'offusquer de voir associé un double nom aussi prestigieux à un résultat dont la démonstration demande si peu de connaissance de la structure du groupe. Ils considéreront au mieux le Corollaire 4.7 de la section suivante comme une version misérable du vrai Théorème de Borel-Tits, qui est plus riche (voir STEINBERG 1974), puisqu'il parle en réalité d'isogénies entre groupes quasi-simples et non pas seulement d'isomorphismes entre groupes simples (voir le Theorem 4 de BOROVIK 2023), dans un cadre qui n'est pas limité à celui d'un corps de base algébriquement clos. Cependant, on ne peut guère éviter de mentionner Borel et Tits à propos du Théorème 3.1 car son Corollaire 3.2, grâce à l'introduction du langage du premier ordre, donne un sens mathématique précis à une formulation heuristique vague du résultat (voir ZIL'BER 1984), à savoir que la structure de variété du groupe est déterminée (de quelle manière ?) par sa seule loi de groupe.
(ii) J'ai cru opportun de reprendre dans POIZAT 1988 l'essai de ZIL'BER 1984, qui exprimait dans son introduction l'intuition correcte que la Théorie des Modèles avait quelque chose à dire sur le Théorème de Borel-Tits ; mais il la traduisait ensuite dans un Lemma 5 dont l'énoncé m'a semblé insuffisant et la démonstration peu convaincante.
(iii) Le corps K lui-même ne vit pas dans l'univers de G ; c'est un objet du second ordre par rapport à G, c'est-à-dire un corps K tel que G soit $G(K)$; il a seulement un sosie, une copie L, qui est définissable dans G par une formule du premier ordre.
(iv) L'ingrédient essentiel de la démonstration, celui qui met en jeu la simplicité du groupe, est la notion d'internité de Hrushovski, valable dans des contextes bien plus généraux que la finitude du rang de Morley. Elle est l'aboutissement d'un long cheminement mathématique, car elle s'inscrit dans le prolongement de

[10] Voyez le sous-titre de POIZAT 1987.

la Théorie de Galois des équations algébriques (POIZAT 1983), de celle des équations différentielles linéaires, associée aux noms de Liouville, Picard et Vessiot, généralisée ensuite par Kolchin à ce que nous qualifions aujourd'hui d'équations différentielles internes au corps des constantes (POIZAT 1985, Ch. 18), et aussi du groupe de liaison ("binding group") de ZIL'BER 1980 (voir POIZAT 1987, p. 54).

Exemple 3.3. L'exemple le plus immédiat d'internité est donné par l'action à gauche G_g d'un groupe G sur lui-même, qui est la structure associée à la fonction binaire $x^{-1}.y$; G et G_g sont interdéfinissables, chacun ayant une copie définie sans paramètres dans l'autre : celle de G dans G_g est obtenue sur le quotient de $G\times G$ par la relation quaternaire d'équipollence $x^{-1}.y = u^{-1}.v$. En fixant un de ses points, on voit que G_g est G-interne, avec comme groupe de liaison l'action de G par translation sur lui-même.

Cette structure G_g , de même que sa duale G_d , est plus forte que la version affine G_{aff} du groupe G , définie par l'équipollence, et dont le groupe de liaison est le groupe des translations bilatères, isomorphe au produit de G par son groupe inverse divisé par le sous-groupe central-diagonal.

Cet exemple très simple nous confronte à une distinction subtile entre le défini et le définissable, qui est au cœur-même de la notion d'internité. Quand nous travaillons dans la structure G_g , le groupe G est définissable sans paramètres, étant paramétré par les couples de points de G_g : il est donc G_g-interne, avec un groupe de liaison réduit à l'identité ; G_g est définissablement isomorphe à la structure définie sur G par la fonction $x^{-1}.y$, mais pour témoigner d'un tel isomorphisme il faut fixer un point de G_g .

Exemple 3.4. Autre exemple classique : un plan projectif arguésien P , dont la relation de colinéation permet de définir un corps L ; P est L-interne, avec PSL_2 comme groupe de liaison, car on obtient un isomorphisme entre P et $P(L)$, le plan projectif associé au corps L , en fixant trois points ; ce plan est une structure constructible autonome au sens de la Définition 4.1 à venir.

Exemple 3.5. Les multicorps définis dans la Section 4.

Pour élever le débat, et nous placer dans ce qui est à mon avis le véritable cadre convenant au Théorème de Borel-Tits, nous développerons dans la section suivante les conséquences du Théorème 3.1 sur les isomorphismes dans un contexte plus abstrait, où il n'est plus question de groupes ; dans la dernière section, nous reviendrons aux particularités des groupes algébriques simples. En attendant, nous examinons ce que ce résultat nous dit de leurs extensions et restrictions élémentaires.

Si $G = G(K)$ est un groupe simple infini, défini dans un corps algébriquement clos K par une formule $G(\ )$ sans paramètres, comment pouvons-nous décrire la théorie du groupe nu G ?

Nous savons qu'il est possible de définir dans G, avec l'aide d'un uplet de paramètres $\bar{a}$, un corps L et un isomorphisme entre G et $G(L)$. Cela s'exprime par une formule élémentaire $\gamma(\bar{x})$ que $\bar{a}$ satisfait.

Notons $\gamma_n(\bar{x})$ la formule déclarant en outre que le corps L n'a pas d'extension de degré $\leq n$, et qui précise si $p = 0$ ou $p \neq 0$ suivant que $p \leq n$ est ou non la caractéristique du corps de base K. Comme tout corps infini définissable dans G est isomorphe à K, notre groupe satisfait $(\exists \bar{x})\, \gamma(\bar{x})$ et $(\forall \bar{x})\, \gamma(\bar{x}) \rightarrow \gamma_n(\bar{x})$.

Dans un modèle de cette liste d'énoncés T, on trouve $\bar{a}$ satisfaisant tous les $\gamma_n(\bar{a})$, si bien que ce modèle est isomorphe à $G(L)$ où L est un corps algébriquement clos ; comme T est ω_1-catégorique, ce qui était prévu par ZIL'BER 1977, c'est la théorie de G.

Si G_1 est une restriction élémentaire de G, il contient un $\bar{a}$ satisfaisant $\gamma(\bar{x})$, et cette formule a même sens dans G et dans G_1 ; réciproquement, si cela a lieu, G_1 est restriction élémentaire de G, car le plongement de G_1 dans G correspond au plongement naturel de $G(k)$ dans $G(K)$, où k est un sous-corps algébriquement clos de K.

Quand on relit l'énoncé du Theorem 3 de Borovik, on comprend alors que $G(K_\infty)$ est le modèle premier de la théorie de G, et que le plongement considéré est élémentaire. On en obtient donc la traduction suivante, qui sonne comme une musique divine aux oreilles des dévots de la Théorie des Modèles :

Théorème 3.6. *Si G est un groupe algébrique simple, sur un corps algébriquement clos, et M est un sous-groupe de G contenant une restriction élémentaire de G, tel que la structure (G, M) soit de rang de Morley fini, alors $M = G$.*

Le géomètre doit pour une fois - et c'est justice - être mis en garde contre un danger de confusion. Le modèle premier de la théorie du corps K, qui est le corps des nombres algébriques, est un sous-corps de K bien déterminé, bien que la Théorie de Galois nous donne une pléthore d'isomorphismes de K_∞ dans K. Par contraste, le modèle premier de la théorie du groupe G se plonge de multiples façons dans G, suivant le choix du paramètre $\bar{a}$; il n'est pas formé des points de G algébriques (au sens modèle-théorique) sur $\emptyset$ car G, étant simple, n'a pas de sous-groupe caractéristique propre. Par contre les extensions élémentaires de G ne causent pas de difficulté : elles correspondent aux extensions du corps K, puisque nous disposons dans G du paramètre $\bar{a}$.

Arrivé à ce point, je ne peux plus éviter la question de la modèle-complétude de la théorie de G ; elle semble liée à la nature de la formule $\gamma(\bar{x})$. D'après MUSTAFIN-POIZAT 2006 la réponse à la question suivante est positive dans le cas de PSL_2.

Question C. *Si* G = G(K) *est un groupe algébrique simple sur le corps algébriquement clos* K , *et si* k *est algébriquement clos, est-ce-que tout plongement de* G(k) *dans* G(K) *est élémentaire ? Plus précisément, existe-t'il un sous-corps* k' *de* K *isomorphe à* k *tel qu'il soit conjugué du plongement canonique de* G(k') *dans* G(K) *?*

Note. Dans CHERLIN 1979, Gregory Cherlin exprime son admiration pour le naturel et la simplicité de la démonstration de Zil'ber, tout en déclarant qu'il était parvenu à une conclusion semblable qui s'appuyait lourdement sur la structure des groupes algébriques simples ; comme sa démonstration est restée inédite, il est difficile de dire si ce qu'il avait en tête pourrait apporter quelque lumière sur les questions posées ici.

4. Un contexte débarrassé de toute référence à un groupe

Nous poursuivons l'étude du Théorème de Borel-Tits dans le cadre des structures constructives autonomes ainsi définies :

Définition 4.1. *Nous dirons que* S *est une structure constructible autonome, relativement au corps algébriquement clos* K , *si sa base, infinie, est constructible, ainsi que toutes les fonctions et relations nommées dans son langage, supposé fini, et si en outre, pour chaque* n , *toute partie constructible de* S^n *est définissable, avec paramètres, dans le langage de la structure* S .

Exemple 4.2. Le groupe $GL_2(K)$ n'est pas autonome. En effet, il est le produit de son dérivé $SL_2(K)$ par son centre, isomorphe à K* , qui est formé des matrices diagonales ; on définit une copie L du corps de base dans le dérivé, mais si on reste au niveau du groupe il n'y a aucun moyen d'établir une corrélation entre L et le centre. Le groupe $GL_2(K)$ est bidimensionnel, pas ω_1-catégorique.

D'après le Corollaire 3.2, les groupes algébriques simples sont notre paradigme de structures constructibles autonomes. La Proposition 1.20, p. 122, de ABC 2008 montre, par un argument assez opaque faisant intervenir les groupes radiciels, que les groupes algébriques quasi-simples le sont aussi. En fait, ce type de démonstration est extrêmement flexible, car il y a beaucoup de façons d'affecter aux points du groupe des coordonnées dans son quotient ; voici la plus simple que j'ai trouvée :

Théorème 4.3. (i) *Dans un contexte de rang de Morley fini, un groupe* G *quasi-simple, dont le générique n'est pas orthogonal à un ensemble définissable* A , *est* A-*interne*.
(ii) *Un groupe algébrique quasi-simple, sur un corps algébriquement clos, est autonome*.

Démonstration. (i) On note $H = G/Z(G)$; on obtient une surjection de $H \times H$ sur l'ensemble des commutateurs de G en associant à (x,y) le commutateur commun de leurs images réciproques dans G ; comme il existe un entier m tel que tout point du dérivé G' de G soit le produit de m commutateurs, cela donne une surjection f de H^{2m} sur G qui est définissable dans G. En effet, comme H est son propre dérivé, G' et G ont même rang, et $G = G'$.

Comme H est simple, et que son générique est co-algébrique à celui de G, il est A-interne, ainsi que $G = f(H^{2m})$.
(ii) $H = G/Z(G)$ permet de définir une copie L du corps de base K, image d'un isomorphisme σ définissable dans K ; comme il est autonome, l'application σ^* de $H(K)$ dans $H(L)$ est définissable dans sa structure de groupe nue ; comme $\sigma^*(f)$ est définissable dans L, l'application σ^* de $G(K)$ dans $G(L)$ est définissable dans le groupe nu G. **Fin**

Remarque 4.4. Cette démonstration ne montre pas que, si $G/Z(G)$ est un groupe algébrique, G en est un aussi ; en effet, le groupe $G/Z(G)$ définit un corps nu algébriquement clos L, et une copie de G est définissable dans L, mais il n'est pas sûr que L reste nu quand il est vu depuis G.

Nous montrons maintenant, pour les structures constructives autonomes, une sorte de réciproque au Corollaire 3.2, à savoir qu'elles sont K-internes, ce qui ne pose pas de difficultés car la définition de l'autonomie incorpore en quelque sorte l'internité. Après en avoir tiré quelques corollaires, nous préciserons ensuite la manière de définir en elles des copies du corps de base, ce qui facilitera l'étude de leurs automorphismes.

Notation. Soient σ un isomorphisme entre les corps K et L, et φ une formule du langage des corps, à paramètres dans K, définissant une structure S ; nous notons $\sigma^*\varphi$ la formule, à paramètres dans L, obtenue en remplaçant les paramètres de φ par leurs images par σ, et σ^*S la structure définie dans L par $\sigma^*\varphi$. Il faut remarquer que cet isomorphisme σ^* n'a de sens que si on fixe la formule définissant S.

Théorème 4.5. *Soit S une structure constructible autonome, sur le corps algébriquement clos K ; alors on peut définir dans S (ou plutôt S^{eq}) une copie L du corps K, isomorphe à K par un isomorphisme σ définissable dans K. Pour chacun de ces corps L, l'isomorphisme σ^* induit par σ entre S et σ^*S est définissable dans S. En outre, la théorie de S est ω_1-catégorique.*

Démonstration. Par élimination des imaginaires, S est isomorphe à une partie constructible d'une puissance cartésienne de K ; comme elle est infinie, une de ses projections P est infinie, ce qui donne une copie de K privée éventuellement d'un nombre fini de points ; comme tout point de K est somme

de deux points d'une quelconque de ses parties cofinies, on obtient une copie définissable de K sur un quotient de $P \times P$.

Comme σ^*S est définissable dans S et σ^* est définissable dans K , ce dernier est définissable dans S puisque que c'est une structure autonome.

On décrit la théorie de S à peu près comme nous l'avons fait dans le cas d'un groupe algébrique simple, sauf que maintenant il faut tenir compte des paramètres $\bar{b}$ dans L qui interviennent dans la formule définissant $\sigma^*(S)$, en plus des paramètres $\bar{a}$ dans S qui interviennent dans la définition de σ^* (par exemple, le corps K avec un point transcendant nommé dans son langage est une structure constructible autonome). On minimise le degré de transcendance de $\bar{b}$, si bien qu'aucun $\bar{\beta}$ de degré inférieur ne pourra définir un objet constructiblement isomorphe à S . Ces paramètres seront représentés par des uplets $\bar{x}$ et $\bar{y}$ dans la formule $\gamma(\bar{x},\bar{y})$, qui précise que $\bar{y}$ satisfait un système générateur des équations à coefficients entiers satisfaites par $\bar{b}$, et à la théorie on ajoute que si $\gamma(\bar{x},\bar{y})$ est satisfait alors $\bar{y}$ n'annule pas d'équations non satisfaites par $\bar{b}$. **Fin**

Corollaire 4.6. *Si on ajoute de la structure* Σ *à une structure constructible autonome* S *, sur un corps algébriquement clos* K *, de sorte que* (S, Σ) *reste de rang de Morley fini, alors* (K, S, Σ) *est de rang de Morley fini.*

Démonstration. La structure $(L, \sigma^*(S), \sigma^*(\Sigma))$, étant définissable dans (S, Σ) , est de rang de Morley fini, ainsi que son image réciproque par σ^* . **Fin**

Corollaire 4.7 (Théorème de Borel-Tits sur les isomorphismes). (i) *Soit* S *une structure constructible sur le corps algébriquement clos* K *d'une part, et sur le corps algébriquement clos* K' *d'autre part. On suppose que* S *est autonome relativement à* K *; alors les corps* K *et* K' *sont isomorphes, et* S *est autonome relativement à* K' .
(ii) *Soient* S *une structure constructible autonome, sur le corps algébriquement clos* K *, et un isomorphisme* τ *entre* S *et une structure* S' *constructible sur le corps algébriquement clos* K' *; alors* S' *est autonome, et les corps* K *et* K' *sont isomorphes, par un isomorphisme tel que* τ *se décompose en l'isomorphisme induit associé suivi d'un isomorphisme définissable dans* S' .

Démonstration. (i) S est à la fois défini par une formule $S(K)$ et une formule $S'(K')$. Comme elle est autonome du côté de K , on peut y définir une copie L de ce corps ; L , étant définissable dans K' , lui est définissablement isomorphe ; par ailleurs, S est définissablement, dans S et a fortiori dans K' , isomorphe à $S'(L)$; on en déduit que $S(L)$ et $S'(L)$, et aussi $S(K')$ et $S'(K')$, sont définissablement isomorphes au sens de K' . Or $S(K')$ est autonome.
(ii) L'isomorphisme τ fait apparaître S' comme $S(K_1)$ où $K_1 = \sigma(K)$ est un corps isomorphe à K ; autrement dit $\tau = \sigma^*$, et le corps K_1 a une copie L

définissable dans S' : le corps L est isomorphe à K_1 par θ définissable dans K_1. Le point (i) montre que S' = S'(K') est autonome, et que l'isomorphisme θ^* entre S' et S(L) est définissable dans S' ; τ est donc la composition de l'ismorphisme de S(K) vers S(L) induit par $\theta.\sigma$, suivi de θ^{*-1}. **Fin**

Corollaire 4.8 (Théorème de Borel-Tits sur les automorphismes). *Soient* S *une structure constructible autonome, sur le corps algébriquement clos* K, *un corps infini* L *définissable dans* S, *et un automorphisme* τ *de* S ; *alors* τ *se décompose en des homomorphismes constructibles et l'isomorphisme induit* σ^* *de* S(L) *sur* S(σ.L), *où* σ *est l'isomorphisme de corps induit par* τ *sur* L ; τ *est constructible (c'est-à-dire définissable dans* S, *ou de façon équivalente dans* K*) si et seulement si* σ *l'est.*

Démonstration. Soit α un isomorphisme de S = S(K) dans S(L) induit par un isomorphisme de K dans L définissable dans K ; τ le conjugue sur un isomorphisme α' entre S et S(σ.L) ; τ se décompose donc en α, σ^*, et l'inverse de α', les deux extrêmes étant définissables dans S. Si τ est définissable σ l'est aussi, et si σ est définissable σ^* l'est également. **Fin**

Théorème 4.9. *Soit* S *une structure constructible autonome, sur un corps algébriquement clos* K *de caractéristique nulle ; alors :*
(i) *on peut définir sans paramètres dans* S *(ou plus exactement dans* S^{eq}*) une copie* L *du corps* K *;*
(ii) *si* τ *est un automorphisme de* S *tel que la structure* (S, τ) *soit superstable,* τ *est constructible (c'est-à-dire définissable dans* S, *ou de façon équivalente dans* K *!) ;*
(iii) *si* τ *est un automorphisme d'ordre fini de* S, *son carré* τ^2 *est constructible ;*
(iv) *le groupe* Aut(S) *des automorphismes constructibles de* S *est lui-même constructible, et c'est le plus grand groupe d'automorphismes de* S *tel que* (S, Aut(S)) *soit superstable.*

Démonstration. (i) Nous avons vu qu'on peut définir dans S un corps L_1 définissablement isomorphe à K, avec l'aide d'un uplet de paramètres a_1, qu'on peut d'ailleurs supposer canonique pour la chose. Soit A l'ensemble des a qui permettent de définir un corps infini L_a de la même façon que a_1 permet de définir L_1 ; comme S élimine le quanteur "il existe une infinité de ... ", A est définissable dans S, et sans paramètres (il suffit d'ailleurs de déclarer que le corps est quadratiquement clos, c'est-à-dire satisfait à $(\forall x)(\exists y)\ y^2 - y = x$, pour garantir son infinitude).

Comme S est autonome, pour tout a dans A il existe un isomorphisme σ_b entre L_1 et L_a définissable dans S à l'aide d'un uplet de paramètres b. Montrons, par induction sur le rang et le degré de Morley de A, que la

définition de σ_b peut être obtenue uniformément lorsque a parcourt A ; pour cela, on considère (après avoir éventuellement remplacé S par une extension élémentaire saturée) a de rang maximum dans A ; la définition de son σ_b convient pour tout a' d'une partie A' de A de même rang de Morley que A, si bien que l'induction s'applique à A-A' ; il ne reste plus qu'à faire un patchwork pour assembler les morceaux, ce qui peut conduire à allonger b pour pouvoir distinguer des cas. Nous obtenons finalement un ensemble définissable B, et, pour b parcourant B, une famille uniformément définissable d'isomorphismes σ_b entre L_1 et un L_a, de sorte que chaque L_a soit l'image d'au moins un σ_b. Naturellement, beaucoup de paramètres interviennent dans la définition de B, par exemple a_1, ainsi que les paramètres de la décomposition de A.

Posant alors $\tau_c = \sigma_b.\sigma_{b'}^{-1}$, nous obtenons un ensemble C paramétrant une famille uniforme, close pour la prise d'inverse, d'isomorphismes entre un L_a et un $L_{a'}$, de sorte que pour chaque couple (a,a') dans $A\times A$ il y ait au moins un c dans C associé à un isomorphisme entre L_a et $L_{a'}$. En remplaçant C par la réunion des ensembles semblablement définis et ayant la même propriété, c'est-à-dire en incorporant au paramètre c ceux qui interviennent dans la définition de l'ensemble C, nous obtenons un ensemble D, qui a encore cette propriété, mais qui, lui, est définissable sans paramètres.

Comme nous sommes en caractéristique nulle, le corps L_a n'a pas d'automorphisme constructible autre que l'identité, et il n'y a qu'un seul isomorphisme définissable entre L_a et $L_{a'}$. Nous considérons alors la réunion disjointe des L_a, qui est l'ensemble U des couples (a,x), $a \in A$, $x \in L_a$; sur cet ensemble, la relation E suivante est définissable sans paramètres : $(a,x)\ E\ (a',y)$ s'il existe d dans D tel que τ_d soit un isomorphisme entre L_a et $L_{a'}$ et que $\tau_d(x) = y$; elle n'est rien d'autre que la relation d'équivalence qui déclare que x et y se correspondent par l'unique isomorphisme définissable entre L_a et $L_{a'}$, et le corps L cherché est le quotient U/E.

(ii) Comme le corps L est définissable sans paramètres dans S, τ induit un automorphisme σ superstable de L, qui ne peut être que l'identité d'après un résultat de Hrushovki (voir POIZAT 1987, p. 191 ; j'ai écrit "superstable" pour rendre hommage à Hrushovski, mais c'est à peu près évident si on suppose le rang de Morley fini) ; τ est donc constructible d'après le Corollaire 4.8.

(iii) τ induit un automorphisme σ d'ordre fini du corps algébriquement clos L ; d'après le Théorème d'Artin, s'il ne vaut pas l'identité, c'est la conjugaison relativement à un sous-corps réel-clos de L de codimension deux, dont le carré vaut l'identité.

(iv)[11] Comme S est L-interne, ses automorphismes qui fixent point par point le corps L constituent le groupe de liaison, qui est définissable dans S . **Fin**

Le traitement de la caractéristique p est plus délicat, et nécessite la définition suivante.

Définition 4.10. *Nous appelons* multicorps *une structure constructible dont la base* $M = (L_1, \ldots L_n)$ *est la réunion disjointe d'un nombre fini de copies du corps de base (algébriquement clos)* K , *et le langage est constitué des quatre relations suivantes :*
(i) *l'équivalence exprimant que* x *et* y *appartiennent au même* L_i *;*
(ii) *le graphe de l'addition des corps, composé des triplets* (x,y,z) *appartenant au même* L_i *et tels que* z *soit la somme de* x *et de* y *au sens de ce corps ;*
(iii) *le graphe du produit des corps défini semblablement ;*
(iv) *et enfin une relation binaire* $\theta(x,y)$ *dont la restriction à* $L_i \times L_j$ *est le graphe d'un isomorphisme* θ_{ij} *entre les corps* L_i *et* L_j *; on supposera que chaque* θ_{ii} *vaut l'identité.*

Exemple 4.11. Nous décrivons ici tous les bicorps $B = (L_1,L_2)$, en remplaçant la quatrième relation par une fonction θ de B dans B dont la restriction au premier corps est un isomorphisme θ_1 de L_1 vers L_2 , et sa restriction θ_2 au second est un isomorphisme de L_2 vers L_1 . On remarque que θ est un automorphisme de la structure, qui échange les deux corps, et que B est une structure autonome équivalente au corps K dès qu'on se permet de fixer un paramètre ; nous allons déterminer les circonstances qui font que le bicorps permet de définir *sans paramètres* une copie de K .

En caractéristique nulle, $\theta_2.\theta_1(x)$ est par hypothèse un automorphisme constructible du corps L_1 , qui vaut donc l'identité, et il en est de même de $\theta_1.\theta_2(y)$; autrement dit θ_2 et θ_1 sont inverses l'un de l'autre, θ est involutive, et on obtient un troisième corps L_3 définissable sans paramètres dans B en passant au quotient par la relation d'équivalence $y = x \vee y = \theta(x)$. Ce cas n'a aucun intérêt, car le bicorps n'est alors rien d'autre qu'une simple duplication du corps de base K .

En caractéristique p , $\theta_2.\theta_1(x)$ est une puissance, positive ou négative, de l'automorphisme de Frobenius : $\theta_2.\theta_1(x) = x\hat{}p^n$. Symétriquement, $\theta_1.\theta_2(y) = y\hat{}p^n$; en effet, y est de la forme $y = \theta_1(x)$, et $\theta_1.\theta_2.\theta_1(x) = \theta_1(x\hat{}p^n) = y\hat{}p^n$.

Supposons dans un premier temps que $n = 1$, et montrons que B n'a pas d'automorphisme involutif σ ; si σ est d'ordre fini et conserve les deux corps, il vaut l'identité d'après le Théorème d'Artin ; s'il les échange, c'est une involution, de la forme $\sigma = (\sigma_1,\sigma_2)$, où σ_1 et σ_2 sont inverses l'un de l'autre ;

[11] Je dois cet argument à Hrushovski, que je remercie ; en effet, dans la version première de cet article, indigne disciple de Liouville, Picard, Vessiot et Krasner, je n'avais pas reconnu le groupe de Galois !

comme σ un automorphisme de la fonction θ , il doit commuter avec elle, ce qui signifie que $\varphi = \theta_2.\sigma_1 = \sigma_2.\theta_1$, si bien que le carré de φ est l'automorphisme de Frobenius $\theta_2.\theta_1$ du corps algébriquement clos L_1 . Cela est interdit par la théorie de Galois des corps finis, car le groupe des automorphismes du corps à p^d éléments est cyclique et engendré par le frobenius ; or si d est pair le générateur du groupe cyclique d'ordre d n'est pas un carré.

Le même raisonnement vaut si l'exposant n est impair : B n'a pas d'automorphismes involutifs, et en fait pas d'automorphismes d'ordre fini autre que l'identité.

Si $n = 2m$ est pair, l'automorphisme involutif $(\theta_1(x\hat{}p^{-m}),\theta_2(y\hat{}p^{-m}))$ est définissable sans paramètres, et c'est d'ailleurs l'unique automorphisme d'ordre fini de B . Dans ce cas, un passage au quotient permet de définir sans paramètres une troisième copie L_3 du corps de base K .

Théorème 4.12. *Soit* S *une structure constructible autonome, sur un corps algébriquement clos* K *de caractéristique* p *; alors*
(i) *on peut définir sans paramètres dans* S *un multicorps ;*
(ii) *si* τ *appartient à un groupe superstable d'automorphismes de* S *, il est constructible ;*
(iii) *si* τ *est un automorphisme d'ordre fini de* S *, il est constructible ;*
(iv) *il n'y a qu'un nombre fini de groupes superstables maximaux d'automorphismes de* S *; ils sont tous constructibles et ont tous même composante connexe.*

Démonstration. (i) De même qu'en caractéristique nulle, nous définissons sans paramètres une famille uniforme L_a de copies de K , ainsi qu'une famille uniforme, indexée par D , d'automorphismes les reliant.

En caractéristique p les automorphismes définissables du corps K sont les puissances du frobenius, et si σ et τ sont deux isomorphimes entre L_a et $L_{a'}$, on doit avoir $\sigma.x = (\tau.x)^q = \tau.(x^q)$, où $q = p^n$ pour un certain entier relatif n . Pour chaque a , nous considérons l'ensemble définissable des automorphismes y de L_a qui s'obtiennent par composition d'un isomorphisme de L_a vers un $L_{a'}$ et d'un isomorphisme de ce $L_{a'}$ vers L_a , tous deux paramétrés dans D . Ils forment une famille discrète, chacun d'eux étant de la forme $y = x\hat{}p^n$, où n est un entier relatif ; par compacité, ils sont en nombre fini, et si on fixe a la relation exprimant que x et y dans L_a se correspondent par un de ces automorphismes s'écrit $(y-x\hat{}q_1).(y-x\hat{}q_2). \ldots . (x-y\hat{}r_1).(x-y\hat{}r_2). \ldots = 0$, où les q_i et les r_j sont des puissances positives de la caractéristique. Par élimination des quanteurs dans K , le degré de ce polynôme est borné (je ne vois pas pour cela de démonstration basée sur l'absence de propriété de recouvrement fini), et il existe un entier N , indépendant de a , tel que $-N \leq n \leq N$ pour tous les exposants n décrivant cette famille d'automorphismes de L_a .

On voit que, quels que soient a et a' dans A, il y a au plus $2N+1$ isomorphismes distincts entre L_a et $L_{a'}$ qui sont paramétrés par D. Nous pouvons les individualiser en les ordonnant, en décrétant que $\sigma \leq \tau$ si $\tau.x = (\sigma.x)\hat{}p^n$ pour un $n \geq 0$; l'existence de N permet de distinguer le plus petit, et obtenir une famille uniforme $\sigma_{aa'}$, indexée par $A\times A$, d'automorphismes de L_a dans $L_{a'}$.

Fixons maintenant un type π dans A de rang de Morley maximum. Nous définissons sur l'ensemble U la relation E_π suivante : $(a,x)\ E_\pi\ (a',y)$ si pour tout g dans π, indépendant de $\{a, x, a', y\}$, $\sigma_{ag}(x) = \sigma_{a'g}(y)$. E_π est une relation d'équivalence : pour vérifier qu'elle est transitive, on prend g dans π indépendant de tout le monde. Et elle est définissable car le type π l'est, mais sa définition demande l'emploi du paramètre (imaginaire) canonique de π, lequel est algébrique sur $\emptyset$. Posons $L_\pi = U/E_\pi$; les conjugués de L_π forment un ensemble fini, définissable sur $\emptyset$, de copies de K.

(ii) Ce point nous renvoie à une question ouverte depuis longtemps, antérieure à la Conjecture d'Algébricité, puisqu'elle est posée dans MACINTYRE 1971, et met en scène un corps de Wagner avant l'heure : *un corps de rang de Morley fini peut-il avoir un automorphisme définissable non constructible, c'est-à-dire autre qu'une puissance du frobenius ?* En caractéristique p, le résultat de Hrushovski cité plus haut affirme seulement qu'un groupe A d'automorphismes de K tel que (K,A) soit superstable est réduit à l'identité.

Notons σ l'action de τ sur un multicorps $M = (L_1, \ldots L_n)$ définissable sans paramètres ; comme c'est un automorphisme pour la relation θ, $\sigma.\theta_{ij} = \theta_{i'j'}.\sigma$ quand $\sigma(L_i) = L_{i'}$ et $\sigma(L_j) = L_{j'}$. Si σ fixe l'un de ces corps, l'hypothèse implique qu'il le fixe point par point, et est constructible d'après le Corollaire 4.8 ; s'il échange deux d'entre eux, l'étude des bicorps que nous avons faite montre qu'il les fixe tous les deux, ou bien fixe un troisième corps, et on conclut de même.

Pour traiter le cas général, nous considérons un cycle de longueur q de l'action de σ sur ces corps, que nous notons $(L_1, L_2, \ldots L_q)$: modulo q, $\sigma(L_i) = L_{i+1}$. Remarquons que l'hypothèse implique que σ^q agit comme l'identité sur chacun des corps L_i.

Si nous renommons θ_i l'isomorphisme $\theta_{i,i+1}$ entre les corps L_i et L_{i+1}, l'automorphie de σ se traduit par $\sigma.\theta_i = \theta_{i+1}.\sigma$. La restriction σ_i de σ à L_i s'écrit $\theta_i.\beta_i$ où β_i est un automorphisme du corps L_i, et la commutation de σ et de θ s'exprime par : $\theta_{i+1}.\theta_i.\beta_i = \theta_{i+1}.\beta_{i+1}.\theta_i$, soit encore $\beta_{i+1}.\theta_i = \theta_i.\beta_i$.

Par ailleurs $\theta_q. \ldots . \theta_2.\theta_1$ est un automorphisme α constructible du corps L_1, c'est-à-dire une puissance du Frobenius. En conclusion, la restriction de σ^q à L_1 vaut $Id = \theta_q.\beta_q. \ldots . \theta_2.\beta_2.\theta_1.\beta_1 = \theta_q. \ldots .\theta_2.\theta_1.\beta_1{}^q = \alpha.\beta_1{}^q$. Il en suit que β_1 est lui aussi une puissance du frobenius ; il en est de même de chaque β_i, si bien que l'action de σ sur $(L_1, L_2, \ldots L_q)$ est définissable.

Pour pouvoir appliquer le Corollaire 4.8, on observe que σ comme τ agissent sur le corps définissable L, quotient du multicorps $(L_1, L_2, \ldots L_q)$ par le groupe cyclique engendré par σ.
(iii) On reprend la démonstration du point précédent, et on constate que le Théorème d'Artin implique que σ fixe chaque point du corps L.
(iv) Soient $M = (L_1, \ldots L_n)$ un multicorps définissable sans paramètres dans S, et A la composante connexe du groupe (constructible car c'est un groupe de liaison) des automorphismes de S qui fixent point par point chacun des corps $L_1, \ldots L_n$; A est normalisé par tous les automorphismes de S. Nous avons vu que, si τ appartient à un groupe superstable d'automorphismes de S, il appartient au groupe A_L des automorphismes fixant point par point un corps L obtenu par quotient à partir de cycles de $L_1, \ldots L_n$; A est la composante connexe de A_L, et comme il n'y a qu'un nombre fini de possibilités pour L, il n'y a aussi qu'un nombre fini de choix pour τ modulo A. **Fin**

5. Retour aux groupes algébriques simples

L'idéologie gouvernant cet article, c'est qu'on peut démontrer des résultats subtils de Géométrie Algébrique par des arguments triviaux de Théorie des Modèles. Ce genre de sport a ses limites, et, quand il est question d'un groupe algébrique simple G, pour trouver des applications concrètes à ces résultats il est souvent nécessaire d'aller voir de plus près la structure de G.

Pour pouvoir préciser de quoi on parle, nous introduisons la définition suivante :

Définition 5.1. *Un groupe constructible autonome est un groupe algébrique infini, considéré dans un langage constructible qui lui confère l'autonomie et qui contient sa loi de groupe.*

On peut se demander si, ici comme ailleurs, la présence d'une loi de groupe a un effet de redressement sur les frobenius :

Question D. *Dans un groupe constructible autonome sur un corps algébriquement clos de caractéristique* p *, peut-on définir sans paramètres une copie du corps de base ?*

Nous commençons par quelques cas particuliers, qui donnent l'impression que la question se pose principalement pour les variétés abéliennes.

1. Le groupe G est le groupe additif K^+ du corps de base ; en caractéristique nulle, les automorphismes définissables de G sont de la forme $x \to a.x$; en caractéristique p il y en a d'autres, de la forme $a.x^{p^n}$, mais tout groupe infini définissable d'automorphismes de G correspond à l'action d'une copie du corps de base (voir POIZAT 1987, Chapitre 3.b). L'autonomie permet de définir, à l'aide d'un uplet a de paramètres, une copie K_a de l'action du corps K sur son groupe additif G ; en quotientant la réunion des K_a par la relation

d'équivalence "avoir même action sur G ", on définit sans paramètres un groupe A d'automorphismes de G ; l'anneau engendré par A est une copie du corps de base définie sans paramètres : sur $A \cup \{0\}$, l'addition se fait point par point et la multiplication est la composition.

La même démonstration vaut pour un "groupe vectoriel" G , isomorphe à $(K^+)^n$; en effet, l'anneau des endomorphismes linéaires de G est définissable grâce à un uplet de paramètres comprenant une base de G ; c'est en fait le plus grand anneau définissable d'endomorphismes de G , le seul à être de dimension n^2 ; la définissabilité du rang de Morley permet d'obtenir une famille uniforme de copies de cet anneau, que le quotient par l'équivalence "avoir même action sur G " pourvoit d'une définition sans paramètres ; le corps K est son centre.

2. G est le groupe multiplicatif K^* du corps K . Quels sont alors les corps constructibles dont G est le groupe multiplicatif ? Comme ces corps sont définissablement isomorphes, ce sont les images du corps K par les automorphismes constructibles de G . Comme G est une variété affine, un endomorphisme constructible de G s'écrit comme une composition d'un polynôme multiplicatif en x et x^{-1} et d'une puissance du frobenius ; ce dernier conserve les corps, et les seules applications x^n qui soient bijectives sont x et x^{-1} . Autrement dit, il n'y a que deux corps constructibles K_1 et K_2 , dont G soit le groupe multiplicatif : leurs additions se correspondent par conjugaison par l'inversion de G , et un nouveau quotient définit sans paramètres une copie du corps K .

3. Si G est le groupe $SL_2(K)$, on définit une copie du corps de base grâce au groupe vectoriel V dérivé d'un de ses borels B ; V est conjugué de ses semblables puisque les borels le sont. Mais les conjugaisons sont des morphismes algébriques, qui ne peuvent introduire de puissances du frobenius, si bien qu'en caractéristique p comme en caractéristique nulle elles ne peuvent définir qu'un unique isomorphisme entre deux corps de la famille ; un passage au quotient donne alors la copie du corps de base cherchée.

En généralisant ce dernier exemple, on répond à la Question D dans un cas significatif :

Théorème 5.1. *Un groupe algébrique simple (infini) permet de définir sans paramètres une copie du corps de base, même en caractéristique* p .

Démonstration. Les borels du groupe sont conjugués, ainsi que les composantes connexes des groupes des éléments d'ordre p des centres de leurs dérivés, qui sont des groupes vectoriels (non triviaux !) d'après HUMPHREYS 1981, Proposition 20.2 p. 127 et Corollary 20.4 p. 130. **Fin**

Par ailleurs le Corollaire 4.7 appliqué aux groupes donne ceci :

Corollaire 5.2. *Tout isomorphisme entre un groupe algébrique simple* G = G(K) *, sur le corps* K *algébriquement clos, et un groupe* H = H(L) *algébrique sur le corps algébriquement clos* L *, lorsque ces deux groupes sont munis de leur structures de variétés respectives, envoie constructible sur constructible et fermé de Zariski sur fermé de Zariski.*

Démonstration. Tout isomorphisme échange les ensembles définissables, qui sont dans le cas présent les constructibles ; quand on considère les groupes comme des variétés algébriques, les transports de structure échangent les fermés de Zariski ; il en est de même des automorphismes de groupe constructibles, car ce sont des morphismes en caractéristique nulle, et des quasi-morphismes en caractéristique p (combinaisons de morphismes et de puissances négatives du frobenius). **Fin**

Ce Corollaire 5.2 enveloppe d'un mystère ténébreux la Conjecture d'Algébricité : si elle est vérifiée, il y aura une façon intrinsèque de distinguer les fermés de Zariski parmi les ensembles définissables dans les groupes simples nus ! Une réciproque est donnée par HRUSHOVSKI-ZIL'BER 1996.

D'autre part, nous avons montré que, si A est un groupe de rang de Morley fini (ou même seulement superstable) d'automorphismes de G , il est composé d'automorphismes constructibles. Mais, pour les applications, on a besoin d'un résultat plus fort : sa composante connexe A° est formée d'automorphismes intérieurs, comme il est montré - un peu rapidement à mon goût[12] - dans ABC 2008 p. 134, qui s'appuie sur un théorème de HUMPHREYS 1981 qu'il vaut la peine de citer in extenso :

Theorem (HUMPHREYS 1981, p.160). *Let G be semisimple.*
(a) Aut *G* = (Int *G*)*D*.
(b) *The natural map D* → *Γ induces a monomorphism* Aut *G*/Int *G* → *Γ ; in particular,* Int *G has finite index in* Aut *G*.

Chez Humphreys, Aut G désigne le groupe des automorphismes du groupe G qui sont, ainsi que leurs inverses, des *morphismes* de la variété de G : ce sont des applications polynomiales puisque la variété de G est affine. En caractéristique nulle, ils sont identiques aux automorphismes constructibles du groupe G . En caractéristique p , les automorphismes constructibles de G sont des quasi-morphismes ; comme G est un groupe affine définissable sans paramètres, ils sont de la forme $\alpha.\varphi$ où α est un polynôme et φ l'automorphisme induit par une puissance du frobenius ; en minimisant son degré, on peut supposer que α n'est pas un polynôme en les puissances p° des inconnues ; l'inverse de α est alors de la même forme $\beta.\varphi'$; $\alpha.\beta.\varphi'^{r-1} = Id$, et

[12] Que signifie "As *F* can be interpreted in a Borel *B* and the action of *Aut(F)* on *F* can be interpreted via its action on *B*, …" ? De plus la citation de Humphreys n'est pas conforme à l'original.

en différentiant on voit que φ' est l'identité, si bien que α est un isomorphisme au sens géométrique.

On voit que $\mathrm{Aut}\, G$ est normal dans le groupe des automorphismes constructibles de G, car $\varphi.\alpha = \alpha'.\varphi$, où le polynôme α' est obtenu en faisant agir φ sur les coefficients du polynôme α.

$\mathrm{Int}\, G$ est le groupe des automorphismes intérieurs, isomorphe à G, D est le groupe des automorphismes qui fixent un borel et un tore maximal donnés, et Γ est le groupe (fini) des automorphismes du système de racines associé.

On en déduit, suivant Altinel, Borovik et Cherlin, que $\mathrm{Aut}\, G$ est définissable dans le corps K. Nous précisons la suite :

Théorème 5.3. *Soient G un groupe algébrique simple sur un corps algébriquement clos K, et A un groupe d'automorphismes de G tel que la structure (G,A) soit superstable ; alors les éléments de A sont des morphismes géométriques.*

Démonstration. D'après le Corollaire 4.8, A est formé d'automorphismes de groupe constructibles. En caractéristique nulle, ce sont des morphismes.

En caractéristique p, ce sont des composés de morphismes et d'action d'une puissance du frobenius sur une représentation linéaire à coefficients entiers du groupe G. Comme $\mathrm{Aut}(G)$ est définissable, on peut l'inclure dans A en préservant la superstabilité ; et alors le quotient $A/\mathrm{Aut}(G)$, s'il n'était pas trivial, serait cyclique infini. C'est clairement impossible dans le cas ω-stable ; pour obtenir l'impossibilité dans le cas superstable, on vérifie que l'hypothèse est conservée quand on remplace (G,A) par une extension élémentaire saturée. **Fin**

Remarque 5.4. Au bout du compte, nous constatons une cohérence de notations, car le groupe, noté $\mathrm{Aut}(G)$ par Humphreys, des automorphismes géométriques de G est bien le plus grand groupe superstable d'automorphismes de G, ceux qui fixent point par point le corps du Théorème 5.1. C'est à la fois rassurant et troublant, car, si la notion de constructible se suffit à elle-même au niveau de G, celle de morphisme n'a de sens que vue de K.

L'amour de la généralité, et celui de ma spécialité mathématique favorite, m'invite à conclure par une dernière question :

Question E. *Peut-on trouver une raison purement modèle-théorique expliquant pourquoi la composante connexe de $\mathrm{Aut}(G)$ est formée des automorphismes intérieurs, c'est-à-dire expliquant pourquoi le groupe $\mathrm{Aut}(G)$ a même dimension que G ?*

Exercice final. La citation ouvrant cet article est extraite de l'édition de 1932 du Larousse du XX° siècle ; j'invite mes lectrices et mes lecteurs à essayer de la placer dans la conversation.

Références

ABC 2008 Tuna Altinel, A.V. Borovik & Gregory Cherlin, *Simple Groups of Finite Morley Rank,* American Mathematical Society

BHMPW 2009 Andreas Baudisch, Martin Hils, Amador Martín Pizarro & Frank Wagner, *Die böse Farbe,* Journal de l'Institut de Mathématiques de Jussieu, 8, 415-443

BMPZ 2007 Andreas Baudisch, Amador Martin-Pizarro & Martin Ziegler, *Red Fields,* the Journal of Symbolic logic, 72, 207-225

BOREL 1970 Armand Borel, *Properties and linear representations of Chevalley groups,* Lecture Notes in Mathematics 131

BOREL-TITS 1973 Armand Borel & Jacques Tits, *Homomorphismes "abstraits" de groupes algébriques simples,* Annals of Mathematics, 97, 499-571

BOROVIK 1984 Aleksandr Vasil'evič Borovik, *Théorie des groupes finis et groupes incomptablement catégoriques* (en russe), prépublication n° 511, Novosibirsk

BOROVIK 2023 Id., *Finite group actions on abelian groups of finite Morley rank,* à paraître au Journal of Model Theory

BOROVIK-NESIN 1994 Aleksandr Vasil'evič Borovik & Ali Azizoğlu Nesin, *Groups of Finite Morley Rank,* Clarendon Press, Oxford

CACEYDO-HILS 2015 Juan Diego Caceydo & Martin Hils, *Bad fields with torsion,* the Journal of Symbolic Logic, 80, 221-233

CHERLIN 1979 Gregory Cherlin, *Groups of small Morley rank,* Annals of Mathematical Logic, 17, 1-23

HRUSHOVSKI-ZIL'BER 1996 Ehud Hrushovski & Boris Zil'ber, *Zariski geometries,* Journal of the American Mathematical Society, 9, 1-56

HUMPHREYS 1981 James E. Humphreys, *Linear Algebraic Groups,* Springer

MACINTYRE 1971 Angus Macintyre, *On ω_1-categorical theories of fields,* Fundamenta Mathematicae, 71, 1-25

MUSTAFIN-POIZAT 2006 Yerulan Mustafin & Bruno Poizat, *Sous-groupes superstables de $SL_2(K)$ et de $PSL_2(K)$,* Journal of Agebra, 297, 155-167

POIZAT 1983 Bruno Poizat, *Une théorie de Galois imaginaire,* the Journal of Symbolic Logic, 48, 1151-1170

POIZAT 1985 Id., *Cours de Théorie des Modèles,* Nur al-Mantiq wal-Ma'rifah

POIZAT 1987 Id., *Groupes Stables,* Nur al-Mantiq wal-Ma'rifah

POIZAT 1988 Id., *MM. Borel, Tits, Zil'ber et le Général Nonsense,* the Journal of Symbolic Logic, 53, 124-131

POIZAT 2001 Id., *Quelques modestes remarques à propos d'une conséquence inattendue d'un résultat surprenant de Monsieur Frank Olaf Wagner,* the Journal of Symbolic Logic, 66, 1637-1646

ROCHE 2017 Olivier Roche, Thèse de doctorat, Université Claude Bernard (Lyon-I)

STEINBERG 1974 Robert Steinberg, *Abstract homomorphisms of simple algebraic groups,* Séminaire Bourbaki, n° 435, 307-426

THOMAS 1983 Simon Thomas, *The classification of simple periodic linear groups,* Archiv der Math., 41, 103-116

WAGNER 2001 Frank Wagner, *Fields of finite Morley rank,* the Journal of Symbolic Logic, 66, 703-706

WAGNER 2003 Id., *Bad fields in positive characteristic,* Bulletin of the London Mathematical Society, 35, 499-502

WEIL 1948 André Weil, *Foundations of Algebraic Geometry,* American Mathematical Society

ZIL'BER 1977 Boris Iosifović Zil'ber, *Groupes et anneaux de théorie catégorique* (en russe), Fundamenta Mathematicae, 55, 173-188

ZIL'BER 1980 Id., *Totally categorical theories; structural properties and the non-finite axiomatizability,* Lecture Notes in Mathematics, 834, 381-410

ZIL'BER 1984 Id., *Some model theory of simple algebraic groups over algebraically closed fields,* Colloquium Mathematicum, 48, 173-180

20 septembre 2024

ON THE RK-PREORDER ON C-CONES OF RK-MINIMAL ULTRAFILTERS

N.L. Polyakov

HSE University,
11 Pokrovksy Bulvar, Moscow, 109028, Russia
e-mail: npolyakov@hse.ru

Many works in the theory of ultrafilters consider different (pre)orders on the set $\boldsymbol{\beta}X$ (of ultrafilters on the set X). Apparently, the Rudin-Keisler and Comfort preorders on $\beta\omega$ are most well studied, see, e.g., [1, 2, 3], but there are still many open problems in this area. In this paper we describe the Rudin-Keisler preorder on the lower cones of RK-minimal ultrafilters with respect to the Comfort preorder.

1 Basic definitions

For any set X the set of all subsets of X is denoted by $\mathscr{P}(X)$. An *ultrafilter* on X is a set $\mathfrak{u} \subseteq \mathscr{P}(X)$ such that

1. $\emptyset \notin \mathfrak{u}$;
2. if $A \in \mathfrak{u}$ and $B \in \mathfrak{u}$, then $A \cap B \in \mathfrak{u}$;
3. if $A \in \mathfrak{u}$ and $A \subseteq B$, then $B \in \mathfrak{u}$;
4. $A \in \mathfrak{u}$ or $X \setminus A \in \mathfrak{u}$

for all $A, B \subseteq X$. The set of ultrafilters on X is usually denoted by $\boldsymbol{\beta}X$ and provided with a natural topology with the base

$$\{\{\mathfrak{u} \in \boldsymbol{\beta}X : A \in \mathfrak{u}\} : A \subseteq X\}.$$

This topological space is compact, Hausdorff, zero-dimensional and extremely disconnected. An ultrafilter $\mathfrak{u} \in \boldsymbol{\beta}X$ is *principal* if $\mathfrak{u} = \{A \subseteq X : a \in A\}$ for some $a \in X$. Principal ultrafilters on X are usually identified with elements

of X, so $\boldsymbol{\beta}X$ is considered as an extension of X (called a *StoneČech compactification* of X). For any function $f : X \to \boldsymbol{\beta}Y$, the *ultrafiter extension* $\widetilde{f} : \boldsymbol{\beta}X \to \boldsymbol{\beta}Y$ is defined by the formula

$$\widetilde{f}(\mathfrak{u}) = \{S \subseteq Y : (\forall A \in \mathfrak{u})\,(\exists a \in A)\, S \in f(a)\}$$

for all $\mathfrak{u} \in \boldsymbol{\beta}X$. We obtain an equivalent definition if we put

$$\widetilde{f}(\mathfrak{u}) = \{S \subseteq Y : (\exists A \in \mathfrak{u})\,(\forall a \in A)\, S \in f(a)\}.$$

The function $\widetilde{f}$ is the unique continuous (with respect to the natural topology) function from $\boldsymbol{\beta}X$ to $\boldsymbol{\beta}Y$ which extends the function f. Considering functions $f : X \to Y$ as functions from X to $\boldsymbol{\beta}Y$ with a range consisting of principal ultrafilters, we also have the definition of the ultrafilter extension $\widetilde{f} : \boldsymbol{\beta}X \to \boldsymbol{\beta}Y$ for each function $f : X \to Y$.

The *Rudin-Keisler preorder* (or RK-*preorder*) on $\boldsymbol{\beta}X$ is the binary relation $\leqslant_{\mathrm{RK}} \subseteq \boldsymbol{\beta}X \times \boldsymbol{\beta}X$ defined by

$$\mathfrak{u} \leqslant_{\mathrm{RK}} \mathfrak{v} \Leftrightarrow \widetilde{f}(\mathfrak{v}) = \mathfrak{u} \text{ for some } f : X \to X.$$

An ultrafilter $\mathfrak{u} \in \boldsymbol{\beta}X$ is called RK-*minimal* if it is non-principal and

$$\mathfrak{v} \leqslant_{\mathrm{RK}} \mathfrak{u} \;\Rightarrow\; \mathfrak{v} \text{ is principal or } \mathfrak{u} \leqslant_{\mathrm{RK}} \mathfrak{v}$$

for any $\mathfrak{v} \in \boldsymbol{\beta}X$. There are many different characterizations of RK-minimal ultrafilters, see [4], Theorem 9.6, and also [5]. In particular, a non-principal ultrafilter $\mathfrak{u} \in \boldsymbol{\beta}\omega$ is RK-minimal if and only if it is a Ramsey ultrafilter and if and only if it is a quasi-normal ultrafilter.

The equivalence relation $\leqslant_{\mathrm{RK}} \cap \leqslant_{\mathrm{RK}}^{-1}$ is denoted by $\approx_{\mathrm{RK}}$. The equivalence class of an ultrafilter $\mathfrak{u} \in \boldsymbol{\beta}X$ with respect to the relation $\approx_{\mathrm{RK}}$ is called *a type* of ultrafilter $\mathfrak{u}$ and is denoted by $\tau(\mathfrak{u})$, see [4]. The Rudin-Keisler preorder naturally extends to the quotient set $\boldsymbol{\beta}X/_{\approx_{\mathrm{RK}}}$: $\tau(\mathfrak{u}) \leqslant_{\mathrm{RK}} \tau(\mathfrak{v}) \Leftrightarrow \mathfrak{u} \leqslant_{\mathrm{RK}} \mathfrak{v}$ for all types $\tau(\mathfrak{u})$ and $\tau(\mathfrak{v})$ of ultrafilters $\mathfrak{u}$ and $\mathfrak{v}$, respectively. Obviously, $\leqslant_{\mathrm{RK}}$ is a partial order on $\boldsymbol{\beta}X/_{\approx_{\mathrm{RK}}}$. Therefore, we call the relation $\leqslant_{\mathrm{RK}}$ on the set $\boldsymbol{\beta}X/_{\approx_{\mathrm{RK}}}$ the *Rudin-Keisler order* (or RK-*order*).

To define the Comfort preorder on $\boldsymbol{\beta}X$ we need some topological concepts. Let $\mathfrak{u} \in \boldsymbol{\beta}X$. A point $y \in Y$ of a topological space (Y, T) is called the $\mathfrak{u}$-limit of a function $f : X \to Y$ if for any neighborhood U of y the set $\{x \in X : f(x) \in U\}$ belongs to $\mathfrak{u}$. The $\mathfrak{u}$-limit of a function f is denoted by the symbol $\mathfrak{u}\text{-}\lim f$. A topological space (Y, T) is called $\mathfrak{u}$-*compact* if for any $f : X \to Y$ there exists $\mathfrak{u}\text{-}\lim f \in Y$. The *Comfort preorder* $\leqslant_{\mathrm{C}}$ on $\boldsymbol{\beta}X$ is defined as follows: for all ultrafilters $\mathfrak{u}, \mathfrak{v} \in \boldsymbol{\beta}X$, $\mathfrak{u} \leqslant_C \mathfrak{v}$ iff any $\mathfrak{v}$-compact topological space (Y, T) is $\mathfrak{u}$-compact.

It is well known that $\leqslant_{\mathrm{RK}} \subseteq \leqslant_{\mathrm{C}}$, and hence $\approx_{\mathrm{RK}}$ is a congruence of the structure $(\boldsymbol{\beta}X; \leqslant_{\mathrm{C}})$. Thus, we can assume that the Comfort preorder is defined on $\boldsymbol{\beta}X/_{\approx_{\mathrm{RK}}}$. More information can be found in the [2, 3].

The C-*cone* of an ultrafilter $\mathfrak{u} \in \boldsymbol{\beta}X$ is the set

$$\mathrm{Con}_{\mathrm{C}}(\mathfrak{u}) = \{\tau(\mathfrak{v}) : \mathfrak{v} \in \boldsymbol{\beta}X \text{ and } \mathfrak{v} \leqslant_{\mathrm{C}} \mathfrak{u}\}.$$

An ultrafilter $\mathfrak{u} \in \boldsymbol{\beta}X$ is called C-*minimal* if it is non-principal and

$$\mathfrak{v} \leqslant_{\mathrm{C}} \mathfrak{u} \Rightarrow \ \mathfrak{v} \text{ is principal or } \mathfrak{u} \leqslant_{\mathrm{C}} \mathfrak{v}$$

for any $\mathfrak{v} \in \boldsymbol{\beta}X$. It is well known (see [2]) that if the type of ultrafilter $\mathfrak{v} \in \boldsymbol{\beta}\omega \setminus \omega$ belongs to the C-cone of some RK-minimal ultrafilter $\mathfrak{u} \in \boldsymbol{\beta}\omega$, then $\mathfrak{v}$ is a C-minimal ultrafilter. The inverse implication remains an open problem.

2 Main result

For all posets $\mathfrak{A} = (A, \leqslant_0)$ and $\mathfrak{B} = (B, \leqslant_1)$, their *sum* is the poset $\mathfrak{A} + \mathfrak{B} = (C, \leqslant_2)$, where $C = A \cup B'$, $A \cap B' = \emptyset$, $(A, \leqslant_2) = \mathfrak{A}$, $(B', \leqslant_2) \cong \mathfrak{B}$, and $a \leqslant_2 b$ for all $a \in A$ and $b \in B'$.

For any model $\mathfrak{M}$ and ultrafilter $\mathfrak{u} \in \boldsymbol{\beta}X$, the ultrapower of $\mathfrak{M}$ modulo $\mathfrak{u}$ is denoted by $\prod\limits_{\mathfrak{u}} \mathfrak{M}$.

For any limit ordinal α and non-decreasing sequence $\{\mathfrak{M}_\beta\}_{\beta<\alpha}$ of models in the same signature, the direct limit of $\{\mathfrak{M}_\beta\}_{\beta<\alpha}$ is denoted by $\lim\limits_{\beta\to\alpha} \mathfrak{M}_\beta$.

For any poset $\mathfrak{A}$, ultrafilter $\mathfrak{u} \in \boldsymbol{\beta}X$, and ordinal α, define the *overbuilding ultralimit* $\operatorname{olim}\limits_{\mathfrak{u},\alpha}$ of $\mathfrak{A}$ of rank α modulo $\mathfrak{u}$ by recursion on α:

i. $\operatorname{olim}\limits_{\mathfrak{u},0} \mathfrak{A} = \mathfrak{A}$;

ii. if $\alpha = \beta + 1$, $\operatorname{olim}\limits_{\mathfrak{u},\beta} \mathfrak{A} = (A, \leqslant_0)$, and $\prod\limits_{\mathfrak{u}} \operatorname{olim}\limits_{\mathfrak{u},\beta} \mathfrak{A} = (B, \leqslant_1)$ then

$$\operatorname{olim}_{\mathfrak{u},\alpha} \mathfrak{A} = \operatorname{olim}_{\mathfrak{u},\beta} \mathfrak{A} + \mathfrak{B},$$

where $\mathfrak{B}$ is the submodel of $\prod\limits_{\mathfrak{u}} \operatorname{olim}\limits_{\mathfrak{u},\beta} \mathfrak{A}$ with the universe

$$\{b \in B : (\forall a \in A)\, b \cap a = \emptyset\};$$

iii. if α is a limit ordinal, then $\operatorname{olim}\limits_{\mathfrak{u},\alpha} \mathfrak{A} = \lim\limits_{\beta\to\alpha} \operatorname{olim}\limits_{\mathfrak{u},\beta} \mathfrak{A}$.

This construction resembles the construction of a *limiting ultrapower* of a model (also called an *ultralit* of a model), but does not coincide with it. In particular, an overbuilding ultralimit of positive rank of a finite poset $\mathfrak{A}$ is not isomorphic to $\mathfrak{A}$.

Denote the one-element poset $(1, \leqslant)$ by $\mathfrak{O}$.

Theorem 1. *For any* RK*-minimal ultrafilter* $\mathfrak{u} \in \boldsymbol{\beta}\omega$

$$(\mathrm{Con_C}(\mathfrak{u}), \leqslant_{\mathrm{RK}}) \cong \operatorname*{olim}_{\mathfrak{u},\omega_1} \mathfrak{O}.$$

Sketch of proof. First, we establish the "ordinal stratification" of the Comfort preorder on $\boldsymbol{\beta}\omega/_{\approx_{\mathrm{RK}}}$ (essentially introduced in [8, 9]). For any ultrafilter $\mathfrak{u} \in \boldsymbol{\beta}\omega$ and ordinal α we define the sets $U_\alpha(\mathfrak{u}), U_{<\alpha}(\mathfrak{u}) \subseteq \boldsymbol{\beta}\omega/_{\approx_{\mathrm{RK}}}$:

i. $U_0(\mathfrak{u}) = \{\tau(0)\}$,

ii. for $\alpha > 0$, we put $U_{<\alpha}(\mathfrak{u}) = \bigcup\limits_{\beta<\alpha} U_\beta(\mathfrak{u})$ and

$$U_\alpha(\mathfrak{u}) = \{\tau(\widetilde{f}(\mathfrak{u})) : f \in (\boldsymbol{\beta}\omega)^\omega \text{ and } (\forall i < \omega)\, \tau(f(i)) \in U_{<\alpha}(\mathfrak{u})\}.$$

We prove that for each ultrafilters $\mathfrak{u} \in \boldsymbol{\beta}\omega$

$$\mathrm{Con_C}(\mathfrak{u}) = U_{<\omega_1}(\mathfrak{u}). \tag{1}$$

Next, we show that if an ultrafilter $\mathfrak{u}$ is RK-minimal, then we can restrict ourselves to injective functions $f : \omega \to \boldsymbol{\beta}\omega$ with a discrete range when constructing the sets $U_\alpha(\mathfrak{u})$. A set $W \subseteq \boldsymbol{\beta}X$ is *discrete* if there is a partition $\{A_{\mathfrak{w}}\}_{\mathfrak{w}\in W}$ of X such that $A_{\mathfrak{w}} \in \mathfrak{w}$ for all $\mathfrak{w} \in W$. Let DF be a set of all injective functions $f : \omega \to \boldsymbol{\beta}\omega$ with a discrete range. For any ultrafilter $\mathfrak{u} \in \boldsymbol{\beta}\omega$ and ordinal $\alpha > 0$ we define the sets $V_\alpha(\mathfrak{u}), V_{<\alpha}(\mathfrak{u}) \subseteq \boldsymbol{\beta}\omega/_{\approx_{\mathrm{RK}}}$:

i. $V_1(\mathfrak{u}) = \{\tau(\mathfrak{u})\}$,

ii. for $\alpha > 1$, we put $V_{<\alpha}(\mathfrak{u}) = \bigcup\limits_{\beta<\alpha} V_\beta(\mathfrak{u})$ and

$$V_\alpha(\mathfrak{u}) = \{\tau(\widetilde{f}(\mathfrak{u})) : f \in \mathrm{DF} \text{ and } (\forall i < \omega)\, \tau(f(i)) \in V_{<\alpha}(\mathfrak{u})\}.$$

We prove that for any positive ordinal α and RK-minimal ultrafilter $\mathfrak{u} \in \boldsymbol{\beta}\omega$

$$U_\alpha(\mathfrak{u}) = V_\alpha(\mathfrak{u}) \cup \{\tau(0)\}. \tag{2}$$

Finally, we will need the fact that for all functions $f, g \in \mathrm{DF}$ and ultrafilter $\mathfrak{u} \in \boldsymbol{\beta}\omega$

$$\widetilde{f}(\mathfrak{u}) \leqslant_{\mathrm{RK}} \widetilde{g}(\mathfrak{u}) \Leftrightarrow \{i < \omega : f(i) \leqslant_{\mathrm{RK}} g(i)\} \in \mathfrak{u} \tag{3}$$

(see, e.g., [10]).

Using the facts (1) – (3), the theorem can be easily proved by induction on α. □

The equivalence relation $\leqslant_{\mathrm{C}} \cap \leqslant_{\mathrm{C}}^{-1}$ on $\boldsymbol{\beta}X/_{\approx_{\mathrm{RK}}}$ is denoted by $\approx_{\mathrm{C}}$. For any $\mathfrak{u} \in \boldsymbol{\beta}X$, let $[\mathfrak{u}]_{\mathrm{C}} = \{\tau(\mathfrak{v}) : \mathfrak{v} \in \boldsymbol{\beta}X \text{ and } \tau(\mathfrak{v}) \approx_{\mathrm{C}} \tau(\mathfrak{u})\}$. It is easy to see that for any RK-minimal ultrafilter $\mathfrak{u} \in \boldsymbol{\beta}\omega$ and non-principal ultrafilter $\mathfrak{v} \leqslant_{\mathrm{C}} \mathfrak{u}$ we have: $\mathfrak{u} \leqslant_{\mathrm{RK}} \mathfrak{v}$ and, so,

$$[\mathfrak{v}]_{\mathrm{C}} \cup \{\tau(0)\} = \mathrm{Con}_{\mathrm{C}}(\mathfrak{u}).$$

Therefore, theorem 1 immediately entails the following corollary.

Corollary 1. *Let* $\mathfrak{u}, \mathfrak{v} \in \boldsymbol{\beta}\omega$. *If* $\mathfrak{u}$ *is* RK*-minimal and* $\tau(\mathfrak{u}) \in [\mathfrak{v}]_{\mathrm{C}}$, *then*

$$([\mathfrak{v}]_{\mathrm{C}}, \leqslant_{\mathrm{RK}}) \cong \operatorname*{olim}_{\mathfrak{u},\omega_1} \mathfrak{O}.$$

Discussion. Can the poset $\operatorname*{olim}_{\mathfrak{u},\omega_1} \mathfrak{O}$ be described more explicitly? Note that, e.g., $\operatorname*{olim}_{\mathfrak{u},\omega+1} \mathfrak{O}$ is isomorphic to the ultrapower of $(\omega, \leqslant)$ modulo $\mathfrak{u}$ where $\leqslant$ is the natural ordering of ω. Are the posets $\operatorname*{olim}_{\mathfrak{u},\omega_1} \mathfrak{O}$ and $\operatorname*{olim}_{\mathfrak{v},\omega_1} \mathfrak{O}$ isomorphic for all RK-minimal ultrafilters $\mathfrak{u}, \mathfrak{v} \in \boldsymbol{\beta}\omega$? Let us call a C-minimal ultrafilter $\mathfrak{v} \in \boldsymbol{\beta}\omega$ a *normal C-minimal ultrafilter* if $\tau(\mathfrak{u}) \in [\mathfrak{v}]_{\mathrm{C}}$ for some RK-minimal ultrafilter $\mathfrak{u} \in \boldsymbol{\beta}\omega$. Is the statement inverse to Corollary 1 true? In other words, is it true that the condition "there exists an RK-minimal ultrafilter $\mathfrak{u} \in \boldsymbol{\beta}\omega$ for which $([\mathfrak{v}]_{\mathrm{C}}, \leqslant_{\mathrm{RK}}) \cong \operatorname*{olim}_{\mathfrak{u},\omega_1} \mathfrak{O}$" exactly characterises normal C-minimal ultrafilters $\mathfrak{v} \in \boldsymbol{\beta}\omega$?

References

[1] A.R. Blass, The Rudin-Keisler ordering of P-points // Trans. Amer. Math. Sot. 179 (1973), 145–166.

[2] S. García-Fereira, Three orderings on $\beta(\omega) \setminus \omega^*$ // Topology and its Applications 50, 3 (1990): 199–216.

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

[4] W.W. Comfort, S. Negrepontis, The theory of ultrafilters. Springer, Berlin (1974).

[5] N.L. Polyakov, On the Canonical Ramsey Theorem of Erdős and Rado and Ramsey Ultrafilters // Dokl. Math. 108 (2023): 392–401.

[6] N.L. Poliakov, D.I. Saveliev, On two concepts of ultrafilter extensions of first-order models and their generalizations // Logic, Language, Information, and Computation, Lecture Notes in Computer Science, 10388, eds. J. Kennedy, R. J. G. B. de Queiroz, Springer, Berlin, Heidelberg, 2017, 336–348.

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

[8] D.I. Saveliev (joint work with N.L. Polyakov), Between the RudinKeisler and Comfort preorders // Report at the conference Ultramath, Pisa (2022).

[9] N.L. Poliakov, D.I. Saveliev, Between the RudinKeisler and Comfort preorders // Report at the International Conference on Topology and its Applications, Nafpaktos (2023).

[10] D.D. Booth, Ultrafilters on a countable set // Ann. Math. Logic 2 (1970) l–24.

ПРЕЛИЕВЫ ДУБЛИ ВИТТА

А.П. Пожидаев

ИМ СО РАН, пр. Ак. Коптюга 4, Новосибирск, Российская Федерация
e-mail: app@math.nsc.ru

Введение

Данная статья является вариантом доклада, представленного на XVI международной конференции "*Пограничные вопросы теории моделей и универсальной алгебры*" (Эрлагол-2024), который расширен в изложении новых результатов и сокращен в обзорной части. Доказательства приводимых результатов могут быть найдены в [1].

Напомним, что алгебра $\mathcal{A}$ над полем F называется *левосимметрической* (или *прелиевой*), если она удовлетворяет тождеству левосимметричности

$$(x, y, z) = (y, x, z).$$

Аналогично определяются правосимметрические алгебры, которые антиизоморфны левосимметрическим. Самыми известными левосимметрическими алгебрами являются ассоциативные алгебры и алгебры Новикова. Лево(право)симметрические алгебры естественно возникают и используются в различных областях математики (см. предыдущие работы автора по данной тематике, например, [2]).

Пусть d — ненулевое дифференцирование алгебры $\mathcal{A}$. Напомним, что $\mathcal{A}$ называется *d-простой*, если умножение в $\mathcal{A}$ нетривиально и в $\mathcal{A}$ нет собственных d-инвариантных идеалов; при этом дифференцирование d называется *простым*.

В [2] даны различные обобщения конструкции Мицухары и построены некоторые классы простых прелиевых алгебр, полученных при помощи данных конструкций, в частности, — простые дубли Витта $\mathcal{A}_d$ и $\mathcal{W}_d(\mathcal{A})$ ассоциативной коммутативной d-простой алгебры $\mathcal{A}$ с ненулевым дифференцированием d.

Оказывается, что автоморфизмы данных конечномерных дублей Витта сводятся (в характеристике $p > 2$) к автоморфизмам исходной алгебры $\mathcal{A}$, которые (почти)перестановочны (с точностью до некоторого обратимого элемента) с дифференцированием d.

Отметим, что изучению групп автоморфизмов, перестановочных с простым дифференцированием алгебры $K[x_1, \ldots, x_n]$ над алгебраически замкнутым полем K характеристики 0, посвящено множество работ (см., например, [3-4]). Заметим, что вопросы описания простых дифференцирований и (почти)перестановочных с ними автоморфизмов алгебры многочленов от $n \geq 2$ переменных остаются открытыми как над полями характеристики 0, так и над полями характеристики $p > 0$. Некоторые дальнейшие ссылки по данной тематике могут быть найдены, например, в [3].

Зафиксируем произвольное основное поле F, мультипликативную группу которого обозначим через F^*. Если $\mathcal{A}$ — некоторая алгебра над F, то через $\operatorname{Aut}\mathcal{A}$ обозначаем группу автоморфизмов алгебры $\mathcal{A}$.

1 Автоморфизмы дубля Витта $\mathcal{A}_d$

Прежде всего напомним самый известный пример левосимметрической алгебры, на котором основаны дубли Витта. Пусть $\mathcal{A}$ — ассоциативная коммутативная алгебра над полем F, d — ненулевое дифференцирование алгебры $\mathcal{A}$ (линейное над F). Определим на $\mathcal{A}$ новое умножение правилом $x \circ y = xd(y)$. Обозначим полученную алгебру через $\mathcal{A}(d)$. Хорошо известно, что $\mathcal{A}(d)$ является алгеброй Новикова, т. е., в частности, левосимметрической алгеброй. В случае характеристики не 2 хорошо известно, что $\mathcal{A}(d)$ проста тогда и только тогда, когда $\mathcal{A}$ является d-простой (см., например, [5]).

Автоморфизм ψ алгебры $\mathcal{A}$ такой, что $\psi d = d\psi$ будем называть *перестановочным* с дифференцированием d. Обозначим через $\operatorname{Aut}_d\mathcal{A}$ подмножество в $\operatorname{Aut}\mathcal{A}$, состоящее из автоморфизмов перестановочных с d:

$$\operatorname{Aut}_d\mathcal{A} := \{\phi \in \operatorname{Aut}\mathcal{A} : \phi d = d\phi\}.$$

Предложение 1. $\operatorname{Aut}_d\mathcal{A}$ *является подгруппой в* $\operatorname{Aut}\mathcal{A}$.

Пусть $\mathcal{A}$ — ассоциативная коммутативная алгебра над полем F с ненулевым дифференцированием d и $\overline{\mathcal{A}}$ — изоморфная копия алгебры $\mathcal{A}$ (как векторного пространства).

Дубль Витта $\mathcal{A}_d$. Рассмотрим прямую сумму $\mathcal{A} \oplus \overline{\mathcal{A}}$, где произведение определено правилами

$$\bar{x} \cdot y = xd(y), \quad x \cdot \bar{y} = 0, \quad x \cdot y = xy + \overline{xy}, \quad \bar{x} \cdot \bar{y} = \overline{xd(y)}$$

для всех $x, y \in \mathcal{A}$. Полученная алгебра обозначается через $\mathcal{A}_d$ и называется *дублем Витта* алгебры $\mathcal{A}$. В [2] доказано, что $\mathcal{A}_d$ является левосимметрической алгеброй, которая проста тогда и только тогда, когда d-проста алгебра $\mathcal{A}$.

Легко видеть, что любой автоморфизм $\phi \in \operatorname{Aut} \mathcal{A}_d$ однозначно определяется четверкой линейных отображений ψ, η, θ, π алгебры $\mathcal{A}$, а именно

$$\phi(a) = \psi(a) + \overline{\eta(a)}, \quad \phi(\bar{a}) = \theta(a) + \overline{\pi(a)}.$$

Обозначим ϕ через $(\psi, \eta, \theta, \pi)$, а отображение $\phi = (\psi, 0, 0, \psi)$ — через $\psi + \overline{\psi}$.

Теорема 1. *Пусть $\mathcal{A}$ — конечномерная ассоциативная коммутативная d-простая алгебра, которая не является полем, d — ненулевое дифференцирование алгебры $\mathcal{A}$. Тогда $\phi \in \operatorname{Aut} \mathcal{A}_d$ тогда и только тогда, когда $\phi = \psi + \overline{\psi}$ для некоторого $\psi \in \operatorname{Aut}_d \mathcal{A}$.*

Следствие 1. *Пусть $\mathcal{A}$ — конечномерная ассоциативная коммутативная d-простая алгебра над алгебраически замкнутым полем F. Тогда*

$$\operatorname{Aut} \mathcal{A}_d \cong \operatorname{Aut}_d \mathcal{A}.$$

2 Автоморфизмы обобщенного дубля Витта $\mathcal{W}_d(\mathcal{A})$

Дубль Витта $\mathcal{W}_d(\mathcal{A})$. Рассмотрим прямую сумму $\mathcal{A} \oplus \overline{\mathcal{A}}$, где произведение определено правилами

$$x \cdot y = xy, \ x \cdot \bar{y} = \overline{xy}, \ \bar{x} \cdot y = xd(y) + \overline{xy}, \ \bar{x} \cdot \bar{y} = \overline{xd(y)}$$

для всех $x, y \in \mathcal{A}$. Полученная алгебра обозначается через $\mathcal{W}_d(\mathcal{A})$ и называется левосимметрическим *обобщенным дублем Витта*.

В [2] доказано, что $\mathcal{W}_d(\mathcal{A})$ является левосимметрической алгеброй, которая проста тогда и только тогда, когда d-проста алгебра $\mathcal{A}$.

Автоморфизм ψ алгебры $\mathcal{A}$ такой, что $\psi d = \alpha d \psi$ для некоторого обратимого $\alpha \in \mathcal{A}$, будем называть *обратимо перестановочным* (α-*перестановочным*) с d (*скалярно перестановочным*, если $\alpha \in F^*$). Обозначим через $\operatorname{Aut}_d^* \mathcal{A}$ и $\operatorname{Aut}_d^\star \mathcal{A}$ подмножества в $\operatorname{Aut} \mathcal{A}$, состоящие из автоморфизмов, скалярно и обратимо перестановочных с d:

$$\operatorname{Aut}_d^* \mathcal{A} := \{\phi \in \operatorname{Aut} \mathcal{A} : \phi d = \alpha d \phi \text{ для некоторого } \alpha = \alpha_\phi \in F^*\};$$

$\mathrm{Aut}_d^\star \mathcal{A} := \{\phi \in \mathrm{Aut}\,\mathcal{A} : \phi d = \alpha d\phi$ для некоторого обратимого $\alpha = \alpha_\phi \in \mathcal{A}\}$.

Предложение 2. *$\mathrm{Aut}_d^* \mathcal{A}$ и $\mathrm{Aut}_d^\star \mathcal{A}$ являются подгруппами в $\mathrm{Aut}\,\mathcal{A}$; при этом $\mathrm{Aut}_d\,\mathcal{A}$ является нормальной подгруппой в $\mathrm{Aut}_d^* \mathcal{A}$.*

Рассмотрим отображение $\phi = (\psi, 0, 0, \alpha_\psi\psi)$. При $\psi \in \mathrm{Aut}_d^* \mathcal{A}$ выполняется равенство $\psi d = \alpha d\psi$ для некоторого $\alpha \in F^*$. Так как дифференцирование d предполагается фиксированным, то в этом случае α однозначно определяется по автоморфизму ψ. Будем использовать обозначение ϕ_ψ для автоморфизма $\phi = (\psi, 0, 0, \alpha_\psi\psi)$.

Лемма 1. *Пусть $\phi = (\psi, 0, \theta, \pi)$ и $\mathrm{Ker}\,\theta = 0$. Тогда $\phi \in \mathrm{Aut}\,\mathcal{W}_d(\mathcal{A})$ тогда и только тогда, когда $1 \in \mathrm{Im}\,d$, $\psi \in \mathrm{Aut}_d^\star \mathcal{A}$, и $\phi := \psi(\gamma) := (\psi, 0, \gamma\psi, \alpha\psi)$, где $\gamma^2 + \alpha d(\gamma) = 0, 2\gamma + d(\alpha) = 0$, α, γ — обратимые элементы из $\mathcal{A}$.*

При $\psi \in \mathrm{Aut}_d^\star \mathcal{A}$ выполняется равенство $\psi d = \alpha d\psi$ для некоторого фиксированного обратимого $\alpha = \alpha_\psi \in \mathcal{A}$. В случае характеристики не 2 элемент γ из леммы 1 однозначно определяется по α. Таким образом, автоморфизм $\psi(\gamma)$ алгебры $\mathcal{W}_d(\mathcal{A})$ полностью определяется автоморфизмом $\psi \in \mathrm{Aut}_d^\star \mathcal{A}$. Будем также использовать обозначение ${}_\psi\phi$ для $\psi(\gamma)$ в случае поля характеристики не 2.

Теорема 2. *Пусть $\mathcal{A}$ — конечномерная ассоциативная коммутативная d-простая алгебра над алгебраически замкнутым полем F характеристики не 2, $d \neq 0$. Тогда $\phi \in \mathrm{Aut}\,\mathcal{W}_d(\mathcal{A})$ тогда и только тогда, когда либо $\phi = \phi_\psi$ при $\psi \in \mathrm{Aut}_d^* \mathcal{A}$, либо $\phi = {}_\psi\phi$ при $\psi \in \mathrm{Aut}_d^\star \mathcal{A}$.*

Следствие 2. *Пусть $\mathcal{A}$ — конечномерная ассоциативная коммутативная d-простая алгебра над алгебраически замкнутым полем характеристики не 2, $d \neq 0$. Тогда*

$$\mathrm{Aut}\,\mathcal{W}_d(\mathcal{A}) \cong \mathrm{Aut}_d^\star \mathcal{A}.$$

Список литературы

[1] A. P. Pozhidaev, Automorphism groups of the pre-Lie Witt doubles, Sib. Mat. Zh. **65**, 6 (2024); translation in Sib. Math. J. **65**, 6 (2024).

[2] A. P. Pozhidaev, On a generalized Mizuhara construction, Sib. Mat. Zh. **65**, 3 (2024), 545–559; translation in Sib. Math. J. **65**, 3 (2024), 599–610.

[3] L. N. Bertoncello, D. Levcovitz, On the isotropy group of a simple derivation, J. Pure Appl. Algebra **224**, 1 (2020), 33–41.

[4] L. G. Mendes, I. Pan, On plane polynomial automorphisms commuting with simple derivations, J. Pure Appl. Algebra **221**, 4 (2016), 875–882.

[5] V. N. Zhelyabin, A. S. Tikhov, Novikov–Poisson algebras and associative commutative derivation algebras, Algebra i Logika **47**, 2 (2008), 186–202; translation in Algebra and Logic **47**, 2 (2008), 107–117.

АЛГЕБРА КОНЕЧНЫХ ПРЕДИКАТОВ И МОДЕЛИРОВАНИЕ ГИБКИХ ПРОЦЕССОВ

М.Н. Рудометкина*, А.В. Чехонадских**

*ТУСУР **НГТУ
*пр. Ленина, 40, г. Томск, 634050, РФ
**пр. К. Маркса, 20, г. Новосибирск, 630048, РФ
e-mail: mn.rud@inbox.ru, chekhonadskikh@corp.nstu.ru

Обзор посвящен логико-алгебраическим аспектам математического аппарата, предназначенного для анализа процессов (process mining) с использованием искусственного интеллекта. Сфера применения таких средств охватывает разработку программного обеспечения для преобразования информационных ресурсов и поиска информации в web-источниках, разбора текстов и метатекстов, скомпонованных из разнородного материала, для бизнес-процессов и сложных технологических схем, инженерно-конструкторских работ и др.

Прежде всего, рассматривается алгебра конечных предикатов как универсальный язык описания дискретных моделей процессов различной природы, в том числе требующих компараторной идентификации в дополнение к структурной и параметрической.Далее указываются особенности логических сетей как средства распараллеливания задач обработки символьной информации в системах искусственного интеллекта; вкратце приводятся принципы сетевого представления сложно разветвленных процессов в виде Workflow-сетей (WF-nets) на основе структуризации их логов (следов выполнения с метками времени) и иерархизации модели. Особое внимание уделено моделированию и настройке гибких процессов (flexible processes), в том числе в идентификации и автоматизации синтеза инженерно-технических систем.

Ключевые слова: конечный предикат, алгебра предикатов, дискретный процесс, логическая сеть, гибкий процесс, анализ процессов, настраиваемая модель, древовидный граф, стационарная линейная система, система автоматического управления, регулятор пониженного порядка, критическая корневая диаграмма.

1 Введение

Большинство интеллектуальных систем, искусственных или естественных, дискретно. Естественными средствами описания для них оказываются понятия и структуры дискретной математики: языки программирования, логические исчисления, язык теории алгоритмов, аппарат теории графов. Однако непосредственному использованию этих средств для моделирования гибких процессов препятствует то, что они предполагают описание функциональных или однозначных алгоритмов, в то время как модели гибких процессов включают нефункциональные отношения, т.е. многозначные связи, для формализации которых используется аппарат алгебры конечных предикатов (АКП).

Приближение дискретных языков к постоянно расширяющемуся кругу прикладных задач инициирует появление ряда новых концепций. Например, основная функция естественного интеллекта — способность к речевому общению в естественных языках — многозначна, в силу чего естественный язык предполагает формальные средства выражения многозначных и множественнозначных соотношений, то есть семантических соответствий произвольного вида.

Алгебры высказываний и предикатов (Линденбаума-Тарского) содержат такие возможности. Однако логические исчисления, дополненные аппаратом булевых уравнений, сопряжены с двоичной семантикой, чего для представления (моделирования) гибких процессов недостаточно. Если классическая логика семантически факторизуется в двузначную булеву алгебру, то в интеллектуальных системах, равно как и в естественном языке, приходится использовать многозначные буквенные символы. Аппарат многозначной логики приближается к естественному языку, однако и в ее семантике преобладают однозначные функции, а не отношения. А теория уравнений в многозначной логике находится в предварительной стадии развития.

Использование исчисления предикатов для целей математического описания интеллектуальных систем наталкивается на ту же трудность: исчисление малопригодно для описания конечных объектов. Исчисление предикатов не располагает универсальными средствами для записи произвольных конечных отношений в виде формул [1, 2].

Для формализации конечных объектов и процессов, оперирующих символьной информацией, существует универсальный аппарат на базе алгебры конечных предикатов (АКП). Он развивается свыше полувека и за это время показал свою эффективность в теории искусственного интеллекта [3, 4], значительная часть задач которого сводится к иден-

тификации его структур [5-8]. Применение аппарата алгебры конечных предикатов способствовало развитию теории компараторной идентификации [9-12] — разновидности косвенной идентификации, применяемой к объектам и процессам, выходные сигналы которых недоступны для прямых измерений. Такими являются практически все функции естественного интеллекта и многие функции искусственного интеллекта. Аналогично реализуется средствами АКП и обработка цифровой информации вычислительными системами, преобразующими входную информацию в соответствующий выход. И человеческий интеллект, и цифровые вычислительные системы работают с конечными наборами символьной информации различной размерности. Авторы [1]: указывают: «Какие структуры и функции человеческого интеллекта должна изучать теория интеллекта? Очевидно, те и только те, которые, в принципе, доступны интеллекту машинному. Машинный же интеллект, то есть цифровая вычислительная машина, может действовать только механически, он способен воспроизводить лишь детерминированные, дискретные и конечные информационные процессы. *Детерминированные процессы* — это процессы с однозначным исходом, в них отсутствует фактор случайности. *Дискретные процессы* — это процессы, в которых информация имеет вид отдельных порций или квантов — цифр, букв, слов, формул и т.д., в них отсутствует фактор непрерывности. *Конечные процессы* — это такие процессы, в которых может участвовать лишь конечное число единиц информации, в них отсутствует фактор бесконечности. Таким образом, теория интеллекта представляет собой науку о математическом описании детерминированных, дискретных и конечных интеллектуальных процессов, воспроизводимых человеческим разумом, и структур, обеспечивающих реализацию таких процессов, которая ориентирована на совершенствование цифровой вычислительной техники и ее практическое использование».

Краткое описание вышеназванных интеллектуальных средств и некоторые возможности их применения представлены в настоящем обзоре.

2 Алфавитные операторы и алгебра конечных предикатов

Для моделирования переработки информации классический аппарат алфавитных операторов подходит почти без изменений; особенностей две:

1) область определения алфавитных операторов бесконечномерна;

2) входной и выходной языки алфавитного оператора могут содержать слова только одинаковой длины.

Введение в определение алфавитного оператора требования конечномерности приводит к понятию конечного алфавитного оператора [1]. Это понятие расширяет теорию: во-первых, оно соответствует общему свойству всех моделей, с которыми оперирует человек — свойству конечномерности (конечной разрядности), во-вторых, теория конечных алфавитных операторов и основанная на них алгебра конечных предикатов удобнее своих бесконечномерных аналогов в применении к области информационных систем.

Расширение понятия конечного алфавитного оператора на случай слов различной длины во входном и выходном языках существенно усложнило бы математический язык для записи таких операторов. Алгебра конечных предикатов, разработанная Ю.П. Шабановым-Кушнаренко и его соавторами, преодолевает это затруднение.

Алгебра конечных предикатов. Для формального описания систем естественного и искусственного интеллекта нужен математический аппарат, который позволил бы в удобной форме записать любой конечный алфавитный оператор. Из этих соображений была разработана концепция конечных предикатов.

Определение [1]. Пусть A — конечный алфавит, состоящий из k букв $a_1, ..., a_k$; Σ — множество, состоящее из двух элементов, обозначаемых символами $0, 1$ и называемых соответственно «ложью» и «истиной». Переменную, заданную на множестве A, будем называть буквенной; переменную, заданную на множестве Σ, — логической. Конечным n-местным предикатом над алфавитом A называется любая функция $f(x_1, ..., x_n) = t$ от n буквенных аргументов $x_1, ..., x_n$, заданных на множестве A^n, принимающая логические значения t.

Как видно из определения, в отличие от значений переменных конечных алфавитных операторов, которые являются словами, у соответствующих этим операторам конечных предикатов аргументы имеют символьные значения $a_1, ..., a_k$. Переход к буквенным переменным позволяет разрабатывать удобный математический аппарат для описания различных интеллектуальных систем.

Введение конечных предикатов дает возможность представления не только однозначных конечных алфавитных операторов, но и многозначных операторов [13]. Практика моделирования систем искусственного интеллекта показала, что многозначные алфавитные операторы удобны для математического описания высказываний и других объектов теории интеллекта. Однозначным же алфавитным операторам отводится роль

средства математического описания деятельности интеллекта.

Следующим шагом развития математического аппарата является введение алгебры конечных предикатов (АКП, [1]): «Каждая алгебра конечных предикатов полностью характеризуется алфавитом букв A, состоящим из k символов $a_1, ..., a_k$, и алфавитом переменных B, состоящим из n символов $x_1, ..., x_n$. Средствами алгебры конечных предикатов с алфавитом букв A и алфавитом переменных B может быть записан любой n-местный k-ичный предикат $f(x_1, ..., x_n)$, заданный над алфавитом A».

Чтобы не создавать модификаций АКП, отличающихся алфавитами букв и переменных для каждой конкретной задачи, в [13] была введена универсальная АКП. Эта алгебра имеет алфавит букв $A = \{a_1, ..., a_{x_0}\}$ и алфавиты переменных $B_1 = \{\xi_{11}, ..., \xi_{1\nu_1}\}, \ldots, B_\pi = \{\xi_{\pi 1}, ..., \xi_{\pi\nu_\pi}\}$. Порядок π универсальной алгебры, количества букв и переменных $x_0, \nu_1, ..., \nu_\pi$ в ее алфавитах всегда остаются неопределенными.

Затем вводятся правила построения формул АКП. Формулы строятся из следующих символов: букв $a_1, a_2, ..., a_k$, переменных $x_1, x_2, ..., x_n$, знаков дизъюнкции $\vee$ и конъюнкции $\wedge$, открывающей и закрывающей скобок, логических констант 0 и 1.

Кроме обычных логических операций, в АКП используется операция узнавания буквы [14]:

$$x_i^a = \begin{cases} 1, \text{ если } x_i = a, \\ 0, \text{ если } x_i \neq a. \end{cases}$$

Алгебра конечных предикатов является полной, т.е. ее средствами можно описывать любые конечные отношения [13]. Однако интеллект — это не только конечные отношения, но и действия над ними. Аппаратом второй ступени является алгебра предикатных операций [14]. Язык алгебры предикатных операций также универсален, причем он пригоден для выражения действий над отношениями. Так, между конечными предикатами и конечными отношениями стандартным образом устанавливается биекция: если $R(x_1, x_2, ..., x_n)$ — некоторое n-местное отношение, заданное на декартовом произведении $A_1 \times A_2 \times \cdots \times A_n$ некоторых алфавитных множеств $A_1, A_2, \ldots, A_n$, то ему сопоставляется предикат (характеристическая функция)

$$f(x_1, ..., x_n) = \begin{cases} 1, \text{ если } (x_1, ..., x_n) \in R, \\ 0, \text{ если } (x_1, ..., x_n) \notin R. \end{cases}$$

Эта конструкция позволяет применить формальный аппарат конечных предикатов для описания конечных отношений, которые принадле-

жат к наиболее общим видам связей, применяющихся в математике и различных приложениях.

3 Некоторые приложения АКП

Очевидная область применения АКП — описание понятий и структур конечной математики. Многие логические и теоретико-множественные понятия используются при построении интеллектуальных систем, а математическое описание структур конечной математики на языке алгебры конечных предикатов создает теоретический фундамент для построения информационных систем с искусственным интеллектом [3, 4]. Но средства формульной записи конечных отношений и действий над ними, минимизации формул алгебры конечных предикатов, введение универсальной алгебры делают рассмотренный аппарат удобным формализмом для процессных структур (под этим термином понимают процессные знания, например, представление процессов, записанных в логфайлах интеллектуальной системы [23]).

Одной из важных возможностей использования аппарата конечных предикатов становится декомпозиции уравнений алгебры конечных предикатов [16, 17], т.е. замены одного сложного уравнения эквивалентной ему системой более простых уравнений. Она предназначена для регуляризации решения уравнений АКП, а также упрощения и сокращения записи уравнений этой алгебры.

Методы решения уравнений АКП и минимизации формул, аналогичные методам алгебры логики, разрабатываются в [17–20]. Метод минимизации уравнений АКП предложен в [13]. После создания математических моделей интеллектуальных функций обычно требуется реализовать их алгоритмически или аппаратно. С этой целью разработаны методы построения переключательных цепей, позволяющих выполнить схемную реализацию конечных предикатов [13]. Например, дизъюнктивным и конъюнктивным нормальным формам предикатов соответствуют трехступенчатые переключательные цепи. Первая ступень таких цепей образуется из элементов узнавания букв. В цепях, построенных по дизъюнктивным нормальным формам, вторая ступень образуется из элементов совпадения, а третья — из элементов разделения. В цепях, построенных по конъюнктивным нормальным формам, вторая ступень образуется из элементов разделения, а третья — из элементов совпадения.

Переключательные цепи со многими выходами можно применить для построения устройств, реализующих конечные алфавитные операторы. Такие цепи существенно отличаются от комбинационных схем,

применяемых в современных цифровых микросхемах. Комбинационные схемы строятся по формулам алгебры логики из элементов совпадения и разделения (иногда также и из инверторов и блоков других видов). В комбинационных схемах входная и выходная информация имеет вид двоичных кодов, а в переключательных цепях — представлена в форме слов, составленных из букв произвольного конечного алфавита. При использовании переключательных цепей отпадает необходимость в кодировании входной и декодировании выходной информации, что неизбежно при применении комбинационных схем. Кроме того, существуют методы построения обратимых переключательных цепей для реализации произвольных отношений. Еще одно направление развития аппарата конечных предикатов, которое стало самостоятельной областью с развитой теорией и практическими приложениями — это компараторная идентификация. Как говорилось выше, в отличие от классической идентификации объекта по известным сигналам на его входах и выходах, принципиальная особенность компараторной идентификации заключается в недоступности для прямого измерения выходных сигналов идентифицируемого объекта. Классический пример компараторной идентификации, с которого и началось ее развитие — моделирование цветового зрения человека. На входе этого объекта — световые излучения, сигналы физически измеримые. Но на выходе — цвета, являющиеся субъективными ощущениями. Даже если допустить физиологические эксперименты с измерением электрических потенциалов в соответствующих цветовым ощущениям участках головного мозга, в результате мы не получим цвета, которые, по сути, являются «вещью в себе».

Примеры технических объектов, входные физические параметры которых измеримы, а параметры выхода (например, психологические или качественные) для прямого измерения недоступны, довольно многочисленны. К подобным объектам классическая идентификация неприменима, информация об их выходных сигналах может быть только косвенной, качественной и т.п. Компараторная идентификация основана на использовании информации о результатах попарного сравнения реакции на выходные сигналы. Например, на входе предлагается два текста на естественном языке, а на выходе — ответ человека, носителя смысла заданных текстов, об идентичности или неидентичности последних.

На первый взгляд, такой информации недостаточно для построения полной модели объекта. Однако в теории компараторной идентификации устанавливается, что в достаточно широких условиях результат идентификации может быть получен с точностью до изоморфизма [10–12].

Компараторная идентификация имеет ряд специфических отличий от прямой идентификации объектов. В отличие от прямой идентификации, она распадается на две самостоятельные задачи — структурную и параметрическую идентификации [11]. В ходе структурной идентификации определяется общий вид модели объекта, а параметрическая находит численные параметры гипотетической модели.

Практическое моделирование интеллектуальных функций с помощью АКП приводит к системам логических уравнений, описывающих свойства объектов или процессов. Эти системы уравнений затем можно представить программно или аппаратно. Попытки моделировать все более сложные объекты вели к бóльшим системам логических уравнений. Некоторые задачи, например, семантический анализ текстов естественного языка или перевод текстов с одного языка на другой, позволяют разбивать общую задачу на ряд подзадач и решать их независимо друг от друга. Объединение полученных моделей порождает системы уравнений такого объема, который не позволяет их решать программно на компьютерах последовательного действия за приемлемое время. С другой стороны, реальные задачи зачастую критичны к времени вычисления — как, например, семантический анализ текстов или автоматический перевод. В последнее время решение этой проблемы идет по двум направлениям [21]. Первое — упрощение задачи и формализация только самых важных свойств объекта, в результате чего получается увеличение быстродействия и снижение качества модели. Второе направление — построение полных адекватных моделей и поиск путей более эффективного их использования.

4 Логические сети

В пределах теории конечных предикатов существует достаточно новое направление, открывающее возможность параллельного аппаратного решения сложных задач, связанных с обработкой символьной информации. Теория конечных предикатов имеет некоторые результаты по декомпозиции предикатов, т.е. взаимно однозначного преобразования предикатов одной размерности в предикаты меньшей размерности. Основная идея перехода от последовательного алгоритмического вычисления к параллельному основана на процедуре бинаризации системы предикатов, моделирующей заданный объект, т.е. преобразования системы предикатов произвольной конечной размерности, в систему бинарных предикатов. Графическое представление системы бинарных предикатов называется логической сетью [22, 23]. Логическая сеть m-арного пре-

диката состоит из полюсов и ветвей. Каждому полюсу соответствует своя предметная переменная x_i с областью определения A_i $(i = 1, ..., m)$. Ветви соединяют полюсы, точнее говоря, логическая сеть отыскивает решения уравнения:

$$K(x_1, ..., x_m) = 1,$$

при ограничениях, накладываемых на области изменения переменных $x_i \in P_i \subseteq A_i$ $(i = 1, ..., m)$ [23]. Построению сети, реализующей предикат K, предшествует бинаризация предиката, т.е. представление его в виде

$$K(x_1, ..., x_m) = \bigwedge_{1 \le i \ne j \le m} K_{ij}(x_i, x_j).$$

При этом предикат K может быть представлен или одним предикатом достаточно большой размерности, или эквивалентной системой предикатов [23]. Решение системы уравнений логической сетью осуществляется по тактам. В течение каждого такта одновременно вычисляются все бинарные предикаты сети. На первом такте изменения происходят только в узлах (переменных), смежных с теми, в которых заданы начальные условия. На втором такте — в узлах, смежных с измененными на первом такте и т.д.

Подводя итог этого раздела, выделим основные особенности алгебры конечных предикатов с позиций применимости данного аппарата в сфере моделирования дискретных процессов обработки ресурсов, а также интеллектуального анализа процессов:

— возможность практического моделирования интеллектуальных функций с помощью аппарата конечных предикатов реализуется путем построения системы логических уравнений, описывающих свойства объектов или процессов;

— при решении сложных задач выполняется их декомпозиция и, в конечном итоге построение системы логических уравнений;

— система алгебры предикатов может быть преобразована в логическую сеть на основе бинаризации для перехода к параллельной обработке, что в принципе позволяет использовать возможности современных мультипроцессорных систем;

— ключевое преимущество логических сетей заключается в определении полного набора свойств исследуемого объекта на основе ограниченного входного набора признаков.

5 Моделирование гибких процессов преобразования ресурсов

Обсудим структуризацию и варианты подходов к представлению дискретных процессов преобразования ресурсов [24]. Такие процессы можно выделить для широкого спектра прикладных областей — от сфер программирования (SCRUM и аналогичные технологии, [25, 26]) и искусственного интеллекта (Semantic Web, ChatGPT, [27]) до бизнес-процессов [28, 29].

Ключевая особенность таких процессов, помимо их дискретного характера представляет собой последовательность преобразования ресурсов из одной формы в другую, которая может быть представлена в форме графа, описывающего операции по работе с ресурсами их взаимосвязи — т.е. фактически алгоритм преобразования ресурсов.

5.1 Базовые элементы процесса

Базовое задание процесса основано на его представлении в виде последовательности действий. В базовой модели процесса формально описаны возможные (допустимые) последовательности действий. Однако формальная модель не может быть непосредственно использована при реализации процесса. Для исполнения процесса необходимо создать его экземпляр. На практике создание экземпляра процесса связано с разработкой специализированного программного обеспечения либо конфигурированием подходящей программной платформы — т.е. формальная модель реализуется на уровне программного обеспечения. Идейно рассматриваемый подход близок к объектно-ориентированному: создается класс, а затем — экземпляр класса.

Исполняемый экземпляр процесса может содержать не все включенные в модель последовательности действий, а только пригодные для текущей предметной области (например, с учетом специфики работы конкретной организации либо группы людей, перечня решаемых задач, ограничений внешней среды и т.п.). Выполнение определенного действия для экземпляра процесса означает, что работа, представленная в модели в виде действия, должна выполняться в физическом мире.

Расширенное определение процесса включает перечень исполнителей всех действий процесса. В общем случае указанные исполнители встроены в организационную структуру некоторого коллектива, фирмы, предприятия, входя в состав подразделений (групп) и осуществляя необходимые в указанных подразделениях роли. Роль определяет перечень функциональных обязанностей исполнителей (решаемых задач,

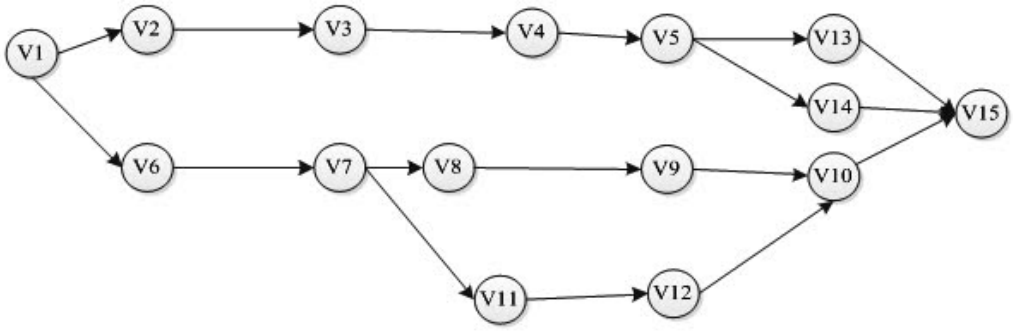


Рис. 1: Пример модели гибкого процесса.

выполняемых операций). Для построения модели процесса преобразования ресурсов традиционно используется аппарат сетей Петри [30] и его модификация WF Net [31]. Однако данный аппарат имеет ряд недостатков при моделировании гибких процессов [32].

5.2 Настраиваемая модель гибкого процесса

Гибкий процесс объединяет в одной модели ряд традиционных, жестко заданных процессов, предоставляет широкий выбор вариантов реализации в зависимости от статических и динамических особенностей предметной области [33–35]. Структура гибких процессов может изменяться вследствие воздействия следующих основных факторов:

скрытые неформализованные знания о выполнении процесса, влияющие на последовательность его активностей;

опыт исполнителей процесса, приводящий к изменению внутренней структуры активностей и, следовательно, изменяющий их результат;

порядок взаимодействия (часто неформальный) исполнителей — людей либо организаций при выполнении процесса;

территориальная распределенность процесса, влияющая на порядок взаимодействия между его составляющими.

Основная цель построения модели гибкого процесса заключается в формализации общего решения, которое в дальнейшем может быть многократно использовано для близких предметных областей путем адаптации. Указанная адаптация выполняется на основе правил настройки (конфигурирования) [36, 37].

Реализация того или иного варианта выполнения процесса обычно осуществляется путем интерпретации конструкции выбора во время выполнения, т.е. проверяется выполнение предопределенного условия с учетом уже выполнившихся операций (произошедших событий).

В то же время часть конструкций выбора, существующих в моде-

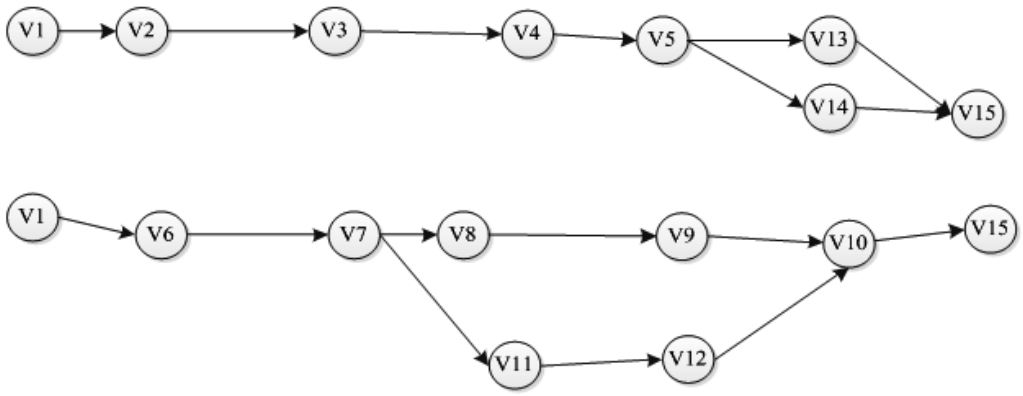


Рис. 2: Сценарии выполнения гибкого процесса.

ли, можно отбросить на этапе конфигурирования, сохранив при этом необходимую функциональность процесса. Следовательно, при конфигурировании выполняется ограничение возможного поведения процесса, а при выполнении — выбор одного из доступных вариантов. Поэтому модель процесса должна обеспечивать обе возможности, хотя провести точную границу между двумя вариантами выбора иногда затруднительно.

Модель процесса в общем случае может быть представлена в виде графа $G = (V, E)$, вершины $Vi \in V$ которого отображают состояния процесса, а дуги $ej \in E$ — переходы между этими состояниями. Каждый переход отражает выполнение некоторого действия процесса (возникновение события для процесса). Выбор действий процесса отображается в модели множественными дугами из одной вершины (рис. 1); в этом иллюстративном примере выполнение процесса начинается с вершины $V1$ и заканчивается достижением вершины $V15$. Заданная в примере модель содержит два основных сценария выполнения процесса, показанных на рис.2).

При выполнении первого сценария последовательность состояний процесса имеет следующий вид $< V1, V2, V3, V4, V5, V13 \wedge V14, V15 >$, а второго — $< V1, V6, V7, < V8, V9 > \wedge < V11, V12 >, V10, V15 >$. Однако в общем случае в обоих сценариях имеются избыточные для конкретной предметной области состояния, которые отсекаются при конфигурировании модели процесса.

5.3 Конфигурирование модели процесса

При конфигурировании (настройке) модели процесса используются два основных оператора: скрытие и блокирование [35]. Скрытие дуг между состояниями процесса предполагает, что соответствующие им

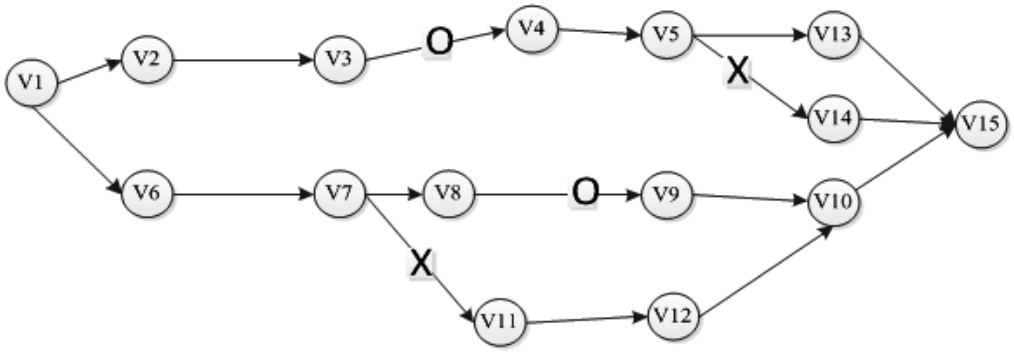


Рис. 3: Конфигурирование модели гибкого процесса.

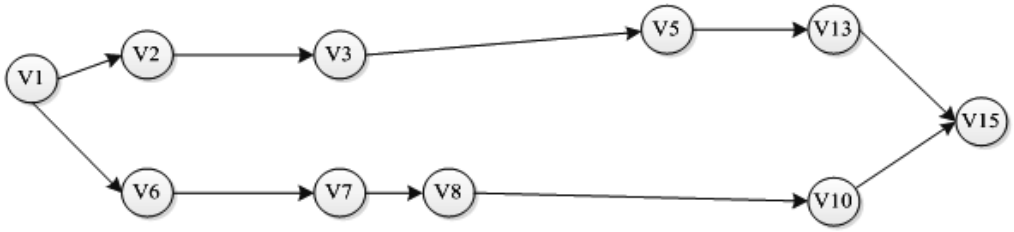


Рис. 4: Конфигурированная модель гибкого процесса.

действия могут выполняться, но их выполнение в модели не отражается. Обычно скрытые действия выполняются по умолчанию.

Блокирование дуги запрещает соответствующее действие либо последовательность действий процесса. Применение операторов блокирования и скрытия в процессе конфигурации приведенного выше примера модели процесса, проиллюстрировано на рис. 3, а результаты конфигурирования модели гибкого процесса представлены на рис. 4. Блокируемые ветви процесса на рисунке отображаются символом **X**, а скрываемые операции — символом **O**.

Таким образом, модель гибкого процесса должна обеспечивать возможности для скрытия либо блокирования последовательностей действий во время конфигурирования.

5.4 Иерархическое представление модели процесса

Графовая модель гибкого процесса может иметь очень сложную структуру, что затрудняет его понимание и не позволяет получить общего представления о наборе возможных сценариев его выполнения. Поэтому для удобной структуризации процесса используется иерархическое представление его модели [38, 39], при построении которого естественно возникают два подхода: условно говоря, разработка сверху–вниз и снизу–вверх. В первом случае первоначально строится обобщенная мо-

дель процесса на самом верхнем уровне. Далее выполняется итеративная процедура детализации модели. На каждом шаге текущая модель процесса разбивается на подпроцессы. Построение модели завершается при достижении уровня отдельных действий процесса — т.е. уровня, на котором выделение подпроцессов уже невозможно.

При моделировании снизу–вверх итеративно выполняется объединение отдельных операций процесса, а также отдельных подпроцессов.

Особая важность иерархического представления для модели гибкого процесса, связана с тем, что такое представление содержит набор допустимых вариантов реализации (сценариев) с учетом условий предметной области. Иерархическое представление позволяет уменьшить сложность модели, упрощает конфигурирование модели за счет отсечения избыточных ветвей, а также иерархия процесса может отражать связанную с процессом организационную структуру, что позволяет эффективно распределить выполнение процесса по исполнителям. В иерархической модели в качестве подпроцессов могут быть использованы уже существующие, разработанные и отлаженные процессы для решения отдельных функциональных задач.

Моделирование иерархической структуры процесса на аппарате сетей Петри WFNet, моделирующем бизнес процессы, связано со значительными трудностями, что и является ключевым недостатком данного аппарата при моделировании гибких процессов. Так, аппарат сетей Петри строит только граф, что оказывается недостаточно полным языком описания. Сложность графов, построенных по лог-файлам ИС, очень высока («спагетти-модель»), что затрудняет анализ такой модели [31, 40]. Формализация модели в виде системы логических уравнений предоставляет бóльшие возможности, например, введение иерархической структуры процесса, упрощающей автоматизированную обработку модели [22].

5.5 Базовые структурные элементы модели процесса

Между действиями процесса возникают довольно сложные взаимосвязи, которые определяют сценарий его исполнения. В частности, для бизнес-процессов в настоящее время выделено несколько десятков шаблонов взаимодействия элементов [29, 41]. При моделировании процессов используется ряд базовых структурных элементов, комбинация которых и обеспечивает широкий набор взаимосвязей между действиями процесса. К таким базовым элементам относятся последовательное выполнение, параллельное выполнение, выбор, цикл. При последовательном выполнении результаты первого действия используются при выполне-

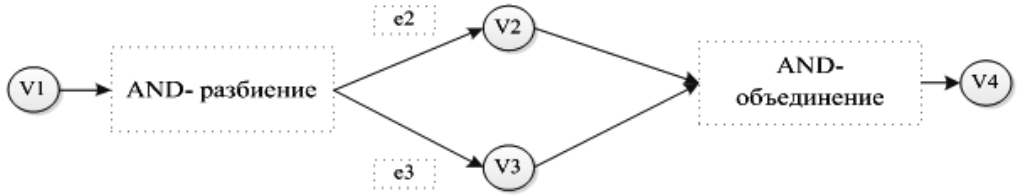


Рис. 5: Параллельное выполнение задач.

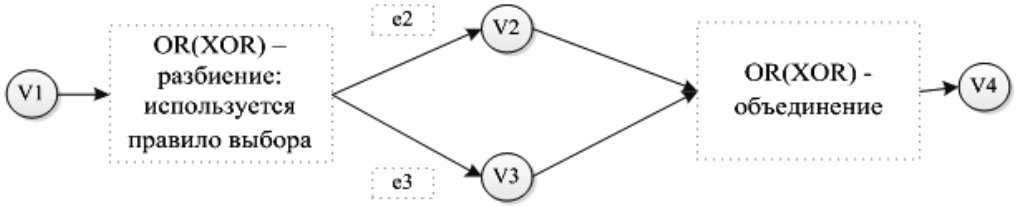


Рис. 6: Реализация выбора.

нии второго. При параллельном выполнении одновременно может выполняться более чем одна задача. Между предшествующим действием процесса и параллельно выполняющимися задачами существует AND-разбиение, а между параллельными задачами и последующим действием — AND-объединение (рис. 5). Оператор AND — развилка, условием или особенностью которой является одновременное выполнение двух и более действий; модель процесса, состоящая из действий и событий (узлы и дуги графа), показана на рис. 5.

Как видно из рис. 1.5, при переходе из состояния $V1$, осуществляется AND-разбиение, после чего выполняются параллельно действия $e2$ и $e3$, что приводит к возникновению состояний $V2$ и $V3$, после чего выполняется AND-объединение и процесс переходит в состояние $V4$.

Сравнивая последовательное и параллельное выполнение, можно отметить, что последовательное выполнение задач фактически является переходом от параллельного при задании соответствующего ограничения, которое может быть вызвано физическими (материальными) причинами. Например, при выполнении операций вручную одним исполнителем организовать параллельное выполнение задач невозможно.

Конструкция выбора реализуется через осуществление одной из нескольких возможных задач (операций). Соответственно, после предшествующего выбору состояния процесса выполняется OR(XOR)-разбиение, а после реализации выбора — OR(XOR)-объединение (рис.6)

Как показано на рис. 6, выбор сводится к выполнению одной из возможных альтернатив $V2$ и $V3$. Однако в модели процесса такой выбор обычно рассматривается как недетерминированный по трем причинам:

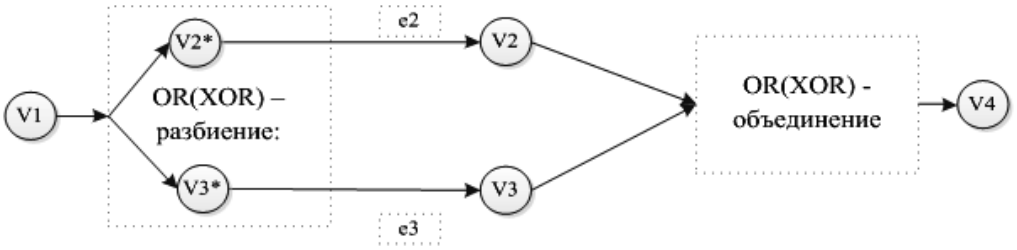


Рис. 7: Детализация разбиения при выборе — предварительные условия.

— обоснование выбора требует усложнения модели путем ее дополнения характеристиками данных и/или исполнителей;

— конкретный выбор часто зависит от текущих характеристик предметной области, поэтому их использование в модели сделали бы ее более специализированной и уменьшили общность;

— при моделировании процесса выбор той или иной ветви в каждом конкретном случае не является определяющим, поскольку при оценке модели необходимо проверить достижимость конечного состояния процесса для всех возможных выборов.

При необходимости правило выбора может быть представлено в виде двух дополнительных состояний $V2^*$ и $V3^*$, достижение каждого из которых является необходимым условием для соответствующего выбора (рис. 7) [42].

Последний из базовых структурных элементов — цикл — отражает многократное повторение последовательности действий процесса. Проверка выхода из цикла, повторения цикла реализуется через OR-разбиение, аналогично представленной выше схеме выбора.

5.6 Особенности модели гибкого процесса

В целом модель гибкого процесса обладает следующими характеристиками:

— является обобщающей, объединяет множество вариантов его поведения, охватывая экспертный опыт для близких, но отличающихся предметных областей;

— основана на использовании базовых структурных элементов, отражающих типовые варианты взаимодействия операций процесса: последовательное, параллельное выполнение, цикл, выбор(ветвление).

Преимущество практического использования состоит в упрощенном конфигурировании путем отбрасывания избыточных для конкретной предметной области вариантов выполнения процесса.

Таким образом, использование гибкой процессной модели значительно облегчает настройку процесса с учетом особенностей предметной области.

Общая оценка такой модели может быть выполнена с учетом ряда основных и дополнительных критериев [43]. К основным, по мнению авторов относятся:

1) наличие альтернативных сценариев развития процесса, отражающих специфику предметной области;

2) возможность построения иерархии уровней детализации модели, облегчающих ее понимание, а также позволяющих интегрировать в модель дополнительные атрибуты (например, организационные взаимосвязи между исполнителями процесса, структуру обрабатываемых данных и т.п.);

3) наличие дополнительных функциональных возможностей, обеспечивающих расширенное применение модели.

К дополнительным критериям относятся:

4) возможность включения в модель различных аспектов процесса (начиная от варьирования последовательности операций процесса и дополняя объектами, которыми оперирует процесс, а также данными и организационной структурой, которая обеспечивает выполнение процесса);

5) допустимость различных форм представления модели, а также ее практическая применимость (схема на бумаге; реализация на существующей коммерческой платформе, индивидуальная разработка; а также доступность модели в интернете);

6) возможность объяснения модели;

7) упрощение практического использования модели, включая специализированную дополнительную информацию (инструкции, руководства) пользователя.

6 Методы интеллектуального анализа процессов

Интеллектуальный анализ процессов (process mining, [26, 44]), предназначен для построения моделей процессов. Исходными данными для анализа являются записи о выполнении процессов, представленные в виде файлов логов событий. Такие логи содержат сведения о последовательности произошедших событий в некоторой информационной системе, как правило, с метками времени. Логи событий могут, напри-

мер, фиксировать выполнение бизнес-процессов, технологических процессов, поведение пользователей в социальных сетях и др. [26]. Основное требование к исходным данным состоит в следующем. Логи должны быть структурированы таким образом, чтобы последовательно во времени фиксировать выделенные группы событий. Каждое из событий фиксирует момент завершения выполнения соответствующего действия процесса. Каждая же из выделенных групп событий отражает выполнение одного экземпляра процесса и, фактически формирует логовый след процесса. Наиболее убедительный подход к интеллектуальному анализу процессов разработан группой под руководством Вила ван дер Аалста и основан на использовании модифицированного аппарата сетей Петри — workflow-сетей [29, 31, 32]. В настоящее время при решении задач интеллектуального анализа процессов используются следующие основные подходы:

вероятностный;

логический;

основанный на workflow-сетях;

эволюционный.

Первый подход основан на подсчете числа появлений одинаковых последовательностей в журнале регистрации событий. При построении модели используются только те последовательности событий, частота появления которых выше заданного исследователем порога. Для оценки слияния либо разделения действий (на основе логики XOR/AND) используются измерители энтропии, количества типов событий, причинной связи и периодичности.

Workflow-сеть предназначена для моделирования последовательности выполнения процесса и отличается от традиционной сети Петри обязательным наличием одной входной и одной выходной позиции. Выполнение задач (действия процесса) моделируются переходами. Взаимосвязи между действиями отображаются с помощью позиций и дуг.

При моделировании потоков работ чаще всего используются AND- и XOR-соединения и разделения, рассмотренные в п. 5.5. При использовании эволюционного подхода так же, как и в workflow-сетях, предполагается, что модель процесса будет иметь одну начальную и одну конечную задачу.

Выполненный анализ базовых исследований в области построения моделей гибких процессов [28, 34, 35, 46, 47] показал, что полная модель такого процесса может быть получена в результате следующих шагов:

выполнение традиционного полного цикла разработки модели гибкого многовариантного процесса;

слияние моделей нескольких «жестких» процессов, которые реализуют идентичную функциональность, но различными способами;

поэтапное дополнение исходной модели процесса новыми возможностями, например, при нахождении неявных знаний (используя опыт сотрудников), их описании и дальнейшем включении в модель;

получение модели с помощью анализа логов, содержащих информацию о нескольких вариантах реализации процесса.

Первый шаг основан на классических подходах к проектированию бизнес-процессов [29, 48] и характеризуется дополнительными затратами на создание различных вариантов реализации процесса.

На втором и третьем шагах могут быть использованы алгоритмы, представленные в работах [35, 49]. Общая идея этой группы алгоритмов состоит в том, что сначала создается базовая модель процесса, которая представляет его типовое поведение (аналог традиционного жестко заданного процесса). Затем полученная модель дополняется возможными вариантами реализации.

Четвертый шаг заключается в предварительном механическом объединении логов для нескольких вариантов реализации процесса и построении модели методами process mining. В этом случае преимущество имеют методы, основанные на эволюционном программировании.

Общий недостаток рассмотренных методов интеллектуального анализа процессов состоит в том, что они базируются на предположении о «плоскостном» характере процесса. Процесс представляется графом, отражающим последовательность (алгоритм) действий, приводящих к требуемому результату. Однако при рассмотрении гибкого процесса нецелесообразно опираться только на «плоский» алгоритм, важно как минимум выполнить декомпозицию подпроцессов и построить их иерархию, а также в перспективе учесть иные его аспекты: обрабатываемые объекты (данные), исполнителей и структуру их взаимодействия.

Традиционные методы интеллектуального анализа процессов требуют доработки применительно к задаче построения модели гибкого процесса. Доработанный метод должен обеспечивать учет дополнительного аспекта процесса — иерархии его действий, а также возможность эффективного отсечения избыточных действий при конфигурировании модели процесса.

7 Синтез систем автоматического управления как гибкий процесс

В концепцию гибкого процесса инженерно-конструкторской природы укладывается почти любой метод синтеза систем автоматического управления (САУ), поскольку даже на стадии работы с готовыми моделями практически каждый из них включает ситуации, рассмотренные в разделе 5, причем во многих процессных фазах. По завершении этого готовый результат в виде определившейся структуры регулятора и конкретных настроек параметров управления может быть принят или отвергнут после тестирования на возмущениях переходных процессов стандартных типов, что носит принципиально компараторный (качественный, см. п.3) характер. Всё это создает значительные трудности для автоматизации практически всех методов синтеза САУ даже при наличии рабочей модели объекта и использовании стандартных блоков регулятора [39, 50].

Рассмотрим как гибкий процесс полиномиальный синтез линейных стационарных САУ пониженного порядка с применением критических корневых диаграмм [51–53], осуществляемый в так называемой частотной области, т.е. после применения преобразования Лапласа к дифференциальным или дифференциально-алгебраическим [54] уравнениям динамических систем. Исходным материалом являются следующие составляющие:

(1) математическая модель объекта (plant) в виде его передаточной функции для одноканального и передаточной матрицы для многоканального случаев $Pl(s) = N_{pl}(s)D_{pl}(s)^{-1}$;

(2) технически допустимые компоновки регулятора (controller): число управляющих воздействий и создающие их стандартные блоки, узлы, где они прилагаются, и др.— т.е. приемлемые передаточные функции (матрицы) регулятора $Con(s) = D_c(s)^{-1}N_c(s)$, в числители которых, как правило, входят настраиваемые параметры управления C; возможно, что для последних будут заданы также некоторые границы значений;

(3) формализация требований к замкнутой системе (т.е. паре объект–регулятор с отрицательной обратной связью) в виде условий на расположение полюсов системы — корней $z_1, \ldots, z_n$ ее характеристического многочлена — в левой комплексной полуплоскости: например, желаемого значения степени устойчивости α, предельной колебательности β (т.е. выполнения неравенств $\max Rez_l \leq -\alpha < 0$ и $\max |Imz_l/Rez_l| < \beta$) и др.; здесь задается вид целевой области и формула α-градуировки, алгебраически выраженной через значения $z_1, \ldots, z_n$ [51, 54].

Таким образом, в качестве начального условия (см. ниже оговорку о предварительной стадии для систем с запаздыванием) задается характеристический многочлен замкнутой системы

$$f_n(s) = \det(N_{pl}(s)N_c(s) + D_{pl}(s)D_c(s));$$

здесь матричная форма и введение определителя det обусловлены несколькими каналами управления, т.е. наличием двух и более управляющих воздействий и контролируемых величин (их число предполагается одинаковым); для одноканальной системы определителя не нужно.

Важно, что многочлены (матрицы) $N_{pl}(s), D_{pl}(s)$ полностью заданы, а многочлены (матрицы) $N_c(s), D_c(s)$ включают в свои коэффициенты параметры регулирования C, причем для одноканальной системы коэффициенты характеристического многочлена зависят от них линейно.

Итак, на входе процесса заданы: число k параметров регулятора, сам свободный вектор C этих параметров и характеристический многочлен $f_n(s)$ степени $n > k$; кроме того, α-градуировка — целевая функция, зависящая от расположения характеристических корней $\{z_l\}$; последнюю нужно минимизировать и убедиться, что ее значения не превышают некоторого отрицательного числа, иногда заданного.

На выходе нужно получить структуру регулятора и значение C^* вектора его параметров, при которых полюса системы минимизируют целевую функцию или удовлетворяют требованиям к ее значению.

Процесс включает в себя несколько стадий.

Предварительная стадия для систем с запаздыванием состоит в выборе аппроксимации Паде для экспоненты в передаточной функции объекта, которая обеспечивала бы удовлетворительное качество модели [50].

Первая стадия: выбор целесообразной структуры регулятора, как правило, состоящей из нескольких стандартных блоков — пропорционального, интегрального, дифференциального, апериодического (П, И, Д, Ап, см. [50]); но стоит отметить и нестандартные возможности — гироскопической стабилизации [55] и др.

Вторая стадия: при небольших k — перечисление критических корневых диаграмм D_j и соответствующих им корневых многочленов $p_\chi(s)$, в коэффициенты которых входят корневые координаты χ; это соответствие жестко определяется корневой диаграммой и α-градуировкой, [52] — или же, при бóльших k, перечисление самих корневых многочленов [53]. Вектор корневых координат χ однозначно задает положение некоторого набора «правых» корней, которые должны лежать на правой границе целевой области [51].

Третья стадия: исследование реализуемости критических диаграмм

— деление многочлена $f_n(s)$ на корневой $p_\chi(s)$ и исследование остатка $r_{\chi,C}(s)$ от деления:

(1) имеет ли решение уравнение $r_{\chi,C}(s) \equiv 0$ как система алгебраических уравнений для коэффициентов остатка; в соответствии с [22], это первый тип предиката, зависящий от вектора C и выражающий необходимое условие реализуемости корневой диаграммы;

(2) нет ли во множестве решений уравнения других корней (помимо тех, которые задаются координатами χ), расположенных правее, чем эти χ-корни — или же самыми правыми оказываются χ-корни; это второй тип предиката, выражающий достаточное условие реализуемости диаграммы;

(3) выполняется ли при таком расположении ограничения для α-градуировки — это третий тип предиката, фактически означающий наличие приемлемых решений при выбранной структуре регулятора.

Пункт (1) допускает преобразование системы уравнений: выражение некоторых корневых координат через другие координаты и параметры управления с последующей подстановкой полученных выражений в оставшиеся уравнения. Если при исходной системе полиномиальных уравнений $r_{\chi,C}(s) \equiv 0$ решение не обнаруживается, то после исключения той или иной корневой координаты оно иногда может быть найдено стандартной вычислительной процедурой (см. [50]; стоит упомянуть и о других сложностях и возможностях преобразования, связанных со спецификой задачи недифференцируемой оптимизации [56]).

Четвертая стадия: сравнить полученные решения (*а*) по достигнутым значениям α-градуировки — чем они меньше, тем выше эффективность регулятора по степени устойчивости и др., и (*б*) по размерам области в пространстве параметров C, где α-градуировка не превосходит значения $\alpha^* + \epsilon$ — чем эта область больше, тем выше робастность регулятора. Если пункты (*а*) и (*б*) не содержат удовлетворительных результатов, нужно вернуться к первой стадии и изменить структуру регулятора или постоянные времени для Ап-регулятора; это повторение выбора регулятора носит не вполне итеративный характер.

Пятая и последняя стадия: сравнение полученных моделей замкнутой системы по импульсной характеристике — отклику замкнутой системы на типичные возмущения — в полном соответствии с понятием компараторной идентификации оптимальной САУ.

Как мы видим, на стадиях с предварительной до третьей создаются характерные для гибких процессов древовидные разветвления [22].

Автоматизация процесса синтеза замкнутой САУ с помощью некоторого программного комплекса предусматривает настройку всей по-

следовательности действий как гибкого процесса в полном согласии с концепцией ван дер Аалста [57].

8 Заключение

В настоящее время область интеллектуального анализа процессов является быстро развивающейся научной областью, захватывающей остроактуальные явления практики [25, 27]. В этой сфере разрабатываются методы моделирования дискретных процессов на основе анализа последовательностей событий, отражающих их выполнение; эти последовательности представлены в виде файлов логов. При этом предполагается наличие лишь приблизительного, часто неформализованного (вербального) описания процесса. Сложность построения адекватной модели процесса на основе анализа логов связана с необходимостью отобразить все возможные варианты поведения процесса на основе исследования следов его выполнения. Особенно остро проблема адекватности модели стоит для гибких процессов, допускающих множество версий их осуществления и адаптируемых к предметной области отсечением избыточных ветвей. Существующие методы процессного моделирования ориентированы в первую очередь на построение традиционного процесса с жестко заданной последовательностью действий. Обычно при построении модели гибкого процесса выполняется либо объединение существующих моделей жестких процессов, либо объединение логов, либо дополнение существующей модели [22, 58, 59]. Однако при моделировании гибкого процесса с адаптируемой структурой необходимо факторизовать избыточность логики его поведения путем иерархизации, что предопределяет важность формализации такого процесса методами process mining, а также расширяет возможности применения в этой области искусственного интеллекта. Подводя итоги всего вышесказанного, можно выделить следующие основные положения: 1) рассмотрение основных особенностей и структурных элементов модели гибкого дискретного процесса преобразования ресурсов показывает важность конфигурирования и иерархического представления процесса; 2) существующие методы интеллектуального анализа процессов ориентированы на построение моделей для процессов жесткой структуры, которые, как правило, не позволяют рассматривать процесс с различной степенью детализации и тем самым затрудняют его восприятие и настройку; 3) аппарат АКП позволяет идентифицировать разнообразные структуры на основе ограниченного входного набора признаков, что обеспечивает возможность выделения структуры гибкого процесса (в том числе

иерархической) на основе анализа логов; 4) модель гибкого процесса, включая его иерархический аспект, расширяет рамки применения искусственного интеллекта на чрезвычайно широкий круг задач — от автоматизации инженерно-технических разработок до обработки текстов на естественном языке.

Список литературы

[1] М.Ф. Бондаренко, Ю.П. Шабанов-Кушнаренко. Об алгебре конечных предикатов // Бионика интеллекта. 2011. № 3 (77). С. 3–13.

[2] Н.В. Голян, Ю.П. Шабанов-Кушнаренко. Предикатные модели неявных связей между процедурами бизнес-процесса // Бионика интеллекта. 2011. № 3 (77). С. 46–49.

[3] М.Ф. Бондаренко , В.А. Чикина. О методе математического описания морфологических отношений и их схемной реализации // Проблемы бионики. 1998. Вып. 48. С. 3–11.

[4] М.Ф. Бондаренко, В.И. Хаханов. Логический ассоциативный мультипроцессор для анализа информации // Бионика интеллекта. 2010. № 2. С. 116–128.

[5] Я.З. Цыпкин. Информационная теория идентификации. М.: Наука. 1995. 336 с.

[6] В.В. Архипов, А.В. Грачева, В.Б. Наумов. Идентификация в сфере искусственного интеллекта и робототехники: сравнительное исследование // Закон. 2023. № 2. С. 96–109.

[7] В.Б. Наумов. Негативные закономерности формирования понятийного аппарата в сфере регулирования Интернета и идентификации // Информационное право. 2018. № 1. С. 32–39.

[8] E. Trikoz, E. Gulyaeva, K. Belyaev. Russian experience of using digital technologies and legal risks of AI // E3S Web of Conferences. 2020. Vol. 224. P. 1–11.

[9] А.С. Соболев, В.А. Доровской, Н.П.Сметюх Метод компараторной идентификации таксономии морских объектов // Вестник Государственного университета морского и речного флота им. адм. С.О. Макарова. 2020. № 5 (12). С. 877–883.

[10] Э.Г. Петров, К.Э. Петров. Компараторная идентификация моделей многофакторного оценивания. М.: Palmarium Academic Publishing 2014. 224 с.

[11] К.Э. Петров, Т.С. Чайникова, И.В. Кобзев, В.Г. Демчук. Компараторная идентификация модели многофакторного оценивания альтернатив с использованием метода бэггинга // Бионика интеллекта. 2019. № 2 (93). С. 21–27.

[12] М.Ф. Бондаренко, С.Ю. Шабанов-Кушнаренко, Ю.П. Шабанов-Кушнаренко. Практические приложения компараторной идентификации линейных конечномерных объектов // Бионика интеллекта. 2009. № 2(71). С. 5–12.

[13] М.Ф. Бондаренко, Ю.П. Шабанов-Кушнаренко. Теория интеллекта. Харьков: изд-во СМИТ, 2007. 576 с.

[14] М.Ф. Бондаренко, З.В. Дударь, Н.Т. Процай и др. Алгебра предикатов и предикатных операций // Радиоэлектроника и информатика. 2004. № 2. С. 56–62.

[15] В.В. Репин, В.Г. Елиферов. Процессный подход к управлению: Моделирование бизнес-процессов. М.: Манн, Иванов и Фербер. 2013. 544 с.

[16] Н.Е. Русакова. О методе расслоения конечного предиката // Бионика интеллекта. 2011. № 3 (77). С. 50–53.

[17] О.И. Синельникова, И.Д. Вечирская. Представление многоместных отношений в виде композиции бинарных отношений // Радиоэлектроника и информатика. 2001. № 3. С. 147–150.

[18] И.Д. Вечирская, В.П. Лоцман. Решение обратной задачи средствами алгебры конечных предикатов // Информатика, математическое моделирование, экономика: Сб. науч. статей по итогам Четвертой Международной научно-практической конференции, г. Смоленск, 23–25 апреля 2014 г. Т. 1. С.28–33.

[19] М.Ф. Бондаренко, Е.В. Журавок, В.А. Чикина. Аппаратный метод решения системы логических уравнений // Проблемы бионики. 1998. Вып. 48. С. 43–47.

[20] Д.Э. Ситников, П.Э. Ситникова. Построение дедуктивных выводов в базах знаний, представленных в виде логических уравнений с дискретными переменными // Вестник ХГПУ. 1999. 51. С. 186–192.

[21] Т.Л. Саати. Принятие решений при зависимостях и обратных связях. Аналитические сети. М.: Ленанд. 2018. 360 с.

[22] М.Н. Рудометкина. Предикатная модель гибкого процесса // Международный журнал прикладных и фундаментальных исследований. 2014. № 10 (2). С. 25–30.

[23] М.Н. Рудометкина, В.Г. Спицын. Модель логической сети с предикатными операциями // Международный журнал прикладных и фундаментальных исследований. 2014. № 10 (3). С. 21–26.

[24] Е.А. Быков, К.А. Аксенов, А.С. Антонова. Аналитический обзор средств и методов для планирования имитационного эксперимента и синтеза мультиагентных процессов преобразования ресурсов // Современные проблемы науки и образования. 2014. № 2. URL: https://science-education.ru/ru/article/view?id=12599 (дата обращения: 14.10.2024)

[25] A. Berti, S.J. Van Zelst, W. van der Aalst. Process mining for python (PM4Py): bridging the gap between process- and data science, arXiv preprint arXiv:1905.06169, 2019.

[26] M. De Leoni , W.M.P. van der Aalst, M. Dees. A general process mining framework for correlating, predicting and clustering dynamic behavior based on event logs // Information Systems. 2016. 56. P. 235–257.

[27] T. Teubner, C.M. Flath, C. Weinhardt, W. van der Aalst & oth. Welcome to the Era of ChatGPT et al.: The Prospects of Large Language Models // Business & Information Systems Engineering. 2023. 2(65). P. 95–101.

[28] W.M.P. van Der Aalst, M. La Rosa, F.M. Santoro. Business process management: Don't forget to improve the process! // Business & Information Systems Engineering. 2016. 1(58). P. 1–6.

[29] W. van der Aalst, A.H.M. ter Hofstede, B. Kiepuszewski. Workflow patterns // Distlibuted and Parallel Databases. 2003. 1(14). P. 5–51.

[30] С.А. Кудж, А.С. Логинова. Моделирование с использованием сетей Петри // Вестник МГТУ МИРЭА. 2015. № 1 (6). С. 10–22.

[31] A.J.M.M. Weijters, W.M.P. van der Aalst. Rediscovering Workflow Models from Event-Based Data using Little Thumb // Integrated Computer-Aided Engineering, 2(10). 2003. P. 151–162.

[32] W. van der Aalst, M. Pesic, H. Schonenberg. Declarative workflows: Balancing between flexibility and support // Computer Science-Research and Development. 2009. 23. P. 99–113.

[33] J. Mendling, I. Weber, W. van der Aalst & oth. Blockchains for business process management-challenges and opportunities // ACM Transactions on Management Information Systems (TMIS). 2018. 1 (9). P. 1–16.

[34] M. La Rosa, W. van Der Aalst, M. Dumas, F.P. Milani. Business process variability modeling: A survey // ACM Computing Surveys (CSUR). 2017. 1(50). P. 1–45.

[35] M.N. Rudometkina, V.G. Spitsyn. Detection of processing model basic elements in intellectual analysis of flexible processes through business process intelligence // IFOST 2014: The 9th International Forum on on Strategic Techology 2014. Cox's Bazar, Bangladesh: IEEE, 2014. P. 97–101.

[36] M.N. Rudometkina, P.A. Kakovkin, A.V. Chekhonadskikh. Flexible process model design // Key Engineering Materials. 2016. V. 685. P. 892–896.

[37] М.Н. Рудометкина. Использование настраиваемых базовых элементов при построении модели гибкого процесса // Научный вестник НГТУ. 2015. № 1 (58). С. 107–120.

[38] М.Н.Рудометкина, А.В. Чехонадских. Разработка программного обеспечения иерархической модели процесса // Фундаментальные исследования. 2016. № 8-1. С. 59–64.

[39] J.C.A.M. Buijs, B.F. van Dongen, W. van der Aalst. On the Role of Fitness, Precision, Generalization and Simplicity in Process Discovery // Proceedings of CoopIS, LNCS. Springer. 2012. P. 305–322.

[40] W.M.P. van der Aalst, H.M.W. Verbeek. Process mining in web services: the web sphere case // Bulletin of the IEEE Computer Society Technical Committee on Data Engineering. 2008. № 3 (31), P. 45–48.

[41] G.F. Luger. Artificial Intelligence: Structures and Strategies for Complex Problem Solving. 5th Edition. Harlow: Addison Wesley. 2005. 912 p.

[42] F. Gottschalk, W.M.P. van der Aalst, M.H. Jansen-Vullers. Merging Event-driven Process Chains // OTM 2008, Part I. CoopIS 2008. Lecture Notes in Computer Science, v. 5331. Berlin, Heidelberg: Springer Verlag. 2008. P. 418–426.

[43] J. Han, J. Pei, H. Tong. Data Mining: Concepts and Techniques, 4th Edition. Morgan Kaufmann Publishers. Elsevier. 2023. 752 p.

[44] W. van der Aalst. Process mining // Communications of the ACM. 2012. № 8 (55). P. 76–83.

[45] H.M.W. Verbeek, J.C.A.M. Buijs, B.F. van Dongen, W.M.P. van der Aalst. XES, XE Same, and ProM 6 // Information Systems Evolution. Lecture Notes in Business Information Processing. V. 72. Berlin: Springer-Verlag. 2010. P. 60–75.

[46] H. Schonenberg, N. Russell, W. van der Aalst & oth. Process Flexibility: A Survey of Contemporary Approaches // Advances in Enterprise Engineering I. CIAO! EOMAS 2008. Lecture Notes in Business Information Processing. V. 10. Springer, Berlin, Heidelberg. P. 16–30. https://doi.org/10.1007/978-3-540-68644-6_2.

[47] M. La Rosa, M. Dumas, R. Uba, R. Dijkman. Business Process Model Merging: An Approach to Business Process Consolidation // ACM Transactions on Software Engineering and Methodology (TOSEM). 2012. № 2(22). P. 1–42.

[48] D. Nikovski. Workflow Trees for Representation and Mining of Implicitly Concurrent Business Processes // ISAS-2, Barcelona, Spain. June 12-16. 2008. P. 30–36.

[49] C.J. Lakhmi, N.M. Martin. Fusion of Neural Networks, Fuzzy Systems and Genetic Algorithms: Industrial Applications. CRC Press, LLC. 1998. 368 p.

[50] А.В. Чехонадских. Алгебраический подход к стабилизации неклассических динамических систем регулятором пониженного порядка // Algebra and model theory 14. Collection of papers. Novosibirsk: NSTU. 2023. С. 10–24.

[51] А.В. Чехонадских. Корневые координаты в синтезе одноканальных систем автоматического управления пониженного порядка // Автометрия. 2015. № 5 (51). С. 69–81.

A.V. Chekhonadskikh. Root coordinates in the design of SISO control systems // Optoelectronics, Instrumentation and Data Processing. 2015. V. 51. P. 485—495.

[52] А.А. Воевода, А.В. Чехонадских. Построение списка критических расположений полюсов систем автоматического управления // Доклады Академии наук высшей школы Российской Федерации. 2014. № 2–3 (23–24). С. 7–18.

[53] A.V. Chekhonadskikh. Some classical number sequences in control system design // Siberian Electronic Mathematical Reports. 2017. V. 14. P. 620–628.

[54] А.В. Чехонадских. Полиномиальный синтез регуляторов пониженного порядка для одноканальных дескрипторных систем // Автометрия. 2023. № 3 (59). С. 101–111.

[55] А.В. Чехонадских. Оптимальный гироскопический стабилизатор многомерной вибрационной системы // Системы анализа и обработки данных. 2022. № 2 (86). С. 81–94.

[56] А.А. Воевода, А.В. Чехонадских. Преодоление недифференцируемости при оптимизационном синтезе систем автоматического управления // Автометрия. 2010. № 5 (46). С. 11–17.

[57] W.M.P. Van der Aalst, M. Bichler, A. Heinzl. Robotic process automation // Business & information systems engineering. 2018. 60. P. 269–272.

[58] A. Rozinat, C.W. Günther, W.M.P. van der Aalst & oth. The Need for a Process Mining Evaluation Framework // Research and Practice. Lecture Notes in Computer Science. V. 4928. Springer. 2008. P. 84–89.

[59] M. Rosemann, W.M.P. van der Aalst. A Configurable Reference Modelling Language // Information Systems. 1 (32). 2007. P. 1–23.

[60] A.V. Chekhonadskikh. Polynomial design of low-order controllers for SISO DAE systems // Optoelectronics, Instrumentation and Data Processing. 2023. V. 59. P. 372–381.

[61] A.A. Voevoda, A.V. Chekhonadskikh. Overcoming Nondifferentiability in Optimization Synthesis of Automatic Control Systems // Optoelectronics, Instrumentation and Data Processing. 2010. V. 46. P. 408–413.

SOME SPECTRA OF SPHERICAL ORDERABILITY OF FINITE GROUPS

A.S. Savin

Novosibirsk State Technical University,
20, K.Marx avenue, Novosibirsk, 630073, Russia
e-mail: savin.2020@stud.nstu.ru

1 Introduction

The fact of linear and circular ordering of groups is known. Next came the generalization n-spherical orderability. In this work, spherical spectra for finitely given groups are considered, since the study of this issue on finite groups is the starting point for studying on arbitrarily given ones. To determine the spherical spectrum, a program was developed that verifies the fulfillment of the axioms.

2 Some spectra of spherical orderability of finite groups

Let $\overline{x}$ be a n-tuple $(x_1, \ldots, x_n)$, σ be a permutation of degree n. Then the tuple $(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ is denoted by $\overline{x_\sigma}$.

Definition [1, 2]. The following generalization of linear and circular orders produces an n-ball, or n-spherical, or n-circular order relation, for $n \geq 2$, which is described by an an n-ary relation K_n satisfying the following conditions:

(nso1) If $\overline{x} \in A^n$ and σ is a transposition on $\{1, 2, \ldots, n\}$, then $\overline{x} \in K_n$ or $\overline{x_\sigma} \in K_n$;

(nso2) If $\overline{x} \in A^n$ and σ is a transposition on $\{1, 2, \ldots, n\}$, then $\overline{x} \in K_n$ or $\overline{x_\sigma} \in K_n$ iff there are distinct indices i and j such that $x_i = x_j$;

(nso3) For any $\overline{x} \in K^n$ and any element $t \in A$, there is an index i such that $(x_1, \ldots, x_{i-1}, t, x_{i+1}, \ldots, x_n) \in K_n$

Definition [1]. A group G is called (agreed) *n-spherically ordered*, or *n-s-ordered*, if G is provided with a *n-spherical* order K_n such that for any

$(x_1, \ldots, x_n) \in K_n$ and any $y \in G$ the tuples $(x_1y, \ldots, x_ny)$ and $(yx_1, \ldots, yx_n)$ belong to K_n.

A group G is called *n-spherically* orderable, or *n-s-orderable*, if G has a *n-spherically* ordered expansion. A group G is called spherically orderable if it is *n-spherically* orderable for some n.

For a group G we define its *spectrum* Sp_{so} of spherical orderability, or spherical spectrum, as follows:

$$Sp_{so}(G) = \{n \in \omega \setminus \{0, 1\} \mid G \text{ is } n\text{-}spherically\ orderable\} \tag{1}$$

A group G is called totally spherically orderable, or totally s-orderable, if G has maximal spectrum of spherical orderability, i.e. $Sp_{so}(G) = \omega \setminus \{0, 1\}$.

A group G is called almost totally spherically orderable, or almost totally sorderable, if $Sp_{so}(G)$ is a cofinite subset of ω.

A group G is (almost) not s-orderable in any way if $Sp_{so}(G)$ is empty (respectively, finite).

If $|G| = n$, then $\omega \setminus n \subseteq Sp_{\text{so}}(G)$.

3 Algorithm

Explanation

1. $\forall n : 2 < n \leq |G|$, G - consider group. Form tuples of n length with pairwise different elements.
2. Collect $\frac{n!}{2}$ permutations with $\varepsilon_\pi = 1$ from all formed tuples.
3. Collect unique $Orb(p)$ obtained by left and right group multiplication, where p is permutation with $\varepsilon_\pi = 1$.
4. Check if in set of $Orb(p)$ contains permutation p_i with $\varepsilon_\pi = -1$ for p_j, where $i \neq j$.
5. If set of $Orb(b)$ contains the above permutation - there is no n-spherical order for G.

A Project structure

```
CMakeLists.txt
spherical_order.hpp
spherical_order.cpp
```

B Source code

SphericalOrderableGroup is a class, that loads Cayley table by *load* method. Method *isOredered*(n) - returns true if group is n-ordered, otherwise false. Method *isOrdered*() - returns map of associated boolean values with n-orderability.

CMakeLists.txt

```
cmake_minimum_required(VERSION 3.27)

project(sperical_order VERSION 1.0 DESCRIPTION "library for spherical order")

set(CMAKE_CXX_STANDARD 20)
set(SOURCE spherical_order.cpp)

find_package(Boost REQUIRED COMPONENTS container)

add_library(${PROJECT_NAME} STATIC ${SOURCE})

target_link_libraries(${PROJECT_NAME} PRIVATE Boost::container)
```

ssspherical_order.hpp

```
#pragma once

#include <string>
#include <map>
#include <vector>
#include <unordered_set>

namespace so
{

using cayle_table_t = std::vector<std::vector<std::string>>;

class SphericalOrderableGroup
{
public:
    explicit SphericalOrderableGroup(const cayle_table_t & cayleyTable);
    SphericalOrderableGroup() = default;
    ~SphericalOrderableGroup() = default;

    void load(const cayle_table_t & cayleyTable) noexcept;
    [[nodiscard]] std::map<std::uint8_t, bool> isOrdered() const noexcept;
    [[nodiscard]] bool isOrdered(std::uint8_t n) const noexcept;
    void printCayleyTable(char separator) const noexcept;

private:
    [[nodiscard]] std::vector<std::vector<std::uint8_t>> leftOrbits(
        const std::vector<uint8_t> & sequence) const noexcept;
    [[nodiscard]] std::vector<std::vector<std::uint8_t>> rightOrbits(
        const std::vector<uint8_t> & sequence) const noexcept;

    std::vector<std::vector<int>> cayleyTable_;
    std::vector<std::uint8_t> group_;
    std::map<std::string, std::uint8_t> association_;
    std::map<std::uint8_t, std::string> inverseAssociation_;
};

} // namespace so
```

spherical_order.cpp

```
#include "spherical_order.hpp"

#include <boost/container_hash/hash.hpp>

#include <future>
#include <unordered_map>

#include <iostream>
#include <bits/ranges_algo.h>

namespace so
```

```
12 {
13
14 namespace
15 {
16
17 [[nodiscard]] constexpr auto binominalCoefficient(const auto n, const auto k)
18 {
19     return std::tgamma(n + 1) / (std::tgamma(k + 1) * std::tgamma(n - k + 1));
20 }
21
22 template <typename T>
23 [[nodiscard]] std::vector<std::vector<T>> generateCombinations(const std::vector<T> &
       source, const std::uint8_t k)
24 {
25     const auto n = source.size();
26
27     std::vector<std::vector<T>> combinations;
28     combinations.reserve(binominalCoefficient(n, k));
29
30     std::vector bitmask (k, true);
31     bitmask.resize(n, false);
32
33     do
34     {
35         std::vector<T> combination;
36         combination.reserve(k);
37
38         for (auto i = 0; i < n; ++i)
39         {
40             if (bitmask[i])
41             {
42                 combination.emplace_back(source[i]);
43             }
44         }
45         combinations.emplace_back(combination);
46     } while (std::prev_permutation(bitmask.begin(), bitmask.end()));
47     return combinations;
48 }
49
50 [[nodiscard]] std::vector<std::vector<std::uint8_t>> findCycles(
51     const std::vector<std::uint8_t> & sequence,
52     const std::vector<std::uint8_t> & permutation) noexcept
53 {
54     std::vector<std::vector<std::uint8_t>> cycles;
55     std::vector visited (sequence.size(), false);
56     std::unordered_map<std::uint8_t, std::uint8_t> valueToIndex;
57
58     for (auto i = 0; i < sequence.size(); ++i)
59     {
60         valueToIndex[sequence[i]] = i;
61     }
62
63     for (auto i = 0; i < sequence.size(); ++i)
64     {
65         if (visited[i])
66         {
67             continue;
68         }
69
70         std::vector<std::uint8_t> cycle;
71         auto start = i;
72
73         while (!visited[start])
74         {
75             cycle.push_back(sequence[start]);
76
77             visited[start] = true;
78             start = valueToIndex[permutation[start]];
79         }
80         cycles.push_back(cycle);
81     }
82     return cycles;
83 }
84
85 [[nodiscard]] bool isEvenPermutation(
86     const std::vector<std::uint8_t> & sequence,
87     const std::vector<std::uint8_t> & permutation) noexcept
88 {
89     return (sequence.size() - findCycles(sequence, permutation).size()) % 2 == 0;
90 }
91
92 [[nodiscard]] bool isOddPermutation(
93     const std::vector<std::uint8_t>& sequence,
```

```
94      const std::vector<std::uint8_t>& permutation) noexcept
95  {
96      return !isEvenPermutation(sequence, permutation);
97  }
98
99  } // unnamed namespace
100
101 SphericalOrderableGroup::SphericalOrderableGroup(const cayle_table_t & cayleyTable)
102 {
103     load(cayleyTable);
104 }
105
106 std::map<std::uint8_t, bool> SphericalOrderableGroup::isOrdered() const noexcept
107 {
108     std::map<std::uint8_t, bool> hasOrder;
109     for (auto i = 3; i <= group_.size(); ++i)
110     {
111         hasOrder[i] = isOrdered(i);
112     }
113     return hasOrder;
114 }
115
116 bool SphericalOrderableGroup::isOrdered(const std::uint8_t n) const noexcept
117 {
118     using vector_hash = boost::hash<std::vector<std::uint8_t>>;
119
120     std::unordered_set<std::vector<std::uint8_t>, vector_hash> orbits;
121     std::unordered_set<std::vector<std::uint8_t>, vector_hash> even_permutations;
122
123     for (const auto & combination : generateCombinations(group_, n))
124     {
125         auto permutation = combination;
126         do
127         {
128             if (isEvenPermutation(combination, permutation))
129             {
130                 even_permutations.emplace(permutation);
131             }
132         }
133         while (std::ranges::next_permutation(permutation.begin(), permutation.end()).
    found);
134
135         for (const auto & current_permutation : even_permutations)
136         {
137             for (const auto & orbit : leftOrbits(current_permutation))
138             {
139                 orbits.emplace(orbit);
140             }
141             for (const auto & orbit : rightOrbits(current_permutation))
142             {
143                 orbits.emplace(orbit);
144             }
145         }
146     }
147
148     std::vector<std::future<bool>> futures;
149     futures.reserve(orbits.size());
150     for (const auto & first_orbit : orbits)
151     {
152         futures.emplace_back(std::async(std::launch::async, [this, &orbits, &
    first_orbit, n]()
153         {
154             return std::ranges::all_of(
155                 orbits.begin(),
156                 orbits.end(),
157                 [this, & first_orbit, n](const auto & second_orbit)
158                 {
159                     if (n == group_.size())
160                     {
161                         if (first_orbit == second_orbit)
162                         {
163                             return true;
164                         }
165                     }
166                     else
167                     {
168                         auto first_sorted = first_orbit;
169                         auto second_sorted = second_orbit;
170
171                         std::sort(first_sorted.begin(), first_sorted.end());
172                         std::sort(second_sorted.begin(), second_sorted.end());
173
174                         if (first_sorted != second_sorted)
```

```
175                         {
176                             return true;
177                         }
178                     }
179 
180                     auto isOdd = isOddPermutation(first_orbit, second_orbit);
181 
182                     if (isOdd)
183                     {
184                         return false;
185                     }
186 
187                     return true;
188                 });
189         }));
190     }
191 
192     for (auto & future : futures)
193     {
194         // if one or more orbit is odd permutation of other orbit - than not ordered
195         if (!future.get())
196         {
197             return false;
198         }
199     }
200 
201     return true;
202 }
203 
204 void SphericalOrderableGroup::printCayleyTable(const char separator) const noexcept
205 {
206     for (const auto & row : cayleyTable_)
207     {
208         for (const auto & item : row)
209         {
210             std::cout << item << separator;
211         }
212         std::cout << std::endl;
213     }
214 }
215 
216 void SphericalOrderableGroup::load(const cayle_table_t & cayleyTable) noexcept
217 {
218     const auto size = cayleyTable.size();
219     const auto & group = cayleyTable.front();
220 
221     for (auto i = 0; i <size; ++i)
222     {
223         association_[group[i]] = i;
224         inverseAssociation_[i] = group[i];
225     }
226 
227     for (auto i = 0; i < size; ++i)
228     {
229         group_.push_back(association_[group[i]]);
230     }
231 
232     cayleyTable_.resize(size);
233     for (auto & row : cayleyTable_)
234     {
235         row.resize(size);
236     }
237 
238     for (auto i = 0; i < cayleyTable.size(); ++i)
239     {
240         for (auto j = 0; j < cayleyTable[i].size(); ++j)
241         {
242             cayleyTable_[i][j] = association_[cayleyTable[i][j]];
243         }
244     }
245 }
246 
247 std::vector<std::vector<std::uint8_t>> SphericalOrderableGroup::leftOrbits(
248     const std::vector<uint8_t> & sequence) const noexcept
249 {
250     std::vector<std::vector<std::uint8_t>> orbits;
251 
252     for (const auto & g : group_)
253     {
254         std::vector<std::uint8_t> orbit;
255         orbit.reserve(sequence.size());
256 
257         for (const auto i : sequence)
```

```
258         {
259             orbit.push_back(cayleyTable_[g][i]);
260         }
261         orbits.push_back(orbit);
262     }
263     return orbits;
264 }
265
266 std::vector<std::vector<std::uint8_t>> SphericalOrderableGroup::rightOrbits(
267     const std::vector<uint8_t> & sequence) const noexcept
268 {
269     std::vector<std::vector<std::uint8_t>> orbits;
270
271     for (const auto & g : group_)
272     {
273         std::vector<std::uint8_t> orbit;
274         orbit.reserve(sequence.size());
275
276         for (const auto i : sequence)
277         {
278             orbit.push_back(cayleyTable_[i][g]);
279         }
280         orbits.push_back(orbit);
281     }
282     return orbits;
283 }
284
285 } // namespace so
```

C Results

The following are Cayley tables to describe the groups. As well as conclusions about the spectrum obtained programmatically, allowing one to declare spherical order.

Cayley table for D_3

$\cdot$	R_0	R_1	R_2	S_0	S_1	S_2
R_0	R_0	R_1	R_2	S_0	S_1	S_2
R_1	R_1	R_2	R_0	S_1	S_2	S_0
R_2	R_2	R_0	R_1	S_2	S_0	S_1
S_0	S_0	S_2	S_1	R_0	R_2	R_1
S_1	S_1	S_0	S_2	R_1	R_0	R_2
S_2	S_2	S_1	S_0	R_2	R_1	R_0

$$Sp_{so}(D_3) = \omega \setminus \{0, 1, 2, 3, 4, 5, 6\}.$$

Cayley table for $GF(2^2)$

$\cdot$	0	1	A	$A+1$
0	0	0	0	0
1	0	1	A	$A+1$
A	0	A	$A+1$	1
$A+1$	0	$A+1$	1	A

$$Sp_{so}(GF(2^2) = \omega \setminus \{0, 1, 2\}.$$

Cayley table for C_7

$\cdot$	1	A	B	C	D	E	F
1	1	A	B	C	D	E	F
A	A	B	C	D	E	F	1
B	B	C	D	E	F	1	A
C	C	D	E	F	1	A	B
D	D	E	F	1	A	B	C
E	E	F	1	A	B	C	D
F	F	1	A	B	C	D	E

$$Sp_{so}(D_7) = \omega \setminus \{0, 1, 2, 4, 6\}.$$

Cayley table for U_8

$\cdot$	3	5	1	7
3	1	7	3	5
5	7	1	5	3
1	3	5	1	7
7	5	3	7	1

$$Sp_{so}(U_8) = \omega \setminus \{0, 1, 2, 3\}.$$

Cayley table for V_4

$\cdot$	1	a	b	ab
1	1	a	b	ab
a	a	1	ab	b
b	b	ab	1	a
ab	ab	b	a	1

$$Sp_{so}(V_4) = \omega \setminus \{0, 1, 2, 3\}.$$

Cayeley table for Q_8

$\cdot$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	$-j$	j	$-i$	i	1	-1
$-k$	$-k$	k	j	$-j$	i	$-i$	-1	1

$$Sp_{so}(Q_8) = \omega \setminus \{0, 1, 2, 3, 4, 5, 6, 7\}.$$

References

[1] S.V. Sudoplatov, Spherically ordered groups // Siberian Electronic Mathematical Reports. — 2024. — T. 21, No 2. (to appear)

[2] B.Sh. Kulpeshov, S.V. Sudoplatov, Spherical orders, properties and countable spectra of their theories // Siberian Electronic Mathematical Reports. — 2023. — Vol. 20, No. 2. — P. 588–599.

ON CONJUGATELY SEPARABILITY OF NILPOTENT SUBGROUPS AND EQUATIONAL DOMAINS: A SURVEY

M. Shahryari

Sultan Qaboos University,
Department of Mathematics, College of Science, Sultan Qaboos University, Muscat, Oman

e-mail: m.ghalehlar@squ.edu.om

A group G is called CSA (conjugately separated abelian) if every maximal abelian subgroup of G is *malnormal*. This means that if H is a maximal abelian subgroup of G and $x \in G \setminus H$ then $H \cap H^x = 1$. The class of CSA groups is quite wide and has very serious roles in the study of residually free groups, universal theory of non-abelian free groups, limit groups, exponential groups and equational domains in algebraic geometry over groups (see [2], [3], [10] , and [11]). Another class of groups which has been studied extensively is the class of CT (commutative transitive) groups. A group is CT if commutativity is a transitive relation on the set of its non-identity elements. Despite this simple definition, the class of CT groups has also a crucial role in the study of residually free groups and so it has a close connection with CSA groups. Every CSA group is CT but the converse is not true. In the presence of residual freeness, both properties are equivalent, a theorem which is proved by B. Baumslag (see [1]).

During the past few decades, there have been many attempts to study these classes and their generalizations. A generalization of CT groups is introduced in [4] to extend the above mentioned theorem of B. Baumslag. Many interesting relations between CSA and CT groups are presented in [7] as well as an excellent account of the previous works.

It seems that the idea of CT and CSA groups is a small part of a very general concept. Suppose $\mathfrak{X}$ is a variety of groups (it can even be a universal class or even an inductive class of groups closed under subgroup). A group G can be called $\mathfrak{X}T$ then, if and only if for any two $\mathfrak{X}$-subgroups $K_1, K_2 \leq G$ the assumption $K_1 \cap K_2 \neq 1$ implies that $\langle K_1, K_2 \rangle$ is also an $\mathfrak{X}$-group. Similarly, we call a group G a $CS\mathfrak{X}$ group if all of its maximal $\mathfrak{X}$-subgroups

are malnormal.

Although it seems that most parts of our work can be developed for many general classes $\mathfrak{X}$, we focus only on the variety of nilpotent groups of class at most k. Let's denote this variety by $\mathfrak{N}_k$. Hence, we call a group NT_k (nilpotency transitive of class k) if for any two $\mathfrak{N}_k$-subgroups K_1 and K_2, the assumption $K_1 \cap K_2 \neq 1$ implies that $\langle K_1, K_2 \rangle$ is nilpotent of class at most k. Also a group G is CSN_k (conjugately separated nilpotent of class k) if and only if every maximal $\mathfrak{N}_k$-subgroup of G is malnormal. The case $k = 1$ obviously coincides with the ordinary CT and CSA groups. It is also easy to see that the property CSA implies CSN_k: this is true as in every non-abelian CSA group, solvable subgroups are abelian, so the maximal $\mathfrak{N}_k$-subgroups are automatically abelian. However, there is no implications of the form $\mathrm{NT}_k \to CT$ or $\mathrm{CSN}_k \to CSA$ (the second implication is not true as not every maximal abelian subgroup is necessarily a maximal $\mathfrak{N}_k$-subgroup).

1 Basic results

The classes of CSN_k and NT_k groups share many similar properties with the classical cases of CSA and CT groups. Some of these properties are listed below and the reader may see [14] for the proofs. The first result generalizes the fact CSA $\to$ CT.

Proposition ([14]). Every CSN_k group is a NT_k group.

The next result shows that non-$\mathfrak{N}_k$-groups with the property NT_k are indecomposable, as in the case of ordinary CT groups.

Proposition ([14]). Suppose G is an NT_k group. If G is decomposable into the direct product of non-trivial subgroups, then it is a $\mathfrak{N}_k$-group.

Another characterization of NT_k- groups is given in the next statement.

Proposition ([14]). Suppose for every pair of distinct maximal $\mathfrak{N}_k$-subgroups H_1 and H_2 we have $H_1 \cap H_2 = 1$. Then G is NT_k. The converse is also true.

Centralizers play a crucial role in the study of ordinary CT and CSA groups. One may see an important link between CSA groups and extension by the centralizers in the fundamental works of Myasnikov and Remeslennikov (see [10] and [11]). In the case of NT_k groups, we need the following

definition. For every element x in a group G we define a subset

$$C_G^k(x) = \{y \in G : \ \langle x, y\rangle \in \mathfrak{N}_k\}.$$

Note that this set contains the centralizer $C_G(x)$ but of course it is not a subgroup in general. However, the situation will be changed in the presence of the property NT_k.

Proposition ([14]). A group G is NT_k if and only if for any non-identity element $x \in G$, the set $C_G^k(x)$ is a $\mathfrak{N}_k$-subgroup. If G is NT_k then for all non-identity element $x \in G$, the subgroup $C_G^k(x)$ is a maximal $\mathfrak{N}_k$-subgroup and every maximal $\mathfrak{N}_k$-subgroup has this form.

As a result we have the following.

Proposition ([14]). Let G be a CSN_k group and H be a subgroup of G. Then H is also CSN_k.

Using the above result, one can see that in any CSN_k group, every solvable subgroup is nilpotent of class at most k. Indeed, if H is such a subgroup, then H itself is a CSN_k group. Suppose n is the derived length of H. Then $H^{(n-1)}$ is a non-trivial normal abelian subgroup of H. Consequently, a maximal $\mathfrak{N}_k$-subgroup $M \leq H$ which contains $H^{(n-1)}$ cannot be malnormal except in the case when $M = H$. Hence H must be nilpotent of class at most k.

More is true for the classes of NT_k and CSN_k groups: they are both axiomatizable by universal sentences. In order to show this, first we need an easy observation from elementary group theory. Suppose X is an arbitrary subset of a group G. By the notation $[X,_k X]$ we denote the set of all simple commutators of length $k+1$ made by the elements of X. A simple argument shows that if $G = \langle X\rangle$ then $\gamma_{k+1}(G) = \langle [X,_k X]^G\rangle$ where $\gamma_{k+1}(G)$ is the $(k+1)$-th term of the lower central series of G. This implies that G is $\mathfrak{N}_k$ provided that for some generating subset X we have $[X,_k X] = 1$.

Now, for any elements x and y in a group G, suppose $Q(x, y)$ is the first order sentence

$$\bigwedge_{x_1,\ldots,x_{k+1}\in\{x,y\}} [x_1, \ldots, x_{k+1}] \approx 1.$$

Note that we prefer to use the notation $\approx$ for equality in the first order language of groups rather the ordinary $=$. By the above observation the sentence $Q(x, y)$ is true in G if and only if $\langle x, y\rangle$ is $\mathfrak{N}_k$.

Using this notation the following sentence

$$\text{(Subgp)} \qquad \forall x \forall y_1, y_2 : ((x \not\approx 1 \wedge Q(x, y_1) \wedge Q(x, y_2)) \to Q(x, y_1^{-1} y_2))$$

says that for all non-identity element x the subset $C_G^k(x)$ is a subgroup and similarly the sentence

$$\text{(Nil)} \ \forall x \forall y_1, \ldots, y_{k+1} : ((x \not\approx 1) \wedge \bigwedge_{i=1}^{k+1} Q(x, y_i)) \to [y_1, \ldots, y_{k+1}] \approx 1)$$

means that $C_G^k(x)$ is nilpotent of class at most k for each non-identity x. Consequently, the property of being NT_k can be translated to the universal first order sentence Subgp + Nil. In the case of CSN_k groups every maximal $\mathfrak{N}_k$-subgroup has the form of $C_G^k(x)$ for some non-trivial element x, so G is CSN_k if and only if it is NT_k and for all non-identity element $x \in G$, the subgroup $C_G^k(x)$ is malnormal. Hence, if we consider the sentence

$$\text{(Mal)} \qquad \forall x, y, z : ((x, y \not\approx 1 \wedge Q(x, y) \wedge Q(x, y^z)) \to Q(x, z))$$

then the property of being CSN_k can be described by the universal sentence Subgp + Nil + Mal. As a result we have

Proposition ([14]). The classes NT_k and CSN_k are universal. Hence any ultraproduct of NT_k groups is NT_k, and any ultraproduct of CSN_k groups is CSN_k.

There is one more elementary property of NT_k groups. It is similar property of CT groups.

Proposition ([14]). Let G be an NT_k group. Then we have the following.

1- If G is torsion-free and $x^m = y^n$ for some elements $x, y \in G$ and some integers m and n, then $\langle x, y \rangle$ is a $\mathfrak{N}_k$-subgroup.
2- If G is torsion-free and $x^n = y^n$ for some elements $x, y \in G$ and some integer n, then $x = y$.
3- If G is not a $\mathfrak{N}_k$-group then $Z(G) = 1$ (and hence G is not nilpotent).

The next result shows that the class CSN_k is also closed under free product if we avoid groups containing involutions. This is exactly the same property as in [11] for CSA groups and to prove it we only need to mimic

the proof in the CSA case.

Proposition ([14]). Suppose A and B are CSN_k groups without elements of order 2. Then the free product $G = A * B$ is also CSN_k.

Examples of CSN_k and NT_k groups, as well as NT_k groups which are not CSN_k are given in [14]. It is known that every finite CSA group is abelian. The structure of finite CT groups are completely determined. In [14], we showed that finite CSN_k groups are nilpotent of class at most k.

Proposition ([14]). Every finite CSN_k group is nilpotent of class at most k.

In [4] it is shown that a CT group is not CSA if and only if it has a non-abelian subgroup which contains a non-trivial abelian normal subgroup. We showed that this can be generalized to the case of NT_k groups.

Theorem ([14]). An NT_k group G is not CSN_k if and only if it has a subgroup G_0 which is not $\mathfrak{N}_k$ and G_0 itself contains a non-trivial $\mathfrak{N}_k$-subgroup which is normal in G_0.

2 A generalization of residually free groups

Fix a finitely generated free element of the variety $\mathfrak{N}_k$, say A. The free product of any non-empty family of copies of A will be called an A-free group. For example, in the most trivial case, the concepts of $\mathbb{Z}$-free group and ordinary free group are equivalent. Note that every A-free group is CSN_k as A is torsion-free. A group G is called residually A-free if for every non-identity element $g \in G$ there exists a homomorphism α from G to some A-free group such that $\alpha(g) \neq 1$. We call G fully residually A-free if and only if for any finite set of non-identity elements $g_1, \ldots, g_n \in G$ there exists a homomorphism α from G to some A-free group such that $\alpha(g_i) \neq 1$ for all $1 \leq i \leq n$.

Proposition ([14]). Let G be a fully residually A-free group. Then G is CSN_k.

B. Baumslag showed in [1] that the properties of being CT and CSA are equivalent if the given group is residually free. We proved a more general form of the above result. A theorem of Jennings (see [8]) says that

every finitely generated torsion-free nilpotent group embeds into $\mathrm{UT}(r, \mathbb{Z})$, the group of unipotent upper triangular integral matrices for some r. This implies that such a group is linear and hence it is equationally noetherian in the sense of [2]. So we can prove:

Theorem ([14]). A group G is fully residually A-free if and only if it is NT_k and residually A-free.

As a results, we have:

Corollary ([14]). Let G be a NT_k group. If there is a finitely generated free element A in the variety $\mathfrak{N}_k$ such that G is residually A-free, then G is CSN_k.

3 Equational domains

We use the same notations as in [2] and [6]. Suppose G is a group and $X = \{x_1, x_2, \ldots, x_n\}$ is a set of variables. Let $\mathbb{F}[X]$ be the free group generated by X and $G[X] = G * \mathbb{F}[X]$ be the free product of G and $\mathbb{F}[X]$. Every element $G[X]$ is a group word in variables $x_1, x_2, \ldots, x_n$ and coefficients from G. If $w(x_1, \ldots, x_n) \in G[X]$, then $w(x_1, \ldots, x_n) \approx 1$ is called a group equation. Suppose H is a group containing G as a distinguished subgroup. Then we call H a G-group. For a given equation $w(x_1, \ldots, x_n) \approx 1$, the set

$$\{(h_1, \ldots, h_n) \in H^n : \ w(h_1, \ldots, h_n) = 1\}$$

is the solution set of the given equation in H. A system of equations with coefficients from G is any set of equations $S \approx 1$, where $S \subseteq G[X]$. The *algebraic set* corresponding to this system is the set of all common solutions of all equations in $S \approx 1$ in H^n. We denote this algebraic set by $V_H(S)$.

A topology can be defined on H^n using the collection of algebraic sets as a sub-base of closed sets: every algebraic set, every finite union of algebraic sets, and every arbitrary intersection of unions of algebraic sets, is closed. This is called the Zariski topology on H^n. This topology is Noetherian if and only if for every $S \subseteq G[X]$, there exists a finite subset $S_0 \subseteq S$ such that $V_H(S) = V_H(S_0)$. In this case, we say that the group H is *G-equationally Noetherian*. If H is G-equationally Noetherian, then every algebraic set can be decomposed uniquely as a finite union of *irreducible* algebraic sets. The group H is called a G-domain if and only if for any n, the union of every two algebraic sets in H^n is again an algebraic set. In this case, every closed set in

the Zariski topology is an algebraic set. There is another definition for the concept of G-domain in terms of *zero divisors*. An element $x \in H$ is called a zero divisor, if there exists a non-identity element $y \in H$ such that for every $g \in G$, we have $[x^g, y] = 1$. In [6], it is proved that a G-group H is G-domain if and only if H does not contain any non-trivial zero divisor. It is not hard to see that H is a G-domain if and only if it satisfies this property: for every non-trivial subgroup $K \leq H$, if G normalizes K (i.e., $G \subseteq N_H(K)$), then the centralizer $C_H(K)$ is trivial. This becomes more interesting in the case when $H = G$. This is called *Diophantine Geometry* over G. In this case we use the phrases "equationally Noetherian" and "domain" instead of "G-equationally Noetherian" and "G-domain", respectively. As a result, G is a domain if and only if for every non-trivial normal subgroup $K \leq G$, we have $C_G(K) = 1$. This picture is more clear because now, one can see that a non-abelian finite group is a domain if and only if it is monolithic i.e., it has a unique minimal normal subgroup. In the case of infinite groups of course, besides monolithic groups, there are many other groups which are domain. As an example, every non-abelian free group is a domain. This can be generalized to CSA groups. Let G be a CSA group and K be a non-trivial normal subgroup of G. Let $C_G(K) \neq 1$ and so, choose a non-trivial element $x \in G$ such that $[x, K] = 1$. As every CSA group is *commutative transitive* (i.e., the binary relation $[a, b] = 1$ is an equivalence relation on the set of non-trivial elements of G), the subgroup K must be abelian. Let M be a maximal abelian subgroup of G containing K. This subgroup M must be malnormal. But, as K is a normal subgroup, for any $g \in G$ we have $K \subseteq M \cap M^g$, which is a contradiction. This shows that every CSA group is a domain (see also [2]). As we mentioned before, our aim is to generalized this result to a wider class of groups. We only consider the case of Diophantine geometry over a group G which is the most interesting case. In order to proceed with, we need to define one more concept. Let $Y \subseteq G^n$ be an arbitrary subset. A normal subgroup of $G[X]$ can be defined as follows:

$$\mathrm{Rad}(Y) = \{w \in G[X] : \ Y \subseteq V_G(w \approx 1)\}.$$

This is the *radical* of Y over G. The quotient group

$$\Gamma(Y) = G[X]/\mathrm{Rad}(Y)$$

is called the *coordinate group* of Y. In the next section, we will need the following *unification theorem* from [2].

Theorem ([2]). Let G be an equationally Noetherian domain and $Y \subseteq G^n$ be an algebraic set. Then the following are equivalent:

1. Y is irreducible

2. $\Gamma(Y)$ is G-equationally Noetherian G-domain

3. $\Gamma(Y)$ is fully residually G as a G-group

4. $\Gamma(Y)$ has the same universal theory as G

It is known that every CSA group is a domain. Here we have a general form. For proofs look at [12].

Theorem ([12]). Suppose G is CSN_k and not nilpotent. Then G is a domain.

As we saw in the previous section, every (fully residually) A-free group is CSN_k. As a result, we have the following.

Corollary ([12]). Let A be a finitely generated free nilpotent group of class k and F be an A-free group. For a positive integer n, let $Y \subseteq F^n$ be an irreducible algebraic set. Then the coordinate group $\Gamma(Y)$ is a CSN_k group.

In [14], another class of groups is introduced which generalizes CSA groups in a new direction. This is the class of all groups, all maximal locally nilpotent subgroups in which are malnormal. It is shown that in such a group, for every pair K_1 and K_2 of locally nilpotent subgroups, $K_1 \cap K_2 \neq 1$ implies that $\langle K_1, K_2 \rangle$ is also locally nilpotent. It is also mentioned that many properties of these new kind of groups coincide with CSN_k groups. We proved that every non-locally nilpotent group of this kind is also a domain.

Theorem ([12]). Let G be a group which is not locally nilpotent. Let every maximal locally nilpotent subgroup of a group G be malnormal. Then G is a domain.

References

[1] B. Baumslag, Residually free groups // Proc. London Math. Soc. **17**(3), 1967, pp. 402-418.

[2] G. Baumslag, A. Myasnikov, V. Remeslennikov, Algebraic geometry over groups: I. Algebraic sets and ideal theory // J. Algebra, **219**, 1999, pp. 16-79.

[3] C. Champetier, V. Guirardel, Limit groups as limits of free groups // Israel Journal of Mathematics, **146**, 2005, pp. 1-75.

[4] L. Ciobanu, B. Fine, G. Rosenberger, Classes of groups generalizing a theorem of Benjamin Baumslag // Communications in Algebra, **44**(2), 2016, pp. 656-667.

[5] D. Costantino, M. Primož, N. Chiara, Groups in which the bounded nilpotency of two generator subgroups is a transitive relation // Beiträge zur Algebra und Geometrie, **48**(1), 2007, pp. 69-82.

[6] E. Daniyarova, A. Myasnikov, V. Remeslennikov, Algebraic geometry over algebraic structures, II: Fundations // J. Math. Sci., 2012, **185 (3)**, pp. 389-416.

[7] B. Fine, A. Gaglione, G. Rosenberger, D. Spellman, On CT and CSA groups and related ideas // J. Group Theory, 2016, **19**, pp. 923-940.

[8] S.A. Jennings, The group ring of a class of infinite nilpotent groups // Canadian J. Math., 1955, **7**, pp. 169-187.

[9] M. Isaacs, Character theory of finite groups. AMS Chelsea Publishing, 1976.

[10] A. Myasnikov, V. Remeslennikov, Groups with exponents I: Fundamentals of the theory and tensor completions // Siberian Mathematical Journal, **35**(5), 1994, pp. 986-996.

[11] A. Myasnikov, V. Remeslennikov, Exponential groups II: Extensions of centralizers and tensor completions of CSA groups // International Journal of Algebra and Computations, **6**(6), 1996, pp. 678-711.

[12] O. Al-Raisi, M. Shahryari, New classes of groups which are equational domains. Submitted.

[13] V. Remeslennikov, ∃-free groups // Siberian Mathematical Journal, **30**(6), 1989, pp. 193-197.

[14] M. Shahryari, On conjugate separability of nilpotent subgroups // Journal of Group Theory, 2024. https://doi.org/10.1515/jgth-2024-0023.

ТЕРНАРНЫЕ ГРУППОИДЫ, ТЕСНО СВЯЗАННЫЕ С ТЕРНАРНЫМИ КВАЗИГРУППАМИ

Н.А. Щучкин

Волгоградский государственный социально-педагогический университет,
400005, г. Волгоград, проспект имени В.И.Ленина, дом 27
e-mail: nikolaj_shchuchkin@mail.ru

1 Введение

Известны многочисленные разновидности группоидов, тесно связанные с квазигруппами (смотри, например, [1]). Одним из ярких обобщений квазигрупп является тернарная квазигруппа. Аналогично как для квазигрупп, мы рассмотрим несколько тернарных группоидов, тесно связанных с тернарными квазигруппами. Такие тернарные группоиды относятся к неассоциативным алгебраическим структурам, на основе которых разрабатываются криптографические алгоритмы [2].

Известно широкое применение квазигрупп в криптографии (см., например, [3]). В работе [4] отмечалось, что квазигруппы могут быть очень полезны для криптографических целей главным образом потому, что легко определить функции кодирования и декодирования, используя операции квазигрупп, и существует огромное количество квазигрупповых операций над заданным конечным множеством. В этой же работе [4] приводится алгоритм преобразования слов в заданном алфавите. Обобщая бинарный случай этого алгоритма на тернарный случай, в работе [5] были рассмотрены применения тернарных квазигрупп для преобразования слов. Аналогичные преобразования с помощью тернарных группоидов, тесно связанных с тернарными квазигруппами, будут приведены ниже.

Исследовательской проблемой является идентификация подходящих квазигрупп для криптографических целей. В работе [6] отмечалось, что с алгебраической точки зрения полиномиально полные квазигруппы подходят для криптографии. Этот класс квазигрупп прост, поэтому он не

позволяет сократить пространство поиска для атаки методом перебора [7]. Наряду с полиномиально полными квазигруппами в криптографии можно использовать и такого же вида тернарные группоиды, тесно связанные с тернарными квазигруппами. В работе [5] были исследованы алгебраические свойства тернарных квазигрупп, такие как полиномиальная полнота, отсутствие нетривиальных конгруэнций. Аналогичные исследования проведем ниже для тернарных группоидов, тесно связанных с тернарными квазигруппами. Эти свойства могут сыграть важную роль при анализе и проектировании криптографических схем на основе тернарных группоидов, тесно связанных с тернарными квазигруппами.

2 Предварительные сведения

Напомним, что множество Q с одной тернарной операцией f называют тернарной квазигруппой, будем обозначать $\langle Q, f\rangle$, если для любых элементов a, b, c из Q уравнения

$$f(x, b, c) = a, f(a, y, c) = b, f(a, b, z) = c, \tag{1}$$

разрешимы однозначно ([8], стр. 6 при $n = 3$).

В силу однозначной разрешимости уравнений (1), на множестве Q имеются еще три тернарные операции u, v, w, заданные по правилам

$$u(a, b, c) = d \Leftrightarrow f(d, b, c) = a; \tag{2}$$

$$v(a, b, c) = d \Leftrightarrow f(a, d, c) = b; \tag{3}$$

$$w(a, b, c) = d \Leftrightarrow f(a, b, d) = c. \tag{4}$$

Операции u, v, w и f связаны тождествами

$$u(f(x, y, z), y, z) = x = f(u(x, y, z), y, z), \tag{5}$$

$$v(x, f(x, y, z), z) = y = f(x, v(x, y, z), z), \tag{6}$$

$$w(x, y, f(x, y, z)) = z = f(x, y, w(x, y, z)). \tag{7}$$

Таким образом, на тернарную квазигруппу $\langle Q, f\rangle$ можно смотреть как на универсальную алгебру $\langle Q, f, u, v, w\rangle$ с набором тождеств (5) – (7).

Рассмотрим различные тернарные группоиды, в которых разрешимы однозначно не все три уравнения из (1), а только два или одно.

Тернарный группоид $\langle Q, f\rangle$, в котором для любых элементов a, b, c из Q разрешимы однозначно первые два (первое и третье, последние два) уравнения из (1), будем называть тернарной (L, M)-квазигруппой

((L,R)-квазигруппой, (M,R)-квазигруппой). На множестве Q имеются еще две тернарные операции u и v (u и w, v и w), заданные по правилам (2) и (3) ((2) и (4), (3) и (4)). Операции u, v и f (u, w и f, v, w и f) связаны тождествами (5) и (6) ((5) и (7), (6) и (7)).

Итак, на тернарную (L,M)-квазигруппу ((L,R)-квазигруппу, (M,R)-квазигруппу) можно смотреть как на универсальную алгебру $\langle Q, f, u, v\rangle$ ($\langle Q, f, u, w\rangle$, $\langle Q, f, v, w\rangle$) с набором тождеств (5) и (6) ((5) и (7), (6) и (7)).

Тернарный группоид $\langle Q, f\rangle$, в котором для любых элементов a, b, c из Q разрешимо однозначно только первое (второе, третье) уравнение из (1), будем называть тернарной L-квазигруппой (M-квазигруппой, R-квазигруппой). На множестве Q имеется еще одна тернарная операция u (v, w), заданная по правилу (2)) ((3), (4). Операции u и f (v и f, w и f) связаны тождествами (5) ((6), (7)).

Таким образом, на тернарную L-квазигруппу (M-квазигруппу, R-квазигруппу) можно смотреть как на универсальную алгебру $\langle Q, f, u\rangle$ ($\langle Q, f, v\rangle$, $\langle Q, f, w\rangle$) с набором тождеств (5) ((6), (7)).

3 Конечные тернарные группоиды, тесно связанные с тернарной квазигруппой

Пусть множество Q конечно, $Q = \{1, 2, \ldots, m\}$. Тогда любой тернарной (L,M)-квазигруппе ((L,R)-квазигруппе, (M,R)-квазигруппе) $\langle Q, f\rangle$ соответствует 3-мерная матрица m-го порядка

$$B = (b_{ijk} | i, j, k = 1, 2, \ldots, m)$$

([9], стр. 5), где $b_{ijk} = f(i, j, k)$, причем, в силу однозначной разрешимости первых двух (первого и третьего, последних двух) уравнений из (1), в строках направления 1 и 2 (1 и 3, 2 и 3) стоят разные элементы из Q. Верно и обратное, любая 3-мерная матрица m-го порядка $B = (b_{ijk} | i, j, k = 1, 2, \ldots, m)$, у которой в строках направления 1 и 2 (1 и 3, 2 и 3) стоят разные элементы из Q, определяет тернарную (L,M)-квазигруппу ((L,R)-квазигруппу, (M,R)-квазигруппу) $\langle Q, f\rangle$, где операция $f(i, j, k) = b_{ijk}$. Итак, между тернарными (L,M)-квазигруппами ((L,R)-квазигруппами, (M,R)-квазигруппами) и 3-мерными матрицами указанного вида имеется взаимно однозначное соответствие.

Построение 3-мерной матрицы B для тернарной (L,M)-квазигруппы ((L,R)-квазигруппы, (M,R)-квазигруппы) $\langle Q, f\rangle$ является аналогом построения таблицы умножения для обычной квазигруппы $\langle Q, \circ\rangle$, эту таб-

лицу называют латинским квадратом. Наилучшую оценку для числа $L(m)$ латинских квадратов порядка m дает формула

$$L(m) = \left((1+\alpha_m)\frac{m}{e^2}\right)^{m^2},$$

где $\alpha_m \to 0$ при $m \to \infty$ (см., например, [10]).

Мы оцениваем число $L(m;3)$ тернарных (L,M)-квазигрупп ((L,R)-квазигрупп, (M,R)-квазигрупп) порядка m:

$$L(m;3) = L(m)^m.$$

Эта оценка показывает, что количество тернарных (L,M)-квазигрупп ((L,R)-квазигрупп, (M,R)-квазигрупп), построенных на конечном множестве, большое. А значит, имеются перспективы использования тернарных (L,M)-квазигрупп ((L,R)-квазигрупп, (M,R)-квазигрупп) для криптографических целей.

Каждая 3-мерная матрица B, построенная для тернарной (L,M)-квазигруппы ((L,R)-квазигруппы, (M,R)-квазигруппы) $\langle Q,f\rangle$, где $Q = \{1,2,\ldots,m\}$, определяет набор из m латинских квадратов на множестве Q с умножением $i \circ_k j = f(i,j,k)$ ($i \circ_j k = f(i,j,k)$, $j \circ_i k = f(i,j,k)$) ($k = 1,2,\ldots,m$). Таким образом, на 3-мерную матрицу B можно смотреть как на упорядоченный набор латинских квадратов в количестве, равном числу элементов множества Q.

Пусть вновь множество Q конечно и $Q = \{1,2,\ldots,m\}$. Тернарной L-квазигруппе (M-квазигруппе, R-квазигруппе) $\langle Q,f\rangle$ также соответствует 3-мерная матрица $B = (b_{ijk}|i,j,k = 1,2,\ldots,m)$ m-го порядка, где $b_{ijk} = f(i,j,k)$, причем, в силу однозначной разрешимости первого (второго, третьего) уравнения из (1), в строках направления 1 (2, 3) стоят разные элементы из Q. Верно и обратное, любая 3-мерная матрица m-го порядка $B = (b_{ijk}|i,j,k = 1,2,\ldots,m)$, у которой в строках направления 1 (2, 3) стоят разные элементы из Q, определяет тернарную L-квазигруппу (M-квазигруппу, R-квазигруппу) $\langle Q,f\rangle$, где $f(i,j,k) = b_{ijk}$. Итак, между тернарными L-квазигруппами (M-квазигруппами, R-квазигруппами) и 3-мерными матрицами указанного вида имеется взаимно однозначное соответствие.

Мы можем вычислить количество $L'(m;3)$ тернарных L-квазигрупп (M-квазигрупп, R-квазигрупп) порядка m:

$$L'(m;3) = m!^{m^2}.$$

Мы имеем большое число тернарных L-квазигрупп (M-квазигрупп, R-квазигрупп), построенных на конечном множестве. А значит, имеются

перспективы использования тернарных L-квазигрупп (M-квазигрупп, R-квазигрупп) в криптографии.

Каждая 3-мерная матрица B, которая построена выше для тернарной L-квазигруппы (M-квазигруппы, R-квазигруппы) $\langle Q, f\rangle$, где $Q = \{1, 2, \ldots, m\}$, определяет набор m квадратных таблиц умножения на множестве Q с операцией $i \circ_k j = f(i, j, k)$ ($i \circ_j k = f(i, j, k)$, $j \circ_i k = f(i, j, k)$) ($k = 1, 2, \ldots, m$). Таким образом, на 3-мерную матрицу B можно смотреть как на упорядоченный набор таблиц умножения левых квазигрупп в количестве, равном числу элементов множества Q.

4 Преобразования слов

Для преобразования слов в заданном алфавите используют квазигруппы [4]. Мы обобщаем преобразования слов из этой работы на тернарный случай, т.е. в работе [5] было указано преобразование слов с помощью тернарных квазигрупп, а здесь будем преобразовывать слова с помощью тернарных группоидов, тесно связанных с тернарными квазигруппами.

Пусть $\langle Q, f\rangle$ – конечная тернарная (L, M)-квазигруппа, где $Q = \{1, \ldots, m\}$. Множество всех слов в алфавите Q обозначим

$$Q^+ = \{x_1 \ldots x_s | x_i \in Q, s \geq 1\}.$$

Для заданной пары элементов a, b из Q, в терминах работы [4] эти элементы назовем лидерами, на множестве Q^+ определим отображение

$$A_{a,b}(x_1 x_2 \ldots x_s) = y_1 y_2 \ldots y_s =$$

$$= \begin{cases} y_1 = f(x_1, a, b), \\ y_2 = f(x_2, y_1, a), \\ y_{i+1} = f(x_{i+1}, y_i, y_{i-1}), i = 2, 3, \ldots, s-1. \end{cases} \tag{8}$$

Теорема 1. *Отображение $A_{a,b}$, построенное по правилу (8), является биективным.*

Доказательство. Пусть $A_{a,b}(x_1 x_2 \ldots x_s) = A_{a,b}(x'_1 x'_2 \ldots x'_s)$. Тогда имеем $f(x_1, a, b) = f(x'_1, a, b)$, откуда, в силу однозначной разрешимости первого уравнения из (1), имеем $x_1 = x'_1$. Далее, из первого равенства следует $f(x_2, y_1, a) = f(x'_2, y_1, a)$, откуда, по той же причине, имеем $x_2 = x'_2$. Наконец, из первого равенства следует $f(x_{i+1}, y_i, y_{i-1}) = f(x'_{i+1}, y_i, y_{i-1})$, откуда, по той же причине, имеем $x_{i+1} = x'_{i+1}$ для всех

$i = 2, 3, \ldots, s-1$. Инъективность отображения $A_{a,b}$ доказана. Пусть теперь $y_1 y_2 \ldots y_s \in Q^+$. В силу разрешимости первого уравнения из (1), найдутся $x_1, x_2, \ldots, x_s \in Q$ такие, что $y_1 = f(x_1, a, b)$, $y_2 = f(x_2, y_1, a)$, $y_{i+1} = f(x_{i+1}, y_i, y_{i-1})$ для всех $i = 2, 3, \ldots, s-1$. Тогда $A_{a,b}(x_1 x_2 \ldots x_s) = y_1 y_2 \ldots y_s$. □

Для конечной тернарной (L, M)-квазигруппы $\langle Q, f\rangle$ на множестве Q^+ можно определить другое отображение

$$B_{a,b}(x_1 x_2 \ldots x_s) = y_1 y_2 \ldots y_s =$$

$$= \begin{cases} y_1 = f(a, x_1, b), \\ y_2 = f(y_1, x_2, a), \\ y_{i+1} = f(y_i, x_{i+1}, y_{i-1}), i = 2, 3, \ldots, s-1. \end{cases} \tag{9}$$

Аналогично теореме 1 доказывается

Теорема 2. *Отображение $B_{a,b}$, построенное по правилу (9), является биективным.*

Пусть теперь $\langle Q, f\rangle$ – конечная тернарная (L, R)-квазигруппа, где $Q = \{1, \ldots, m\}$. Для заданной пары элементов a, b из Q на множестве Q^+ определим отображение $A_{a,b}$ по правилу (8). Как и выше, отображение $A_{a,b}$, построенное по правилу (8), является биективным.

Для конечной тернарной (L, R)-квазигруппы $\langle Q, f\rangle$ на множестве Q^+ можно определить другое отображение

$$C_{a,b}(x_1 x_2 \ldots x_s) = y_1 y_2 \ldots y_s =$$

$$= \begin{cases} y_1 = f(a, b, x_1), \\ y_2 = f(y_1, a, x_2), \\ y_{i+1} = f(y_i, y_{i-1}, x_{i+1}), i = 2, 3, \ldots, s-1. \end{cases} \tag{10}$$

Аналогично теореме 1 доказывается

Теорема 3. *Отображение $C_{a,b}$, построенное по правилу (10), является биективным.*

Пусть теперь $\langle Q, f\rangle$ – конечная тернарная (M, R)-квазигруппа, где $Q = \{1, \ldots, m\}$. Для заданной пары элементов a, b из Q на множестве Q^+ определим отображения $A_{a,b}$ по правилу (8) и $C_{a,b}$ по правилу (10). Как и выше, отображения $A_{a,b}$ и $C_{a,b}$ являются биективными.

Выбираем теперь конечную тернарную L-квазигруппу (M-квазигруппу, R-квазигруппу) $\langle Q, f\rangle$, где вновь $Q = \{1, \ldots, m\}$. Для заданной пары

элементов a, b из Q на множестве Q^+ определим отображение $A_{a,b}$ по правилу (8) ($B_{a,b}$ по правилу (9), $C_{a,b}$ по правилу (10)). Как и выше, отображение $A_{a,b}$ ($B_{a,b}$, $C_{a,b}$) является биективным.

Для той же пары элементов a, b из Q на множестве Q^+ строим еще одно отображение

$$D_{a,b}(y_1y_2\dots y_s) = x_1x_2\dots x_s =$$

$$= \begin{cases} x_1 = u(y_1, a, b), \\ x_2 = u(y_2, y_1, a), \\ x_{i+1} = u(y_{i+1}, y_i, y_{i-1}), i = 2, 3, \dots, s-1. \end{cases} \tag{11}$$

Теорема 4. *Отображение $D_{a,b}$, построенное по правилу (11), является обратным для отображения $A_{a,b}$.*

Доказательство. Для выбранного слова $x_1x_2\dots x_s$ из Q^+ имеем

$$D_{a,b}(A_{a,b}(x_1x_2\dots x_s)) = D_{a,b}(y_1y_2\dots y_s) = x'_1x'_2\dots x'_s,$$

где

$$x'_1 = u(y_1, a, b) = u(f(x_1, a, b), a, b),$$

$$x'_2 = u(y_2, y_1, a) = u(f(x_2, y_1, a), y_1, a),$$

$$x'_{i+1} = u(y_{i+1}, y_i, y_{i-1}) = u(f(x_{i+1}, y_i, y_{i-1}), y_i, y_{i-1}), i = 2, 3, \dots, s-1.$$

Согласно (5), получим $x'_1 = x_1$, $x'_2 = x_2$, $x'_{i+1} = x_{i+1}$ для $i = 2, 3, \dots, s-1$, т.е. имеем равенство $D_{a,b}(F_{a,b}(x_1x_2\dots x_s)) = x_1x_2\dots x_s$. Аналогично доказывается равенство $A_{a,b}(D_{a,b}(y_1y_2\dots y_s)) = y_1y_2\dots y_s$ для любого слова $y_1y_2\dots y_s$ из Q^+. □

Аналогично для отображения $B_{a,b}$ строится обратное отображение $E_{a,b}$ по правилу

$$E_{a,b}(y_1y_2\dots y_s) = x_1x_2\dots x_s =$$

$$= \begin{cases} x_1 = v(a, y_1, b), \\ x_2 = v(y_1, y_2, a), \\ x_{i+1} = v(y_i, y_{i+1}, y_{i-1}), i = 2, 3, \dots, s-1, \end{cases} \tag{12}$$

а для отображения $C_{a,b}$ строится обратное отображение $F_{a,b}$ по правилу

$$F_{a,b}(y_1y_2\dots y_s) = x_1x_2\dots x_s =$$

$$= \begin{cases} x_1 = w(a, b, y_1), \\ x_2 = w(y_1, a, y_2), \\ x_{i+1} = w(y_i, y_{i-1}, y_{i+1}), i = 2, 3, \ldots, s-1. \end{cases} \quad (13)$$

Для преобразования слов с помощью тернарных (L, M)-квазигрупп, (L, R)-квазигрупп, (M, R)-квазигрупп, L-квазигрупп, M-квазигрупп и R-квазигрупп можно использовать композиции отображений вида (8), (9) и (10). Выбираем набор $\langle Q, f_1\rangle$, $\langle Q, f_2\rangle$, ..., $\langle Q, f_t\rangle$ выше указанных тернарных группоидов и упорядоченные пары $(a_1, b_1), (a_2, b_2), \ldots, (a_t, b_t)$ элементов из Q $(t > 1)$. Строим по правилам (8), (9) и (10) отображения $S^1_{a_1,b_1}, S^2_{a_2,b_2}, \ldots, S^t_{a_t,b_t}$, а затем рассматриваем композицию

$$S_{a_1,b_1,a_2,b_2,\ldots,a_t,b_t} = S^1_{a_1,b_1} \circ S^2_{a_2,b_2} \circ \ldots \circ S^t_{a_t,b_t}. \quad (14)$$

Для этих же тернарных группоидов и пар элементов строим соответственно по правилам (11), (12) и (13) отображения $T^1_{a_1,b_1}, T^2_{a_2,b_2}, \ldots, T^t_{a_t,b_t}$, и также рассматриваем композицию $T_{a_t,b_t,\ldots,a_2,b_2,a_1,b_1} = T^t_{a_t,b_t} \circ \ldots \circ T^2_{a_2,b_2} \circ T^1_{a_1,b_1}$. Очевидно, $T_{a_t,b_t,\ldots,a_2,b_2,a_1,b_1}$ — обратное отображение для отображения $S_{a_1,b_1,a_2,b_2,\ldots,a_t,b_t}$.

В криптографии очень важно, чтобы зашифрованное слово можно было расшифровать однозначно. В нашем случае имеем следующий факт.

Теорема 5. *Пусть $\langle Q, f_1\rangle$, $\langle Q, f_2\rangle$, ..., $\langle Q, f_t\rangle$ — набор тернарных группоидов, каждый из которых является одним из шести тернарных группоидов: (L, M)-квазигруппой, (L, R)-квазигруппой, (M, R)-квазигруппой, L-квазигрупп, M-квазигрупп или R-квазигрупп, где множество $Q = \{1, \ldots, m\}$. Для любого слова $y_1y_2 \ldots y_s$ из Q^+ и для любых упорядоченных пар $(a_1, b_1), (a_2, b_2), \ldots, (a_t, b_t)$ элементов из Q существует единственное слово $x_1x_2 \ldots x_s$ из Q^+ такое, что верно равенство*

$$S_{a_1,b_1,a_2,b_2,\ldots,a_t,b_t}(x_1x_2 \ldots x_s) = y_1y_2 \ldots y_s.$$

Доказательство. Существование и единственность слова $x_1x_2 \ldots x_s$ из Q^+ доказывается применением к слову $y_1y_2 \ldots y_s$ из Q^+ преобразования $T_{a_t,b_t,\ldots,a_2,b_2,a_1,b_1}$. □

5 Конгруэнции на тернарных группоидах, тесно связанных с квазигруппами

Любая конгруэнция на тернарной квазигруппе $\langle Q, f, u, v, w\rangle$ (как на универсальной алгебре с набором тождеств (5) – (7)) это отношение эк-

вивалентности, стабильное относительно всех тернарных операций f, u, v и w. Аналогично будем рассматривать и конгруэнции на тернарных группоидах, тесно связанных с квазигруппами. Оказывается, для конечных тернарных группоидах, тесно связанных с квазигруппами, достаточно рассматривать только стабильность отношения эквивалентности относительно операции f. Докажем этот факт сначала для тернарной (L, M)-квазигруппы.

Теорема 6. *Отношение эквивалентности τ на конечной тернарной (L, M)-квазигруппе $\langle Q, f, u, v\rangle$ является конгруэнцией тогда и только тогда, когда τ стабильно относительно операции f.*

Доказательство. Пусть τ стабильно относительно операции f. Для элементов $a, b \in Q$ рассмотрим перестановки $\alpha_{a,b}(x) = f(x, a, b)$, $\beta_{a,b}(x) = f(a, x, b)$ на множестве Q. Согласно тождествам (2), (3) верно $\alpha^{-1}_{a,b}(y) = u(y, a, b)$, $\beta^{-1}_{a,b}(y) = v(a, y, b)$. Так как Q конечно, то найдутся натуральные числа r, s такие, что $\alpha^r_{a,b} = 1 = \beta^s_{a,b}$. Тогда $\alpha^{r-1}_{a,b} = \alpha^{-1}_{a,b}$, $\beta^{s-1}_{a,b} = \beta^{-1}_{a,b}$.

Пусть $a_1 \tau a_2$, $b_1 \tau b_2$, $c_1 \tau c_2$. Индукцией по n легко доказывается, что для любого натурального n верно $\alpha^n_{b_1,c_1}(a_1)\tau\alpha^n_{b_2,c_2}(a_2)$, $\beta^n_{a_1,c_1}(b_1)\tau\beta^n_{a_2,c_2}(b_2)$. Тогда

$$u(a_1, b_1, c_1) = \alpha^{-1}_{b_1,c_1}(a_1) = \alpha^{r-1}_{b_1,c_1}(a_1)\tau\alpha^{r-1}_{b_2,c_2}(a_2) = \alpha^{-1}_{b_2,c_2}(a_2) = u(a_2, b_2, c_2).$$

Аналогично доказывается стабильность отношения τ относительно операции v. □

Такая же теорема аналогично доказывается и для (L, R)-квазигрупп, (M, R)-квазигрупп, L-квазигрупп, M-квазигрупп, R-квазигрупп.

Класс конгруэнции τ обозначим $[a]_\tau$. Все классы конгруэнции тернарной (L, M)-квазигруппы ((L, R)-квазигруппы, (M, R)-квазигруппы) равномощны, так как конгруэнция тернарной (L, M)-квазигруппы ((L, R)-квазигруппы, (M, R)-квазигруппы) является конгруэнцией на каждой квазигруппе, определяемой тернарной операцией, а классы конгруэнции квазигруппы равномощны (см., например, [11], теорема 3.4). В частности, если тернарная (L, M)-квазигруппа ((L, R)-квазигруппа, (M, R)-квазигруппа) конечна, то порядок каждого класса конгруэнции делит ее порядок.

Элемент e тернарного группоида $\langle Q, f\rangle$ назовем левой (средней или правой) единицей, если верно равенство $f(e, e, a) = a$ ($f(e, a, e) = a$ или $f(a, e, e) = a$ соответственно) для любого элемента $a \in Q$. Тогда на тернарной квазигруппе $\langle Q, f, u, v, w\rangle$ верны равенства $f(e, e, e) = e = u(e, e, e) = v(e, e, e) = w(e, e, e)$, т.е. левая, средняя и правая единицы являются идемпотентами для всех тернарных операций f, u, v, w.

Теорема 7. *Если в тернарной (L, M)-квазигруппе $\langle Q, f\rangle$ имеется левая (средняя, правая) единица e, то для любой конгруэнции τ этой тернарной (L, M)-квазигруппы ее класс $[e]_\tau$ является тернарной (L, M)-подквазигруппой, а любой класс $[a]_\tau = f([e]_\tau, e, a) = f(e, [e]_\tau, a)$ ($[a]_\tau = f([e]_\tau, a, e)$, $[a]_\tau = f(a, [e]_\tau, e)$).*

Доказательство. Пусть посылка теоремы верна и $a, b, c \in [e]_\tau$, тогда $a\tau e$, $b\tau e$, $c\tau e$, откуда $f(a, b, c)\ \tau\ f(e, e, e) = e$, $u(a, b, c)\ \tau\ u(e, e, e) = e$, $v(a, b, c)\ \tau\ v(e, e, e) = e$, т.е. $f(a, b, c), u(a, b, c), v(a, b, c) \in [e]_\tau$. Значит, $[e]_\tau$ – тернарная (L, M)-подквазигруппа. Далее, если e – левая единица, то

$$b \in [a]_\tau \Leftrightarrow b\ \tau\ a \Leftrightarrow u(b, e, a)\ \tau\ u(a, e, a) = e \Leftrightarrow$$

$$\Leftrightarrow b = f(u(b, e, a), e, a) \in f([e]_\tau, e, a).$$

$$b \in [a]_\tau \Leftrightarrow b\ \tau\ a \Leftrightarrow v(e, b, a)\ \tau\ v(e, a, a) = e \Leftrightarrow$$

$$\Leftrightarrow b = f(e, v(e, b, a), a) \in f(e, [e]_\tau, a).$$

Если e – средняя единица, то

$$b \in [a]_\tau \Leftrightarrow b\ \tau\ a \Leftrightarrow u(b, a, e)\ \tau\ u(a, a, e) = e \Leftrightarrow$$

$$\Leftrightarrow b = f(u(b, a, e), a, e) \in f([e]_\tau, a, e).$$

Наконец, если e – правая единица, то

$$b \in [a]_\tau \Leftrightarrow b\ \tau\ a \Leftrightarrow v(a, b, e)\ \tau\ v(a, a, e) = e \Leftrightarrow$$

$$\Leftrightarrow b = f(a, v(a, b, e), e) \in f(a, [e]_\tau, e).$$

□

Аналогично доказываются ниже следующие теоремы.

Теорема 8. *Если в тернарной (L, R)-квазигруппе $\langle Q, f\rangle$ имеется средняя (левая, правая) единица e, то для любой конгруэнции τ этой тернарной (L, R)-квазигруппы ее класс $[e]_\tau$ является тернарной (L, R)-подквазигруппой, а любой класс $[a]_\tau = f([e]_\tau, a, e) = f(e, a, [e]_\tau)$ ($[a]_\tau = f([e]_\tau, e, a)$, $[a]_\tau = f(a, e, [e]_\tau)$).*

Теорема 9. *Если в тернарной (M, R)-квазигруппе $\langle Q, f\rangle$ имеется правая (левая, средняя) единица e, то для любой конгруэнции τ этой тернарной (M, R)-квазигруппы ее класс $[e]_\tau$ является тернарной (M, R)-подквазигруппой, а любой класс $[a]_\tau = f(a, [e]_\tau, e) = f(a, e, [e]_\tau)$ ($[a]_\tau = f(e, [e]_\tau, a)$, $[a]_\tau = f(e, a, [e]_\tau)$).*

Теорема 10. *Если в тернарной L-квазигруппе $\langle Q, f\rangle$ имеется левая (средняя) единица e, то для любой конгруэнции τ этой тернарной L-квазигруппы ее класс $[e]_\tau$ является тернарной L-подквазигруппой, а любой класс $[a]_\tau = f([e]_\tau, e, a)$ ($[a]_\tau = f([e]_\tau, a, e)$).*

Теорема 11. *Если в тернарной M-квазигруппе $\langle Q, f\rangle$ имеется левая (правая) единица e, то для любой конгруэнции τ этой тернарной M-квазигруппы ее класс $[e]_\tau$ является тернарной M-подквазигруппой, а любой класс $[a]_\tau = f(e, [e]_\tau, a)$ ($[a]_\tau = f(a, [e]_\tau, e)$).*

Теорема 12. *Если в тернарной R-квазигруппе $\langle Q, f\rangle$ имеется средняя (правая) единица e, то для любой конгруэнции τ этой тернарной R-квазигруппы ее класс $[e]_\tau$ является тернарной R-подквазигруппой, а любой класс $[a]_\tau = f(e, a, [e]_\tau)$ ($[a]_\tau = f(a, e, [e]_\tau)$).*

В конце этого параграфа рассмотрим достаточный признак простоты для выше указанных шести конечных тернарных группоидов, тесно связанных с тернарной квазигруппой (такой же признак для квазигрупп имеется в [12], Предложение 3.13). Напомним, что тернарный группоид называется простым, если в нем только тривиальные конгруэнции.

Пусть $\langle Q, f\rangle$ – конечная квазигруппа и $Q = \{1, \ldots, m\}$. Для фиксированных элементов $j, k \in Q$ или $i, k \in Q$ или $i, j \in Q$ имеем соответственно подстановки α_{jk} или β_{ik} или γ_{ij} на Q, действующие по правилам $\alpha_{jk}(i) = f(i, j, k)$, $\beta_{ik}(j) = f(i, j, k)$, $\gamma_{ij}(k) = f(i, j, k)$.

Теорема 13. *([5]) Пусть τ – конгруэнция на конечной тернарной квазигруппе $\langle Q, f\rangle$ и подстановка δ, равная одной из подстановок α_{jk}, β_{ik}, γ_{ij}, имеет цикл $\{a, \delta(a), \delta^2(a), \ldots, \delta^{p-1}(a)\}$, $\delta^p(a) = a$. Наименьшее положительное целое число q такое, что $\delta^q(a)\tau a$, делит p.*

Теорема 14. *([5]) Пусть $\langle Q, f\rangle$ – конечная тернарная квазигруппа. Если имеется подстановка δ, равная одной из подстановок α_{jk}, β_{ik}, γ_{ij}, с циклом $\{a, \delta(a), \delta^2(a), \ldots, \delta^{p-1}(a)\}$, $\delta^p(a) = a$, где p – простое число и $p > \frac{|Q|}{2}$, то $\langle Q, f\rangle$ будет простой.*

Аналогично доказываются две ниже приведенные теоремы.

Теорема 15. *Пусть $\langle Q, f\rangle$ – конечная тернарная (L, M)-квазигруппа ((L, R)-квазигруппа, (M, R)-квазигруппа). Если имеется подстановка δ, равная одной из подстановок α_{jk} или β_{ik} (α_{jk} или γ_{ij}, β_{ik} или γ_{ij}), с циклом $\{a, \delta(a), \delta^2(a), \ldots, \delta^{p-1}(a)\}$, $\delta^p(a) = a$, где p – простое число и $p > \frac{|Q|}{2}$, то $\langle Q, f\rangle$ будет простой.*

Теорема 16. *Пусть $\langle Q, f\rangle$ – конечная тернарная L-квазигруппа (M-квазигруппа, R-квазигруппа). Если имеется подстановка δ, равная подстановке α_{jk} (β_{ik}, γ_{ij}), с циклом $\{a, \delta(a), \delta^2(a), \ldots, \delta^{p-1}(a)\}$, $\delta^p(a) = a$, где p – простое число и $p > \frac{|Q|}{2}$, то $\langle Q, f\rangle$ будет простой.*

6 Полиномиально полные тернарные группоиды, тесно связанные с тернарной квазигруппой

Пусть A – непустое множество и F – набор алгебраических операций, действующих на этом множестве. Тогда A называют F-алгеброй. Обозначим через $T(F)$ наименьший клон операций над A, содержащий F. Операции из $T(F)$ называются термальными операциями в сигнатуре F.

Операция $f(x_1, \ldots, x_n)$, действующая на множестве A, называется полиномиальной, если существуют термальная $n+m$-арная операция g и элементы $a_1, \ldots, a_m \in A$ такие, что

$$f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n, a_1, \ldots, a_m)$$

для любых элементов $x_1, \ldots, x_n \in A$.

Клон $Pol(F)$ всех полиномиальных операций является наименьшим клоном, содержащим F и все нульместные операции.

F-алгебра A называется полиномиально полной, если множество всех алгебраических операций, действующих на A, совпадает с $Pol(F)$.

Тернарная операция $m(x, y, z)$, действующая на множестве A, называется термом Мальцева, если верны тождества

$$m(x, x, y) = y = m(y, x, x)$$

.

Теорема 17. *В тернарной (L, M)-квазигруппе $\langle Q, f\rangle$ тернарная операция $m(x, y, z) = f(u(x, v(x, y, z), z), v(x, z, z), z)$ является термом Мальцева.*

Доказательство. Поскольку, согласно тождеству (6), имеем равенство $f(x, v(x, x, y), y) = x$ и элемент $u(x, v(x, x, y), y)$ является решением уравнения $f(t, v(x, x, y), y) = x$ с переменной t (в силу тождества (5), то, в силу однозначной разрешимости этого уравнения, получим $u(x, v(x, x, y), y) =$

x. А тогда, вновь с использованием тождества (6), получим

$$m(x,x,y) = f(u(x,v(x,x,y),y),v(x,y,y),y) = f(x,v(x,y,y),y) = y.$$

Используя тождество (5), получим

$$m(y,x,x) = f(u(y,v(y,x,x),x),v(y,x,x),x) = y.$$

□

Теорема 18. *В тернарной (L,R)-квазигруппе $\langle Q,f\rangle$ тернарная операция $m(x,y,z) = f(u(x,z,w(x,z,y)),y,w(x,y,z))$ является термом Мальцева.*

Доказательство. Поскольку, согласно тождеству (7), имеем равенство $f(x,y,w(x,y,x)) = x$ и элемент $u(x,y,w(x,y,x))$ является решением уравнения $f(t,y,w(x,y,x)) = x$ с переменной t (в силу тождества (5)), то, в силу однозначной разрешимости этого уравнения, имеем

$$u(x,y,w(x,y,x)) = x.$$

А тогда, вновь с использованием тождества (7), получим

$$m(x,x,y) = f(u(x,y,w(x,y,x)),x,w(x,x,y)) = f(x,x,w(x,x,y)) = y.$$

Используя тождество (5), получим

$$m(y,x,x) = f(u(y,x,w(y,x,x)),x,w(y,x,x)) = y.$$

□

Теорема 19. *В тернарной (M,R)-квазигруппе $\langle Q,f\rangle$ тернарная операция $m(x,y,z) = f(x,v(x,x,w(x,x,y)),w(x,x,z))$ является термом Мальцева.*

Доказательство. Поскольку, согласно тождеству (7), имеем равенство $f(x,x,w(x,x,x)) = x$ и элемент $v(x,x,w(x,x,x))$ является решением уравнения $f(x,t,w(x,x,x)) = x$ с переменной t (в силу тождества (6)), то, в силу однозначной разрешимости этого уравнения, получим

$$v(x,x,w(x,x,x)) = x.$$

А тогда, вновь с использованием тождества (7), получим

$$m(x,x,y) = f(x,v(x,x,w(x,x,x)),w(x,x,y)) = f(x,x,w(x,x,y)) = y.$$

Используя тождество (6), получим

$$m(y,x,x) = f(y,v(y,y,w(y,y,x)),w(y,y,x)) = y.$$

□

Алгебра A называется аффинной (см. [12]), если A снабжена структурой аддитивной абелевой группы такой, что каждая термальная операция g имеет вид

$$g(x_1, \ldots, x_n) = a_0 + \alpha_1 x_1 + \ldots + \alpha_n x_n,$$

где $a_0 \in A$, $\alpha_1, \ldots, \alpha_n$ являются групповыми эндоморфизмами. Известно, что если в аффинной алгебре A имеется терм Мальцева, который является полиномиальной операцией, то сложение в определении аффинной алгебры является полиномиальной операцией (см. [12], Предложение 2.7).

Теорема 20. *([13]) Пусть A – конечная F-алгебр, содержащая по меньшей мере два элемента. Тогда следующие условия эквивалентны:*

(i) A полиномиально полна;

(ii) существует терм Мальцева в $Pol(F)$ на A и алгебра A является простой и неаффинной.

Следствие 21. *Пусть $\langle Q, f\rangle$ – конечная тернарная (L, M)-квазигруппа ((L, R)-квазигруппа, (M, R)-квазигруппа), содержащая по меньшей мере два элемента. Тогда $\langle Q, f\rangle$ полиномиально полна если и только если $\langle Q, f\rangle$ является простой и неаффинной.*

Доказательство. В тернарной (L, M)-квазигруппе ((L, R)-квазигруппа, (M, R)-квазигруппа) $\langle Q, f\rangle$ существует терм Мальцева (теорема 17 (теорема 18, теорема 19)). Осталось применить теорему 20. □

References

[1] В.А. Щербаков, О конгруэнциях группоидов, тесно связанных с квазигруппами // Фундаментальная и прикладная математика **14** (5), 237–251 (2008).

[2] В Т. Марков, А.В. Михалчв, А.А. Нечаев, Неассоциативные алгебраические структуры в криптографии и кодировании // Фундамент. и прикл. матем. **21** (4), 621–641 (2016).

[3] М.М. Глухов, О применениях квазигрупп в криптографии // ПДМ **2**, 28–32 (2008).

[4] S. Markovski, D. Gligoroski, V. Bakeva, Quasigroup String Processing: Part 1 // Proc. of Maked. Academ. of Sci. and Arts for Math. And Tect. Sci. XX., 155–162 (1999).

[5] Н.А. Щучкин, Применение тернарных квазигрупп к преобразованию слов // Дискрет. матем., **36:2**, 132Ц-143 (2024).

[6] В.А. Артамонов, Полиномиально полные алгебры // Ученые записки ОГУ, **6:2**, 23–29 (2012).

[7] V.A. Artamonov, S. Chakrabarti, S.K. Pal, Characterization of Polynomially Complete Quasigroups based on Latin Squares for Cryptographic Transformations // Discrete Applied Mathematics, 5–17 (2016).

[8] В.Д. Белоусов, n-Арные квазигруппы, "Штиинца", Кишинев, 1972.

[9] Н.П. Соколов, Введение в теорию многомерных матриц, Наукова думка, Киев, 1972.

[10] H.J. Ryser, Permanents and systems of distinct representatives // Proceedings of the Conference on Combinatorial mathematics and its applications, University of North Carolina, Chapel Hill, 55–70 (1967).

[11] Г.Б.Белявская, T-квазигруппы и центр квазигруппы // Матем. исслед. **3**, 24–43 (1989).

[12] V.A. Artamonov, S. Chakrabarti, S. Gangopadhyay, S.K. Pal, Latin squares of polynomially complete quasigroups and quasigroups generated by shifts // Quasigroups and Related Systems, **21:2**, 117–130 (2013).

[13] J. Hagemann, C Herrmann. Arithmetically locally equational classes and representation of partial functions // Universal Algebra, Estergom (Hungary), vol. 29, Colloq. Math. Soc. J. Bolyai, 345–360 (1982).

STRUCTURE OF SEMIGROUPS ADMITTING GENERALIZED OUTERPLANAR CAYLEY GRAPHS

D.V. Solomatin

Omsk State Pedagogical University,
Tukhachevsky emb., 14, Omsk, 644099, Russia
e-mail: solomatin_dv@omgpu.ru

In this paper we investigate how do the properties of outerplanarity and generalized outerplanarity of Cayley graphs of planar semigroups correlate [1, Problem 4]. In the class of direct products of cyclic semigroups the following results are obtained.

Lemma 1 [2, Theorem 21]. *A finite semigroup S, which is a direct product of non-singleton cyclic semigroups, admits a planar Cayley graph if and only if at least one of the following conditions holds*:

1) $S \cong \langle a \mid a^{r+m} = a^r \rangle \times \left\langle b \;\middle|\; b^{h+t} = b^h \right\rangle$, where for natural numbers r, m, h and t one of the following conditions is satisfied:
1.1) $r = 1$, $h = 1$, $\mathrm{GCD}(m,\ t) < 3$;
1.2) $r = 1$, $m = 2$, $t < 3$;
1.3) $r = 2$, $m = 1$, $h < 4$, $t < 3$;
1.4) $r = 2$, $m = 1$, $h < 5$, $t = 1$;
1.5) $r = 3$, $m = 1$, $h = 3$, $t = 1$;

2) $S \cong \langle a \mid a^{r+m} = a^r \rangle \times \left\langle b \;\middle|\; b^{h+t} = b^h \right\rangle \times \left\langle c \;\middle|\; c^{k+l} = c^k \right\rangle$, where for natural numbers r, m, h, t, k, l one of the following conditions holds:

2.1) $r = 1$, $m = 2$, $h = 1$, $t = 2$, $k = 1$, $l = 2$;
2.2) $r = 1$, $m = 2$, $h = 2$, $t = 1$, $k = 2$, $l = 1$;
2.3) $r = 2$, $m = 1$, $h = 2$, $t = 1$, $k = 2$, $l < 3$;
2.4) $r = 2$, $m = 1$, $h = 2$, $t = 1$, $k = 3$, $l = 1$;

3) $S \cong \left\langle a_0 \mid a_0^{r+m} = a_0^r \right\rangle \times \prod_{i=1}^{n} \left\langle a_i \mid a_i^{2+1} = a_i^2 \right\rangle$, where for natural numbers r and m one of the following conditions is satisfied:

3.1) $r = 1$, $m = 2$;
3.2) $r = 2$, $m < 3$;
3.3) $r = 3$, $m = 1$.

Theorem 1.1 [3, Theorem 3.1]. *A finite semigroup S, which is a direct product of non-singleton cyclic semigroups, admits a generalized outerplanar Cayley graph if and only if at least one of the following conditions holds*:

1) $S \cong \langle a \mid a^{r+m} = a^r \rangle \times \left\langle b \mid b^{h+t} = b^h \right\rangle$, where for natural numbers r, m, h and t one of the following conditions is satisfied:

1.1) $r = 1$, $h = 1$, ($\mathrm{GCD}\,(m,\ t) = 1$ or $m = t = 2$);
1.2) $r = 1$, $m = 2$, ($h < 4$, $t = 1$ or $h = t = 2$);
1.3) $r = 2$, $m = 1$, $h < 4$, $t < 3$;
1.4) $r = 3$, $m = 1$, $h = 3$, $t = 1$;

2) $S \cong \langle a \mid a^{r+m} = a^r \rangle \times \left\langle b \mid b^{h+t} = b^h \right\rangle \times \left\langle c \mid c^{k+l} = c^k \right\rangle$, where for natural numbers r, m, h, t, k, l one of the following conditions is satisfied:

2.1) $r = 1$, $m = 2$, $h = 2$, $t = 1$, $k = 2$, $l = 1$;
2.2) $r = 2$, $m = 1$, $h = 2$, $t = 1$, $k = 2$, $l < 3$;
2.3) $r = 2$, $m = 1$, $h = 2$, $t = 1$, $k = 3$, $l = 1$;

3) $S \cong \left\langle a_0 \mid a_0^{r+m} = a_0^r \right\rangle \times \prod_{i=1}^{n} \left\langle a_i \mid a_i^{2+1} = a_i^2 \right\rangle$, $n > 2$, where for natural numbers r and m one of the following conditions is satisfied:

3.1) $r = 1$, $m = 2$;
3.2) $r = 2$, $m < 3$;
3.3) $r = 3$, $m = 1$.

Theorem 1.2 [3, Theorem 3.2]. *A finite semigroup S, which is a direct product of non-singleton cyclic semigroups, admits an outerplanar Cayley graph if and only if at least one of the following conditions is true*:

1) $S \cong \langle a \mid a^{r+m} = a^r \rangle \times \left\langle b \mid b^{h+t} = b^h \right\rangle$, where for the natural numbers r, m, h and t one of the following conditions is satisfied:

1.1) $r = 1$, $h = 1$, ($\mathrm{GCD}(m, t) = 1$ or $m = t = 2$);
1.2) $r = 1$, $m = 2$, $h = 2$, $t = 1$;
1.3) $r = 2$, $m = 1$, $h < 4$, $t = 1$;

2) $S \cong \prod_{i=1}^{n} \left\langle a_i \mid a_i^{2+1} = a_i^2 \right\rangle$, where $n > 2$.

It's easy to see that next new corollary holds.

Corollary 1. A finite semigroup S, which is a direct product of non-singleton cyclic semigroups, admits a generalized outerplanar Cayley graph, but does not admit an outerplanar Cayley graph if and only if one of the following conditions is true:

1) $S \cong \langle a \mid a^{r+m} = a^r \rangle \times \left\langle b \mid b^{h+t} = b^h \right\rangle$, where for the natural numbers r, m, h and t one of the following conditions is satisfied:

1.1) $r = 1$, $m = 2$, ($h = 3$, $t = 1$ or $h = t = 2$);
1.2) $r = 2$, $m = 1$, $1 < h < 4$, $t = 2$;
1.3) $r = 3$, $m = 1$, $h = 3$, $t = 1$;

2) $S \cong \left\langle a_0 \mid a_0^{r+m} = a_0^r \right\rangle \times \prod_{i=1}^{n} \left\langle a_i \mid a_i^{2+1} = a_i^2 \right\rangle$, where for natural numbers r, m and $n \geq 2$ one of the following conditions is satisfied:

2.1) $r = 1$, $m = 2$;
2.2) $r = 2$, $m = 2$;
2.3) $r = 3$, $m = 1$.

Let $\langle a \mid a^{r+m} = a^r \rangle$ be a cyclic semigroup.

Then $\langle a \mid a^{r+m} = a^r \rangle^1 = \begin{cases} \langle a, 1 \mid a^{r+m} = a^r, a1 = 1a = a \rangle, \text{if } r > 1; \\ \langle a \mid a^{1+m} = a \rangle, \text{otherwise}; \end{cases}$

and $\langle a \mid a^{r+m} = a^r \rangle^{+1} = \langle a, 1 \mid a^{r+m} = a^r, a1 = 1a = a \rangle$ are monoids. Moreover, $\langle a \mid a^{1+m} = a \rangle$ is a monoid.

In the class of direct products of cyclic monoids the following results holds.

Lemma 2 [2, Theorem 22]. *A finite monoid S, which is a direct product of non-singleton cyclic monoids, admits a planar Cayley graph if and only if one of the following conditions holds*:

1) $S \cong \langle a \mid a^{r+m} = a^r \rangle^1 \times \left\langle b \;\middle|\; b^{h+t} = b^h \right\rangle^1$, where for natural r, m, h and t one of the following conditions is satisfied:

1.1) $r = 1$, $m = 2$;
1.2) $m \leq 2$, $t \leq 2$;
1.3) $r = 1$, $m > 2$, $t \leq 2$;

2) $S \cong \langle a \mid a^3 = a \rangle \times \langle b \mid b^3 = b \rangle \times \left\langle c \;\middle|\; c^{k+l} = c^k \right\rangle^i$, where i takes the values indicated below, and for natural k, l one of the following conditions is satisfied:

2.1) $i = 1$, $l \leq 2$;
2.2) $i = +1$, $k = 1$, $l \leq 2$;

3) $S \cong \langle a \mid a^{1+m} = a^1 \rangle^{+1} \times \left\langle b \;\middle|\; b^{h+t} = b^h \right\rangle^i$, where m, h, t are natural numbers, $i \in \{1, +1\}$ and one of the following conditions is satisfied:

3.1) $m = 1$;
3.2) $i = 1$, $h = 1$, $t = 2$;
3.3) $m = 2$, $h = 1$, $i = 1$;
3.4) $m = 2$, $h = 1$, $t = 2$, $i = +1$.

4) $S \cong \left\langle a_0 \;\middle|\; a_0^{r+m} = a_0^r \right\rangle^1 \times \prod_{i=1}^n \langle a_i \mid a_i^2 = a_i \rangle^{+1}$, where $m \leq 2$, $n \leq 2$; or $r = 1$, $m = 1$, $n \leq 3$.

Theorem 2.1 [4, Theorem 1]. *A finite monoid S, which is a product of non-singleton cyclic monoids, admits an outerplanar Cayley graph if and only if at least one of the following conditions is true*:

1) $S \cong \langle a \mid a^3 = a \rangle \times \left\langle b \;\middle|\; b^{h+t} = b^h \right\rangle^1$, where for natural h, t the inequalities $h \leq 2$ and $h + t \leq 4$ are satisfied;

2) $S \cong \langle a \mid a^{1+m} = a \rangle^{+1} \times \left\langle b \;\middle|\; b^{h+t} = b^h \right\rangle^i$, where $i \in \{1, +1\}$ and for natural m, h, t one of the following conditions is satisfied:

2.1) $m = 1$, $t \leq 2$;
2.2) $i = 1$, $m \leq 2$, $h = 1$, $t = 2$;
2.3) $i = 1$, $m = 2$, $h = 1$, $t \leq 2$;

3) $S \cong \left\langle a_0 \;\middle|\; a_0^{r+m} = a_0^r \right\rangle^1 \times \prod_{i=1}^n \langle a_i \mid a_i^2 = a_i \rangle^{+1}$, where for natural r, n,

m, one of the following conditions is satisfied:

3.1) $n = m = 1$;
3.2) $n - 1 = r = m = 1$;
3.3) $n = m - 1 = 1$.

Theorem 2.2 [4, Theorem 2]. *A finite monoid S, which is a product of non-singleton cyclic monoids, admits a generalized outerplanar Cayley graph if and only if at least one of the following conditions holds*:

1) $S \cong \langle a \mid a^{r+m} = a^r \rangle^1 \times \left\langle b \;\middle|\; b^{h+t} = b^h \right\rangle^1$, where for natural h, t the inequalities $h \leq 2$ and $h + t \leq 4$ are satisfied;

2) $S \cong \langle a \mid a^{1+m} = a \rangle^{+1} \times \left\langle b \;\middle|\; b^{h+t} = b^h \right\rangle^i$, where $i \in \{1, \ +1\}$ and given natural m, h, t one of the following conditions is satisfied:

2.1) $m = 1$, $t \leq 2$;
2.2) $i = 1$, $m \leq 2$, $h = 1$, $t = 2$;
2.3) $i = 1$, $m = 2$, $h = 1$, $t \leq 2$;
2.4) $i = +1$, $m = 2$, $h = 1$, $t = 2$;

3) $S \cong \left\langle a_0 \;\middle|\; a_0^{r+m} = a_0^r \right\rangle^1 \times \prod_{i=1}^{n} \langle a_i \mid a_i^2 = a_i \rangle^{+1}$, where for natural r, n, m, one of the following conditions is satisfied:

3.1) $n = m = 1$;
3.2) $n - 1 = r = m = 1$;
3.3) $n = m - 1 = 1$.

Corollary 2 [4, Corollary 1]. A finite monoid S, which is a product of non-singleton cyclic monoids, admits a generalized outerplanar Cayley graph, but does not admit an outerplanar Cayley graph if and only if $S \cong \langle a \mid a^3 = a \rangle^{+1} \times \langle b \mid b^3 = b \rangle^{+1}$.

Note that $\langle a \mid a^{r+m} = a^r \rangle^0 = \begin{cases} \langle a, 0 \mid a^{r+m} = a^r, a0 = 0a = 0 \rangle, \text{if} \;\; m > 1; \\ \langle a \mid a^{r+1} = a^r \rangle, \text{otherwise}; \end{cases}$
and $\langle a \mid a^{r+m} = a^r \rangle^{+0} = \langle a, 0 \mid a^{r+m} = a^r, a0 = 0a = 0 \rangle$ are semigroups with zero. Moreover, $\langle a \mid a^{r+1} = a^r \rangle$ is a semigroup with zero.

In the class of direct products of cyclic semigroups with zero the following result holds.

Lemma 3 [2, Theorem 23]. *A finite semigroup S with zero, which is a direct product of non-singleton cyclic semigroups with zero, admits a planar Cayley graph if and only if at least one of the following conditions is satisfied*:

1) $S \cong \langle a \mid a^{r+m} = a^r \rangle^0 \times \left\langle b \;\middle|\; b^{h+t} = b^h \right\rangle^0$, where for natural numbers r, m, h, t one of the following conditions is satisfied:

1.1) $r = 2$, $m = 1$, $h < 5$, $t = 1$;
1.2) $r = 3$, $m = 1$, $h = 3$, $t = 1$;
1.3) $r = 2$, $m = 1$, $h = 1$, $t = 2$;

2) $S \cong \left\langle a_0 \;\middle|\; a_0^{r+1} = a_0^r \right\rangle \times \prod_{i=1}^n \left\langle a_i \;\middle|\; a_i^{2+1} = a_i^2 \right\rangle$, where $r \leq 3$;

3.1) $S \cong \langle a \mid a^{2+1} = a^2 \rangle \times \langle b \mid b^{2+1} = b^2 \rangle^{+0}$;

3.2) $S \cong \langle a \mid a^{r+m} = a^r \rangle^{+0} \times \langle b \mid b^2 = b \rangle^{+0}$, where r and m are natural numbers, and $m \leq 2$;

4) $S \cong \left\langle a_0 \;\middle|\; a_0^{r+1} = a_0^r \right\rangle \times \prod_{i=1}^n \langle a_i \mid a_i^2 = a_i \rangle^{+0}$, where $n \leq 2$; or $r = 1$, $n \leq 3$.

Theorem 3.1 [5, Theorem 1]. *A finite semigroup S with zero, which is a direct product of non-singleton cyclic semigroups with zero, admits an outerplanar Cayley graph if and only if one of the following conditions holds*:

1) $S \cong \langle a \mid a^3 = a^2 \rangle^0 \times \left\langle b \;\middle|\; b^{h+1} = b^h \right\rangle^0$, where h is a natural number, and $h < 4$;

2) $S \cong \left\langle a_0 \;\middle|\; a_0^{r+1} = a_0^r \right\rangle \times \prod_{i=1}^n \left\langle a_i \;\middle|\; a_i^{2+1} = a_i^2 \right\rangle$, where r and n are natural numbers, and $r \leq 2$; or $r = 3$, $n = 1$;

3) $S \cong \langle a \mid a^{r+m} = a^r \rangle^{+0} \times \langle b \mid b^2 = b \rangle^{+0}$, where r and m are natural numbers, and $m \leq 2$;

4) $S \cong \left\langle a_0 \;\middle|\; a_0^{r+1} = a_0^r \right\rangle \times \prod_{i=1}^n \langle a_i \mid a_i^2 = a_i \rangle^{+0}$, where $n = 1$; or $r = 1$, $n = 2$.

Theorem 3.2 [5, Theorem 2]. *A finite semigroup S with zero, which is a direct product of non-singleton cyclic semigroups with zero, admits a*

generalized outerplanar Cayley graph if and only if one of the following conditions holds:

1) $S \cong \langle a \mid a^{r+m} = a^r \rangle^0 \times \langle b \mid b^{h+t} = b^h \rangle^0$, where for natural numbers r, m, h, t, one of the following conditions is satisfied:

1.1) $r = 2$, $m = 1$, $h < 4$, $t = 1$;
1.2) $r = 3$, $m = 1$, $h = 3$, $t = 1$;

2) $S \cong \langle a_0 \mid a_0^{r+1} = a_0^r \rangle \times \prod_{i=1}^n \langle a_i \mid a_i^{2+1} = a_i^2 \rangle$, where r and n are natural numbers, and $r \leq 3$;

3.1) $S \cong \langle a \mid a^{2+1} = a^2 \rangle \times \langle b \mid b^{2+1} = b^2 \rangle^{+0}$;

3.2) $S \cong \langle a \mid a^{r+m} = a^r \rangle^{+0} \times \langle b \mid b^2 = b \rangle^{+0}$, where r and m are natural numbers, and $m \leq 2$;

4) $S \cong \langle a_0 \mid a_0^{r+1} = a_0^r \rangle \times \prod_{i=1}^n \langle a_i \mid a_i^2 = a_i \rangle^{+0}$, where $n = 1$; or $r = 1$, $n = 2$.

Corollary 3 [5, Corollary 1]. Finite semigroup S which is a product of non-singleton cyclic semigroups with zero admits a generalized outerplanar Cayley graph, but does not admit an outerplanar Cayley graph if and only if one of the following conditions holds:

1) $S \cong \langle a \mid a^4 = a^3 \rangle^0 \times \langle b \mid b^4 = b^3 \rangle^0$;

2) $S \cong \langle a_0 \mid a_0^4 = a_0^3 \rangle \times \prod_{i=1}^n \langle a_i \mid a_i^3 = a_i^2 \rangle$, where $n > 1$;

3) $S \cong \langle a \mid a^3 = a^2 \rangle \times \langle b \mid b^3 = b^2 \rangle^{+0}$.

Let $\Gamma = (\{a_1, \ldots, a_t\}, E_\Gamma)$ be a graph with $V_\Gamma = \{a_1, \ldots, a_t\}$. Then $S_t^n(\Gamma) \cong \langle V_\Gamma \mid a_i a_j = a_j a_i \Longleftrightarrow \{a_i, a_j\} \in E_\Gamma \rangle$ and the identity $x_1 \ldots x_n = y_1 \ldots y_n$ holds in $S_t^n(\Gamma)$ by definition.

In the class of free partially commutative nilpotent semigroups $S_t^n(\Gamma)$ the following result holds.

Lemma 4 [2, Theorem 51]. *The semigroup $S_t^n(\Gamma)$ admits a planar Cayley graph if and only if at least one of the following conditions holds*:

1) Γ is the empty graph;

2) the connected components of the graph Γ are matchings or isolated vertices, and $n \leq 5$;

3) the connected components of the graph Γ are chains or isolated vertices, and $n \leq 4$;

4) the connected components of the graph Γ are "trees" of simple cycles (i.e. cactuses) or isolated vertices, and $n \leq 3$;

5) Γ is any graph and $n \leq 2$, or ($n > 2$ and $t \leq 2$).

Theorem 4.1 [6, Theorem 1]. *For any graph Γ, the semigroup $S_t^n(\Gamma)$ admits an outerplanar Cayley graph if and only if at least one of the following conditions is satisfied*:

1) $t = 1$;

2) $1 \leq n \leq 2$;

3) $n = 3$ and $t = 2$.

Theorem 4.2 [6, Theorem 2]. *The semigroup $S_t^n(\Gamma)$ admits a generalized outerplanar Cayley graph if and only if at least one of the following conditions is satisfied*:

1) $n = 4$ and $t = 2$, and Γ is any graph;

2) $n = 3$ and $t \geq 3$, and the connected components of the graph Γ are chains or isolated vertices;

3) Γ is any graph, and $t = 1$, or $1 \leq n \leq 2$, or ($n = 3$ and $t = 2$).

Corollary 4 [6, Corollary 1]. A free partially commutative nilpotent semigroup $S_t^n(\Gamma)$ admits a generalized outerplanar Cayley graph, but does not admit an outerplanar Cayley graph if and only if one of the following conditions is satisfied:

1) Γ is any graph, and $n = 4$ and $t = 2$;

2) the connected components of the graph Γ are chains or isolated vertices, and $n = 3$ and $t \geq 3$.

In the class of semigroups with one defining relation and partially commutative free semigroup the following result holds.

Lemma 5 [2, Theorem 52]. *A noncyclic semigroup S with one defining relation, admitting a semigroup identity, has a planar Cayley graph if and only if S is anti-isomorphic to one of the semigroups*:

$S_1 = \langle a,\ b \mid ab = ba\rangle$, $S_{2,k} = \left\langle a,\ b \mid ab = b^k\right\rangle$, *where* $k = 1,\ 2, \ldots,$ $S_3 = \langle a,\ b \mid aba = ba\rangle$, $S_4 = \langle a,\ b \mid aba = b\rangle$, $S_5 = \langle a,\ b \mid a^2 = b^2\rangle$, $S_6 = \langle a,\ b \mid aba^2 = ba\rangle$; *or is isomorphic to one of the semigroups*: S_1, $S_{2,1}$, S_4, S_5.

Note that a noncyclic semigroup with one defining relation admitting a semigroup identity is isomorphic or anti-isomorphic to one of the following semigroups: S_1, $S_{2,k}$, where $k = 1,\ 2, \ldots,$ S_3, S_4, S_5 or S_6 [7, P. 52].

Theorem 5.1 [8, Theorem 1]. *If S is a non-cyclic semigroup with a one defining relation and admitting a semigroup identity, then the following conditions are equivalent*:

1) The semigroup S admits an outerplanar Cayley graph;

2) The semigroup S admits a generalized outerplanar Cayley graph;

3) The semigroup S is anti-isomorphic to one of the semigroups:

$S_{2,k} = \left\langle a,\ b \mid ab = b^k\right\rangle$, where $k \leq 3$, $S_3 = \langle a,\ b \mid aba = ba\rangle$; or is isomorphic to the semigroup $S_{2,1} = \langle a,\ b \mid ab = b\rangle$.

Theorem 5.2 [8, Theorem 2]. *If $S(\Gamma)$ is a partially commutative free semigroup corresponding to the commutativity graph Γ of the set of elements generating it, then the following conditions are equivalent*:

1) The semigroup $S(\Gamma)$ admits an outerplanar Cayley graph;

2) The semigroup $S(\Gamma)$ admits a generalized outerplanar Cayley graph;

3) The degree of any vertex in the graph Γ is equal to zero, that is, the semigroup $S(\Gamma)$ is anticommutative.

We present one more result demonstrating semigroups whose generalized outerplanar property of a Cayley graph is equivalent to the property of its planarity.

Let $S_k^n = \langle a_1, \ldots, a_k \mid a_i^2 = a_i, \ \ a_i a_j = a_j a_i, \ \ a_{i_1} a_{i_2} \ldots a_{i_n} = 0 \rangle$ called a n-fan semilattice. In the class of semilattices (commutative semigroups of idempotents) the following result holds.

Theorem 6 [8, Theorem 3]. *If $S = S_k^n$ is a n-fan semilattice, then the following conditions are equivalent*:

1) The semigroup S admits a planar Cayley graph;

2) The semigroup S admits a generalized outerplanar Cayley graph;

3) $|S^{(2)}| \leq 3$, where $S^{(2)}$ is the set of all non-zero words of semigroup S of the form $a_i a_j$, with $i \neq j$.

On the admissibility of graphs taken with a certain orientation and marking of edges as Cayley graphs for semigroups the following result holds.

Theorem 7.1 [2, Theorem 53] (on the admissibility of Pontryagin-Kuratovsky graphs). *If $Cay(S,\ E)$ is the Cayley graph of a finite semigroup S, then $Cay(S,\ E)$*:

1) is not isomorphic to the complete bipartite graph $K_{3,3}$ with any orientation and edge coloring (marking);

2) is isomorphic to the complete graph K_5 with a unique orientation of the edges if and only if $S = \langle a, b \mid ab = ba, a = b^2 = a^3 b, a^2 = ab^2, b = a^3 = a^2 b^2 \rangle$.

Theorem 7.2 [2, Theorem 45] (on the admissibility of Chartrand-Harary graphs). *If $Cay(S,\ E)$ is the Cayley graph of a finite semigroup S, then $Cay(S,\ E)$*:

1) is not isomorphic to the complete graph K_4 with any orientation and edge coloring;

2) is not isomorphic to the complete bipartite graph $K_{2,3}$ with any orientation and edge coloring.

Finally, we use ideas for solving the problem of the admissibility of Pontryagin-Kuratovsky graphs taken with some orientation and marking of edges as Cayley graphs of semigroups and similarly Chartrand-Harary graphs. Consider the question about the admissibility of Sedláček graphs, taken with a certain orientation and marking of edges, as Cayley graphs of semigroups.

Theorem 7.3 [8, Theorem 4] (on the admissibility of Sedláček graphs). *If $Cay(S,\ E)$ is the Cayley graph of a finite semigroup, then $Cay(S,\ E)$ is not isomorphic to any of the Sedláček graphs G_i, where $1 \leq i \leq 12$, with any orientation and edge coloring.*

References

[1] New problems of algebra and logic. 900th anniversary meeting of the seminar // Omsk Algebraic Seminar November 12, 2015, URL: https://www.mathnet.ru/php/seminars.phtml?presentid=12900 (in Russian).

[2] D.V. Solomatin, Researches of semigroups with planar Cayley graphs: results and problems // Prikladnaya Diskretnaya Matematika, 2021, No. 54, pp. 5–57 (in Russian).

[3] D.V. Solomatin, Direct products of cyclic semigroups allowing outerplanar Cayley graphs and their generalizations // Applied Mathematics & Physics, 2024, Vol. 56, No. 1, pp. 13–20 (in Russian).

[4] D.V. Solomatin, Direct products of cyclic monoids admitting outerplanar Cayley graphs and their generalizations // Herald of Tver State University. Series: Applied Mathematics, 2023, No. 4, pp. 43–56 (in Russian).

[5] D.V. Solomatin, Direct products of cyclic semigroups with zero, admitting outerplanar and generalized outerplanar Cayley graphs // Tomsk state university journal of mathematics and mechanics. Mathematics. 2024. No. 90, P. 7 (in Russian).

[6] D.V. Solomatin, Free partially commutative nilpotent semigroups with outerplanar and generalized outerplanar Cayley graphs // Herald of Dagestan State University. Series 1. Natural sciences. 2024. Vol. 39. Issue. 1, pp. 7–13 (in Russian).

[7] L.N. Shevrin, M.V. Volkov, Identities of semigroup // Izvestiya VUZ. Matematika, 1985, Vol. 29, No. 11, pp. 1–64.

[8] D.V. Solomatin, Comparison of outerplanarity and generalized outerplanarity properties for cayley graphs of planar semigroups // Prikladnaya Diskretnaya Matematika, 2024, No. 64, pp. 20–26 (in Russian).

T-PSEUDOFINITE ACTS OVER ABELIAN GROUPS

A.A. Stepanova, E.L. Efremov, S.G. Chekanov

Far Eastern Federal University*,
FEFU Campus, 10 Ajax Bay, Russky Island, Vladivostok, Russia
e-mail: stepltd@mail.ru, efremov-el@mail.ru, chekanov.sg@dvfu.ru

Introduction

The structure $\mathfrak{M}$ of a language L is called pseudofinite if every sentence true in $\mathfrak{M}$ has a finite model. The theory of pseudofinite structures is a well-developed theory. In this article, the concept of T-pseudofiniteness is introduced for models of a theory T, and this concept is considered for the theory of acts over some abelian group. A model $\mathfrak{M}$ of a theory T is called T-pseudofinite if every sentence true in $\mathfrak{M}$ is also true in a finite model of the theory T. It is clear that for every theory T, if a model $\mathfrak{M}$ of this theory is T-pseudofinite then $\mathfrak{M}$ is pseudofinite, and if a model $\mathfrak{M}$ of T is pseudofinite and T is a finite axiomatizable theory then $\mathfrak{M}$ is T-pseudofinite. In particular, for theories T of all (abelian) groups, all fields, all rings, all unars, ar all graphs, the concept of T-pseudofiniteness and pseudofiniteness are coincide. Problems of pseudofiniteness (T-pseudofiniteness) were studied in [1]-[7]. In [8], pseudofinite acts over a monoid with finite number of isomorphism types of finite cyclic subacts were studied; in particular, it is proved that a coproduct of finite acts over monoid is pseudofinite; and as a consequence, it is shown that every act over a finite group is pseudofinite.

In this article for the theory T of all G-acts, where G is a group with only finitely many subgroups of finite index, it is proved that G-acts are T-pseudofinite, if and only if they are elementarily equivalent to a coproduct of finite G-acts. This proposition implies that for divisible group G (for example, the additive groups of rational and real numbers, the multiplicative group of positive real numbers, a quasicyclic group) G-act ${}_GA$ is T-pseudofinite, if and only if ${}_GA$ is a coproduct of one-element G-acts, and if G is the multiplicative group of real numbers then G-act ${}_GA$ is T-pseudofinite, if and only if ${}_GA$ is a coproduct of one-element or two-element

*Supported by RF Ministry of Education and Science (Suppl. Agreement No. 075-02-2024-1440 of 28.02.2024.

G-acts. It is shown that every G-act is T-pseudofinite, if G is the group of integers.

1 Preliminaries

Let us recall some definitions and facts from the theory of acts and model theory (see [9, 10, 11]). Let S be a monoid with identity 1. A structure $\langle A; s\rangle_{s\in S}$ of the language $L_S = \{s \mid s \in S\}$ consisting of unary operation symbols is a (left) *S-act* if $s_1(s_2a) = (s_1s_2)a$ and $1a = a$ for all $s_1, s_2 \in S$ and $a \in A$. An S-act $\langle A; s\rangle_{s\in S}$ is denoted by ${}_SA$. Elements x, y of an S-act ${}_SA$ are called *connected* (denoted by $x \sim y$) if there exist $n \in \omega$, $a_0, \ldots, a_n \in A$, $s_0, \ldots, s_{n-1}, t_0, \ldots, t_{n-1} \in S$ such that $x = a_0$, $y = a_n$, and $t_ia_i = s_ia_{i+1}$. An S-act ${}_SA$ is called *connected* if we have $x \sim y$ for every $x, y \in {}_SA$. It is easy to check that $\sim$ is a congruence relation on the S-act ${}_SA$. The classes of this relation are called *connected components* of the S-act ${}_SA$. *A coproduct* of S-acts ${}_SA_i$ is a disjunctive union of this S-acts. The coproduct of S-acts ${}_SA_i$ is denoted by $\coprod_{i\in I} {}_SA_i$. It is known [9] that every S-act ${}_SA$ can be uniquely represented as a coproduct of connected components.

Let G be a group and H be a subgroup of G. By ${}_GG/H$ we denote G-act ${}_G\{gH \mid g \in G\}$ with unary operations defined as follows: $g(aH) = (ga)H$ for every $g, a \in G$. Each connected G-act has the form ${}_GG/H$ for some subgroup H of G and it has no proper subacts.

The structure $\mathfrak{M}$ of language L is called *pseudofinite* if every sentence true in $\mathfrak{M}$ has a finite model. Let T be a consistent (but possibly incomplete) theory in language L. A model $\mathfrak{M}$ of the theory T is called *T-pseudofinite* if every sentence true in $\mathfrak{M}$ is also true in some finite model of the theory T. It is known that the structure $\mathfrak{M}$ of language L is pseudofinite iff $\mathfrak{M}$ is elementary equivalent to an ultraproduct of finite structures of language L ([12]). The proof of Theorem 1 is some variation of the proof of this proposition.

Theorem 1. *Let T be a theory of language L and $\mathfrak{M}$ be a model of T. Then $\mathfrak{M}$ is a T-pseudofinite structure if and only if $\mathfrak{M}$ is elementary equivalent to the ultraproduct of finite models of the theory T.*

It is clear that T-pseudofiniteness implies pseudofiniteness. From the proof of Theorem 1 from [8] we get

Theorem 2. *Every coproduct of finite S-acts is a T-pseudofinite S-act, where T is the theory of all S-acts.*

Theorem 3 (Loss theorem [11]). *Let $\{\mathfrak{M}_i \mid i \in I\}$ be a set of structures of language L, D be an ultrafilter on I, $\mathfrak{M} = \prod_{i\in I} \mathfrak{M}_i/D$ be the ultraproduct, $\Phi(x_1, \ldots, x_n)$ be the formula of the language L, and $m_1, \ldots, m_n \in \prod_{i\in I} \mathfrak{M}_i$. Then*

$$\mathfrak{M} \models \Phi(m_1/D, \ldots, m_n/D) \Leftrightarrow \{i \in I \mid \mathfrak{M}_i \models \Phi(m_1(i), \ldots, m_n(i))\} \in D.$$

2 T-pseudofinite acts over some groups

Proposition 1. *Let S be a monoid, T be the theory of all S-acts and suppose there are only a finite number of isomorphism types of connected finite S-acts. Then S-act ${}_SA$ is T-pseudofinite, if and only if ${}_SA$ is elementarily equivalent to a coproduct of finite S-acts.*

Proof. Sufficiency follows from Theorem 2. Let us prove the necessity. Suppose that ${}_SA$ is a T-pseudofinite S-act. By Theorem 1, ${}_SA$ is elementarily equivalent to the S-act ${}_SB$, where ${}_SB$ is an ultraproduct of finite S-acts. Suppose there exists an infinite connected component in ${}_SB$ and let $n \in \omega$ be the maximum power of a connected finite S-act. Then there are pairwise distinct $a_0, \ldots, a_n \in B$, and $s_0, \ldots, s_{n-1}, t_0, \ldots, t_{n-1} \in S$ such that $x = a_0$, $y = a_n$, and $t_i a_i = s_i a_{i+1}$. By the theorem of Los, there are pairwise distinct elements in some factor in ultraproduct ${}_SB$, that is this factor is infinite, a contradiction. Thus, the S-act ${}_SB$ is a coproduct of finite S-acts. □

From Proposition 1 we obtain:

Corollary 1. *Let G be a group with only finitely many subgroups of finite index, and let T be the theory of all G-acts. Then a G-act ${}_GA$ is T-pseudofinite, if and only if ${}_GA$ is elementarily equivalent to a coproduct of finite G-acts.*

From the facts that divisible groups, in particular the additive group of rational numbers, the additive group of real numbers, the multiplicative group of positive real numbers, a quasicyclic group, have no proper finite index subgroups, and the multiplicative group of real numbers has exactly two finite index subgroups, and from Corollary 1 we obtain the following.

Corollary 2. *Let G be a divisible group and T be the theory of all G-acts. Then G-act ${}_GA$ is T-pseudofinite, if and only if ${}_GA$ is a coproduct of one-element G-acts.*

Corollary 3. *Let G be the multiplicative group of real numbers and T be the theory of all G-acts. Then the G-act ${}_GA$ is T-pseudofinite, if and only if ${}_GA$ is a coproduct of one-element and two-element G-acts.*

Proposition 2. *Let T be the theory of all $\mathbb{Z}$-acts, where $\mathbb{Z}$ is the group of integers. Then every $\mathbb{Z}$-act is T-pseudofinite.*

Proof. It is clear that each connected $\mathbb{Z}$-act has the form ${}_{\mathbb{Z}}\mathbb{Z}$ or ${}_{\mathbb{Z}}\mathbb{Z}_n$, where $\mathbb{Z}_n$ is the set of all residue classes modulo n. Let

$$ {}_{\mathbb{Z}}A = \coprod_{j\in\alpha} {}_{\mathbb{Z}}\mathbb{Z}^j \sqcup \coprod_{m\in K}\coprod_{j\in\beta_m} {}_{\mathbb{Z}}\mathbb{Z}^j_m \sqcup \coprod_{l\in L}\coprod_{j\in\gamma_l} {}_{\mathbb{Z}}\mathbb{Z}^j_l, $$

where ${}_{\mathbb{Z}}\mathbb{Z}^j$ are the copies of ${}_{\mathbb{Z}}\mathbb{Z}$, ${}_{\mathbb{Z}}\mathbb{Z}^j_i$ are the copies of ${}_{\mathbb{Z}}\mathbb{Z}_i$, K, L are disjoint subsets of the set $\omega \setminus \{0,1\}$, β_m are finite ordinals for all $m \in K$, and γ_l are infinite ordinals for all $l \in I_l$. We will consider a more complex case when $\alpha > 0$ and the sets $K = \{m_0, m_1, \dots,\}$ and $L = \{l_o, l_1, \dots\}$ are infinite. Let ${}_{\mathbb{Z}}B$ denote the ultraproduct $\prod_{n\in\omega} {}_{\mathbb{Z}}C_n/D$, where

$$ {}_{\mathbb{Z}}C_n = {}_{\mathbb{Z}}\mathbb{Z}_n \sqcup \coprod_{j\in\beta_{m_0}} {}_{\mathbb{Z}}\mathbb{Z}^j_{m_0} \sqcup \dots \sqcup \coprod_{j\in\beta_{m_n}} {}_{\mathbb{Z}}\mathbb{Z}^j_{m_n} \sqcup \coprod_{j\le n} {}_{\mathbb{Z}}\mathbb{Z}^j_{l_0} \sqcup \dots \sqcup \coprod_{j\le n} {}_{\mathbb{Z}}\mathbb{Z}^j_{l_n}, $$

D is a nonprincipal ultrafilter on ω. By Theorem 1, ${}_{\mathbb{Z}}B$ is T-pseudofinite $\mathbb{Z}$-act. We will prove that the $\mathbb{Z}$-act ${}_{\mathbb{Z}}B$ is isomorphic to a $\mathbb{Z}$-act of the form

$$ \coprod_{j\in\alpha'} {}_{\mathbb{Z}}\mathbb{Z}^j \sqcup \coprod_{m\in K}\coprod_{j\in\beta_m} {}_{\mathbb{Z}}\mathbb{Z}^j_m \sqcup \coprod_{l'\in L}\coprod_{j\in\gamma_{l'}} {}_{\mathbb{Z}}\mathbb{Z}^j_{l'}, \tag{1} $$

where $\alpha' > 0$, $\gamma_{l'} \ge \omega$. Let $c \in \prod_{n\in\omega} {}_{\mathbb{Z}}C_n$. Then $M_1 = \{n \in \omega \mid c(n) \in \mathbb{Z}_n\} \in D$, or $M_2^k = \{n \in \omega \mid \exists j \in \beta_k\ (c(n) \in \mathbb{Z}^j_k)\} \in D$ for some $k \in K$, or $M_3^l = \{n \in \omega \mid \exists j \le n\ (c(n) \in \mathbb{Z}^j_l)\} \in D$ for some $k \in L$, or $M_4 = \{n \in \omega \mid \exists m \in K\ \exists j \in \beta_k\ (c(n) \in \mathbb{Z}^j_k)$ or $\exists l \in L\ \exists j \le n\ (c(n) \in \mathbb{Z}^j_l)\} \in D$, and M_4 has the following property:

$$ \forall m \in K \cup L(\exists n \in M_4 \exists j(c(n) \in \mathbb{Z}^j_m) \to \exists m' > m \exists n' > n \exists j'(c(n') \in \mathbb{Z}^{j'}_{m'}). $$

If $M_1 \in D$ then subact of ${}_{\mathbb{Z}}C$ generated by c/D is isomorphic to ${}_{\mathbb{Z}}Z$. If $M_2^k \in D$ then subact of ${}_{\mathbb{Z}}C$ generated by c/D is isomorphic to ${}_{\mathbb{Z}}Z_k$. If $M_3^l \in D$ then subact of ${}_{\mathbb{Z}}C$ generated by c/D is isomorphic to ${}_{\mathbb{Z}}Z_l$. If $M_4 \in D$ then subact of ${}_{\mathbb{Z}}C$ generated by c/D is isomorphic to ${}_{\mathbb{Z}}Z$. Thus, ${}_{\mathbb{Z}}B$ is isomorphic to a $\mathbb{Z}$-act ${}_{\mathbb{Z}}E$ of the form (1). It is clear that ${}_{\mathbb{Z}}E \equiv {}_{\mathbb{Z}}A$. By Theorem 2, ${}_{\mathbb{Z}}A$ is T-pseudofinite. □

References

[1] J. Ax, The elementary theory of finite fields // Annals of Mathematics. — 1968. — Vol. 88, No. 2. — P. 239–271.

[2] J. Duret, Les corps pseudo-finis ont la propriété d'indépendance // C. R. Acad. Sei. Paris Sér. — 1980. — Vol. 290. — P. 981–903.

[3] Z. Chatzidakis, Notes on the model theory of finite and pseudo-finite fields. http://www.logique.jussieu.fr/ zoe/papiers/Helsinki.pdf.

[4] D. Macpherson, Model theory of finite and pseudofinite groups // Arch. Math. Logic. – 2018. — Vol. 57. — P. 159–184.

[5] R. Bello-Aguirre, Model theory of finite and pseudofinite rings: PhD thesis // University of Leeds, 2016. https://etheses.whiterose.ac.uk/15771/1/RIBelloAguirrePhDThesis-Aug2016CORRECTED.pdf

[6] N.D. Markhabatov, Approximations of acyclic graphs // The Bulletin of Irkutsk State Univercity, Series "Mathematics". — 2022. — Vol. 40. — P. 104–111. https://doi.org/10.26516/1997-7670.2022.40.104

[7] E.L. Efremov, A.A. Stepanova, S.G. Chekanov, Pseudofinite unars // Algebra and Logic. (in press)

[8] E.L. Efremov, A.A. Stepanova, S.G. Chekanov, Pseudofinite S-acts // Siberian Electronic Mathematical Reports. — 2024. — Vol. 21, No. 1. — P. 271–276. https://doi.org/10.33048/semi.2024.21.020

[9] M. Kilp, U. Knauer, A.V. Mikhalev, Monoids, Acts and Categories. N.Y. — Berlin, Walter de Gruyter. 2000.

[10] I.B. Kozhukhov, A.V. Mikhalev, Acts over semigroups // Fundam. Prikl. Mat. 2020. — Vol. 23, No. 3. — P. 141–199.

[11] C.C. Chang, H. Jerome Keisler, Model theory. Amsterdam, North-Holland Pub. Co.; New York, American Elsevier, 1973.

[12] J. Väänänen, Pseudo-finite model theory // Matemática Contemporânea. — 2003. — Vol. 24. — P. 169–183.

STRUCTURES ON SIGNATURES OF STRUCTURES

A.I. Stukachev

Sobolev Institute of Mathematics
Acad. Koptyug avenue 4
630090 Novosibirsk Russia
e-mail: aistu@math.nsc.ru

R. Montague in "English as a Formal Language" (1970), "Universal Grammar" (1970) and "The Proper Treatment of Quantification in Ordinary English" (1973) proposed a model-theoretic formalism for English known as Montague Intensional Logic (IL). IL is a typed higher-order logic which uses finite types and finite-order functionals to formalize grammar categories of natural languages (in particular, English).

We study complexity issues and algorithmic aspects of objects and constructions of this theory (see [3-7]). Our approach is based on the Ershov-Scott theory of approximation spaces and domains within the framework of Σ-definability in admissible sets (J. Barwise, Yu.L. Ershov).

In model theory, there are many examples of structures and constructions with complex signatures: Morley and Skolem extensions, Marker expansions, Hrushovski construction, etc. On the other hand, in mathematical linguistics, words of a natural language are used as symbols (or signs) to denote entities, properties of entities, properties of properties of entities, etc. The set of these words, symbols or signs form a lexicon or a signature. This is not just a set, there is a certain structure on it, with relations of various arities. For example, each word has a grammar category (sometimes two or more), transitive verbs can posses monotonicity of different directions for different arguments, etc.

Let $\mathfrak{M}$ be a structure of a relational signature $\langle P_0^{n_0}, \ldots, P_k^{n_k} \rangle$ and let $\mathbb{A}$ be an admissible set. The definition below (due to Yu.L. Ershov) can be viewed as an effective version of the well-known model-theoretic notion of interpretability.

Definition 1. Structure $\mathfrak{M}$ is called Σ-*definable in* $\mathbb{A}$ if there are Σ-formulas $\varphi(x_0, y)$, $\psi(x_0, x_1, y)$, $\psi^*(x_0, x_1, y)$, $\varphi_0(x_0, \ldots, x_{n_0-1}, y)$, $\varphi_0^*(x_0, \ldots, x_{n_0-1}, y)$, $\ldots$, $\varphi_k(x_0, \ldots, x_{n_k-1}, y)$, $\varphi_k^*(x_0, \ldots, x_{n_k-1}, y)$ such that, for some parameter

$a \in A$, $M_0 \leftrightharpoons \varphi^{\mathbb{A}}(x_0, a) \neq \varnothing$, $\eta \leftrightharpoons \psi^{\mathbb{A}}(x_0, x_1, a) \cap M_0^2$ is a congruence relation on $\mathfrak{M}_0 \leftrightharpoons \langle M_0, P_0^{\mathfrak{M}_0}, \ldots, P_k^{\mathfrak{M}_0} \rangle$, where

$$P_k^{\mathfrak{M}_0} \leftrightharpoons \varphi_k^{\mathbb{A}}(x_0, \ldots, x_{n_k-1}) \cap M_0^{n_k},\ k \in \omega,$$

$$\psi^{*\mathbb{A}}(x_0, x_1, a) \cap M_0^2 = M_0^2 \setminus \psi^{\mathbb{A}}(x_0, x_1, a),$$

$$\varphi_i^{*\mathbb{A}}(x_0, \ldots, x_{n_i-1}, a) \cap M_0^{n_i} = M_0^{n_i} \setminus \varphi_i^{\mathbb{A}}(x_0, \ldots, x_{n_i-1})$$

for all $i \leqslant k$, and the structure $\mathfrak{M}$ is isomorphic to the quotient structure $\mathfrak{M}_0 / \eta$.

Σ-definability of a model in an admissible set $\mathbb{A}$ is an extension (on computability in $\mathbb{A}$) of the notion of constructivizability of a model (in classical computability theory).

For arbitrary structures $\mathfrak{M}$ and $\mathfrak{N}$, we denote by $\mathfrak{M} \leqslant_\Sigma \mathfrak{N}$ the fact that $\mathfrak{M}$ is Σ-definable in $\mathbb{HF}(\mathfrak{N})$, the least admissible set over $\mathfrak{N}$.

For a structure $\mathfrak{A}$, Σ-*jump of* $\mathfrak{A}$ (see [1,2]) is the structure

$$\mathfrak{A}' = (\mathbb{HF}(\mathfrak{A}), \Sigma\text{-Sat}_{\mathbb{HF}(\mathfrak{A})}).$$

In mathematical linguistics, one of the most important relations on notions and properties is a binary relation of "special case" ($\leqslant$): *cat* $\leqslant$ *animal*, *run* $\leqslant$ *move*, etc. Usually, for notions b_1 and b_2, relation $b_1 \leqslant b_2$ is expressed in natural language by sentences of kind "Every b_1 is b_2" or "All b_1 are b_2".

We construct structures of such kind within the framework of Σ-definability [1,2]. In particular, we present a series of generalized effective structures $\mathfrak{M}_{IL}$ and $\mathfrak{N}_{IL}$ such that

1) $\mathfrak{M}_{IL}$ is a model of Montague Intensional Logic;

2) $\mathfrak{N}_{IL}$ is a structure on the signature of $\mathfrak{M}_{IL}$ with the relation of "special case" ($\leqslant$), and

$$\mathfrak{N}_{IL} \leqslant_\Sigma \mathfrak{M}_{IL}''.$$

The research was supported by the IM SB RAS state assignment, project number FWNF-2022-0012.

References

[1] Yu.L. Ershov, V.G. Puzarenko, and A.I. Stukachev, HF-Computability, In S. B. Cooper and A. Sorbi (eds.): *Computability in Context: Computation and Logic in the Real World*, Imperial College Press/World Scientific (2011), 173-248.

[2] A.I. Stukachev, Effective model theory: an approach via Sigma-definability, *Lecture Notes in Logic*, 41 (2013), 164-197.

[3] A.S. Burnistov, A.I. Stukachev, On inner constructivizability of functional structures, *Algebra and Logic*, v. 61, N1 (2021), 23-41.

[4] A.I. Stukachev, Interval extensions of orders and temporal approximation spaces, *Siberian Mathematical Journal*, v. 62, N4 (2021), 894-910

[5] A.S. Burnistov, A.I. Stukachev, Generalized computable models and Montague semantics, *Studies in Computational Intelligence*, 1081 (2023), 107-124.

[6] A.S. Burnistov, A.I. Stukachev, Computable functionals of finite types in Montague semantics, *Siberian Electronic Mathematical Reports* (submitted).

[7] A.I. Stukachev, U.D. Penzina, Skolem functions and generalized quantifiers for negative polarity items semantics, *Lecture Notes in Networks and Systems*, 1198 (2025), 212-226.

ALGEBRAS FOR DEFINABLE AND TYPE-DEFINABLE SETS IN A STRUCTURE

S.V. Sudoplatov*

Sobolev Institute of Mathematics,
4, Acad. Koptyug avenue, Novosibirsk, 630090, Russia;
Novosibirsk State Technical University,
20, K.Marx avenue, Novosibirsk, 630073, Russia
e-mail: sudoplat@math.nsc.ru

1 Introduction

Relations form the basis of algebraic systems representing links between elements [1], in particular, operations by their graphs. Among all relations, definable relations/sets, defined by suitable formulae of a given signature, play an important role for the structural description [2, 3]. These relations/sets allow us to clarify the expressibility of certain properties through signature relations by means of logical connectives and quantifiers. Systems of definable structures forming univers studied in [4]. In addition to definable relations/sets, type-definable relations/sets are often used in model theory, represented both by a set of type realizations and by intersections of definable relations/sets [5, 6, 7, 8].

This paper examines possibilities for definable and type-definable sets in structures. It is clarified when a type-definable set is definable. Connections of type-definable sets with respect to Boolean combinations are studied. Algebras for definable and type-definable sets and their properties are studied, as well as the hierarchy of these algebras with respect to various sets of parameters. It is shown that type-definable sets of given arity form a distributive lattice which is a Boolean algebra iff each type-definable set is

*The work was carried out in the framework of the State Contract of the Sobolev Institute of Mathematics, Project No. FWNF-2022-0012, and partially supported by Committee of Science in Education and Science Ministry of the Republic of Kazakhstan, Grant No. AP19677451.

formulaically definable. Natural extensions of these lattices are defined, as well as lattices of derivative structures with respect to dynamics of families of type-definable sets over various sets of parameters. Some natural properties of these lattices are studied with respect to signatures and kinds of type-definable sets.

2 Definable and type-definable sets, their algebras

Throughout we consider complete first-order theories and their models.

For a structure $\mathcal{M}$ any subset $P \subseteq M^k$, for some natural k, is said to be a k-ary *property*, *set*, or *relation* in $\mathcal{M}$. Recall that a property P (in $\mathcal{M}$) is *formula definable*, *formulaically definable*, *definable by formula*, or simply *definable* in $\mathcal{M}$ over a set $A \subseteq M$, or A-*definable*, if there is a formula $\varphi = \varphi(\overline{x}, \overline{a})$, $\overline{a} \in A$, such that P is equal to the set $\varphi(\mathcal{M}, \overline{a}) = \{\overline{b} \mid \mathcal{M} \models \varphi(\overline{b}, \overline{a})\}$ of all solutions $\overline{b}$ of φ in $\mathcal{M}$. The formula φ is called *defining* for P in the structure $\mathcal{M}$.

Remark 2.1. Remind [9, 10, 11] that for any $k \in \omega$ and $A \subseteq M$ A-definable subsets of M^k form a Boolean algebra $\mathcal{D}_k^A(\mathcal{M})$, with respect to Boolean operations $\cup$, $\cap$, $\bar{\cdot}$, correspondent to Lindenbaum–Tarski algebra $\mathcal{LT}_k^A(\mathcal{M})$ which consists of equivalence classes $[\varphi(\overline{x})] = \{\psi(\overline{x}) \mid \mathcal{M} \models \forall \overline{x}(\varphi(\overline{x}) \leftrightarrow \psi(\overline{x}))\}$ of formulae $\varphi(\overline{x})$ in the language of $\mathcal{M}$ extended by constants in A, with k free variables in the tuple $\overline{x}$. The correspondence is defined by the isomorphism which maps each equivalence class $[\varphi(\overline{x})]$ to the set $\varphi(\mathcal{M})$ of the solutions of $\varphi(\overline{x})$ in $\mathcal{M}$. In particular, each $\mathcal{D}_k^A(\mathcal{M})$ is closed under Boolean combinations correspondent to equivalence classes of Boolean combinations of formulae $\varphi(\overline{x})$.

Definition. We say that an intersection of A-definable sets B_i, which are defined by formulae $\varphi(\overline{x}, \overline{a}_i)$, $i \in I$, are *consistent* if the set $\{\varphi(\overline{x}, \overline{a}_i), i \in I\}$ is consistent, i.e. it is satisfied in a model of given theory.

Consistent intersections Z of A-definable sets D in $\mathcal{M}$ are called *type-definable* over A or A-*type-definable*. Here we say that formulae $\varphi(\overline{x}, \overline{a})$ used for definable sets D *define* Z. These formulae form a type whose set of realizations in the given structure equals Z.

We denote by $\mathrm{TD}_k^A(\mathcal{M})$ the family of all k-ary A-type-definable sets in $\mathcal{M}$.

We omit the index A in $D_k^A(\mathcal{M})$ and $\mathrm{TD}_k^A(\mathcal{M})$ if the set A is fixed. Here the sets $D_k(\mathcal{M})$ and $\mathrm{TD}_k(\mathcal{M})$ consists of *definable* and *type-definable* sets of the arity k, respectively.

Remark 2.2. By the definition any nonempty A-definable set is A-type-definable, but not vice versa in general case, for instance, if a type is not isolated and it is realized in the given structure.

Proposition 2.3. *An A-type-definable set Z is formulaically A-definable iff either Z is empty, i.e. the correspondent type is omitted in the given structure, or Z is not empty and it is represented as a finite intersection of formulaically A-definable sets.*

Proof. If $Z = \emptyset$ then it is defined by an A-formula $\varphi \wedge \neg\varphi$. Now we assume that $Z \neq \emptyset$. If Z is A-definable then it is an intersection of itself, which is a finite intersection. Finite intersections of A-definable sets are again A-definable in view of Remark 2.1. If Z is not represented as a finite intersection of A-definable sets then it can not be A-definable by the definition. Here each finite intersection of supersets containing Z properly contains Z. □

Since finite intersections of A-definable sets are again A-definable we have the following:

Corollary 2.4. *An A-type-definable set Z is A-definable iff it is defined by a consistent A-formula which forces all formulae used to define Z.*

Proposition 2.5. *The complement $\overline{Z}$ of an A-type-definable set Z is A-definable iff Z is A-definable.*

Proof. If Z is A-definable then its complement $\overline{Z}$ is A-definable, too, in view of Remark 2.1. Conversely, if $\overline{Z}$ is A-definable then $\overline{\overline{Z}} = Z$ is again A-definable. □

Proposition 2.6. *Positive consistent Boolean combinations of A-type-definable sets are again A-type-definable.*

Proof. It suffices to note that for A-type-definable sets Z_1 and Z_2 their union $Z_1 \cup Z_2$ and intersection $Z_1 \cap Z_2$ are again A-type-definable. We take families D_i, $i \in I$, and D'_j, $j \in J$, of A-definable sets, whose intersections define Z_1 and Z_2, respectively. Now $Z_1 \cup Z_2$ is defined by the family of unions $D_i \cup D'_j$, and $Z_1 \cap Z_2$ by the intersections $D_i \cap D'_j$. □

Propositions 2.5 and 2.6, with Remark 2.1, immediately imply:

Theorem 2.7. 1. *Any structure $\mathcal{TD}^A_k(\mathcal{M}) = \langle \mathrm{TD}^A_k(\mathcal{M}) \cup \{\emptyset\}; \cup, \cap\rangle$ is a distributive lattice with the least element $\emptyset$ and the greatest element M^k.*

2. *Any lattice $\langle \mathrm{TD}^A_k(\mathcal{M}) \cup \{\emptyset\}; \cup, \cap\rangle$ forms a Boolean algebra iff*

$$\mathrm{TD}^A_k(\mathcal{M}) = D^A_k(\mathcal{M}).$$

Remark 2.8. Any lattice $\mathcal{TD}_k^A(\mathcal{M})$ is naturally extensible till a Boolean algebra $\mathcal{BTD}_k^A(\mathcal{M})$ by adding Boolean combinations of A-type-definable sets in $\mathrm{TD}_k^A(\mathcal{M})$, and this extension is proper iff $\mathrm{TD}_k^A(\mathcal{M})$ contains a (A-type-definable) set which is not formulaically A-definable. Moreover, this lattice is naturally embeddable into the lattice $\langle \mathrm{ITD}_k^A(\mathcal{M}); \cup, \cap \rangle$ obtained by adding positive Boolean combinations of finitely many and infinitely many A-type-definable sets in $\mathrm{TD}_k^A(\mathcal{M})$, and into the Boolean algebra $\mathcal{IBTD}_k^A(\mathcal{M})$ by adding results of set-theoretic unions, intersections and complements to the set $\mathrm{ITD}_k^A(\mathcal{M})$. The structures $\mathcal{ITD}_k^A(\mathcal{M})$ and $\mathcal{IBTD}_k^A(\mathcal{M})$ are derivative with respect to $\mathcal{TD}_k^A(\mathcal{M})$ and they inherit properties of $\mathcal{TD}_k^A(\mathcal{M})$.

3 Lattices for families of type-definable sets

Remark 3.1. By the definition any (type-)definable set is a set of solutions of some, possibly incomplete, type $p(\overline{\ }) \in S^{\subseteq}(A)$, where $A \subseteq M$.

It is easy to see that each property $P \subseteq M^k$, $k \in \omega$, is type-definable by the set of formulae $\neg \overline{x} \approx \overline{b}$, $\overline{b} \in M^k \setminus P$, i.e. any lattice $\mathcal{TD}_k^M(\mathcal{M})$ is a Cantor Boolean algebra. So in such a case, and for $\mathcal{TD}_k^A(\mathcal{M})$ with $A \subseteq M$ such that $\mathcal{TD}_k^A(\mathcal{M}) = \mathcal{TD}_k^M(\mathcal{M})$, each nonempty element is composed by singletons in this lattice which are atoms. Their complements are co-atoms such that each element $Z \subset M$ is represented as an intersection of co-atoms.

In general case the lattice $\mathcal{TD}_k^A(\mathcal{M})$ contains atoms correspondent to nonempty sets of realizations of complete k-types in $S(A)$, which form ultrafilters. These atoms correspond co-atoms iff these types are isolated, i.e. correspond to A-definable sets D. Thus the co-atoms have the form $\overline{D}$. If $\mathcal{M}$ does not realize isolated k-types in $S(A)$ then $\mathcal{TD}_k^A(\mathcal{M})$ does not have co-atoms.

For any structure $\mathcal{M}$ the lattices $\mathcal{TD}_k^A(\mathcal{M})$ form a hierarchy in the following way. If $A_1 \subseteq A_2 \subseteq M$ then $\mathcal{TD}_k^{A_1}(\mathcal{M})$ is a sublattice of $\mathcal{TD}_k^{A_2}(\mathcal{M})$ and this relation is strict iff A_2 gives more definable sets with respect to A_1. The family $\mathbf{TD}_k(\mathcal{M})$ collecting the lattices $\mathcal{TD}_k^A(\mathcal{M})$, marked by their sets A, forms a distributive lattice $\mathbf{LTD}_k(\mathcal{M}) = \langle \mathbf{TD}_k(\mathcal{M}); \vee, \wedge \rangle$, where

$$\mathcal{TD}_k^{A_1}(\mathcal{M}) \vee \mathcal{TD}_k^{A_2}(\mathcal{M}) = \mathcal{TD}_k^{A_1 \cup A_2}(\mathcal{M}),$$

$$\mathcal{TD}_k^{A_1}(\mathcal{M}) \wedge \mathcal{TD}_k^{A_2}(\mathcal{M}) = \mathcal{TD}_k^{A_1 \cap A_2}(\mathcal{M})$$

for any $A_1, A_2 \subseteq M$.

By the definition this lattice has the least element $\mathcal{TD}_k^{\emptyset}(\mathcal{M})$ and the greatest element $\mathcal{TD}_k^M(\mathcal{M})$. Its atoms are defined by singletons $\{a\}$, where $a \in M$.

This lattice is a fusion of Cantor Boolean algebra on $\mathcal{P}(M^k)$ and lattices $\mathcal{TD}_k^A(\mathcal{M})$. In fact, elements of that Boolean algebra are replaced by these lattices.

Definition. We say that a lattice $\mathbf{LTD}_k(\mathcal{M})$ admits a *regularization* $\mathbf{LTD}_k^r(\mathcal{M})$ if $\mathbf{LTD}_k^r(\mathcal{M})$ is a lattice satisfying the following conditions:

1) the universe $\mathbf{TD}_k^r(\mathcal{M})$ of $\mathbf{LTD}_k^r(\mathcal{M})$ consists of the lattices $\mathcal{TD}_k^A(\mathcal{M})$ without their labels A, i.e. $\mathbf{TD}_k^r(\mathcal{M})$ is the quotient of $\mathbf{TD}_k(\mathcal{M})$ under the equivalence relation $\sim$ identifying pairs $(\mathcal{TD}_k^{A_1}(\mathcal{M}), A_1)$ and $(\mathcal{TD}_k^{A_2}(\mathcal{M}), A_2)$ with $\mathcal{TD}_k^{A_1}(\mathcal{M}) = \mathcal{TD}_k^{A_2}(\mathcal{M})$;

2) the equivalence relation $\sim$ is the congruence relation producing lattice operations of $\mathbf{LTD}_k^r(\mathcal{M})$ by correspondent operations of $\mathbf{LTD}_k(\mathcal{M})$;

3) for any $A_1, A_2 \subseteq M$ the following equality holds:

$$\mathcal{TD}_k^{A_1}(\mathcal{M}) \wedge \mathcal{TD}_k^{A_2}(\mathcal{M}) = \mathcal{TD}_k^{A_1}(\mathcal{M}) \cap \mathcal{TD}_k^{A_2}(\mathcal{M}). \quad (1)$$

If $\mathbf{LTD}_k^r(\mathcal{M})$ exists then we say that $\mathbf{LTD}_k(\mathcal{M})$ is *regular*.

In any case the set $\mathbf{TD}_k^r(\mathcal{M})$ is supplied by the ordinary relation $\subseteq$, where $\mathcal{TD}_k^{A_1}(\mathcal{M}) \subseteq \mathcal{TD}_k^{A_2}(\mathcal{M})$ means that each A_1-type-definable k-ary relation is A_2-type-definable.

Here, for instance, $\mathcal{TD}_k^A(\mathcal{M})$ is an atom iff $\mathcal{TD}_k^A(\mathcal{M})$ is a proper extension of $\mathcal{TD}_k^\emptyset(\mathcal{M})$, i.e. it has a A-type-definable k-ary set which is not $\emptyset$-definable, and there are no A' such that $\mathcal{TD}_k^{A'}(\mathcal{M})$ is proper between $\mathcal{TD}_k^\emptyset(\mathcal{M})$ and $\mathcal{TD}_k^A(\mathcal{M})$, i.e. with an A'-type-definable k-ary set which is not $\emptyset$-definable, and with an A-type-definable k-ary set which is not A'-definable.

Recall [14] that a structure $\mathcal{M}$ is *syntactically* (respectively, *semantically*) *rigid* if $M = \mathrm{dcl}(\emptyset)$ ($|\mathrm{Aut}(\mathcal{M})| = 1$).

Clearly that any syntactically rigid structure is semantically rigid, but not vice versa in general.

The following proposition shows that syntactically rigid structures produce regular lattices $\mathbf{LTD}_k(\mathcal{M})$, but these lattices are trivial, without variations of $\mathcal{TD}_k^{A_1}(\mathcal{M})$. In such a case the lattices $\mathbf{LTD}_k(\mathcal{M})$, as derivative structures, do not give any essential structural information on the initial structure $\mathcal{M}$.

Proposition 3.2. *If $\mathcal{M}$ is a syntactically rigid structure then each lattice $\mathbf{LTD}_k(\mathcal{M})$ is a regular with the singleton lattice $\mathbf{LTD}_k^r(\mathcal{M})$.*

Proof. Since $M = \mathrm{dcl}(\emptyset)$, each tuple $\overline{a} \in M$ is definable, too. Using the arguments for Remark 3.1 we observe that each element of $\mathcal{P}(M^k)$ is $\emptyset$-type-definable, i.e. $\mathbf{LTD}_k(\mathcal{M})$ is formed by unique lattice with the universe $\mathcal{P}(M^k)$. Thus $\mathbf{LTD}_k(\mathcal{M})$ is regular with the singleton lattice $\mathbf{LTD}_k^r(\mathcal{M})$. $\square$

In contrast to Proposition 3.2, the following proposition asserts that the violation of syntactic rigidity, in the presence of an algebraic type, entails non-triviality of the lattice $\mathbf{LTD}_k(\mathcal{M})$ and violation of regularity.

Proposition 3.3. *If a structure $\mathcal{M}$ realizes a complete algebraic k-type $p(\overline{x})$ over $\emptyset$ with at least two realizations then any lattice $\mathbf{LTD}_k(\mathcal{M})$ is not regular.*

Proof. Let $k = 1$, $a_1, \ldots, a_n$ be all pairwise distinct realizations of $p(x)$, $n > 1$, k be a minimal cardinality such that each k-element subset of $p(\mathcal{M})$ defines each element a_i. By the conjecture we have $1 \leq m \leq n-1$. Clearly, the value m is invariant under automorphisms, which connect all elements of $p(\mathcal{M})$. We take a m-element set $A \subset p(\mathcal{M})$, elements $a \in A$ and $b \in p(\mathcal{M}) \setminus A$ we find an automorphism f (of an elementary extension) with $f(a) = b$. Then $|A \cap f(A)| < m$, i.e. $A \cap f(A)$ does not define some element $c \in p(\mathcal{M})$. Hence $\{c\} \in (\mathcal{TD}_1^A(\mathcal{M}) \cap \mathcal{TD}_1^{f(A)}(\mathcal{M})) \setminus \mathcal{TD}_1^{A \cap f(A)}(\mathcal{M})$ contradicting the regularity of $\mathbf{LTD}_k(\mathcal{M})$.

For arbitrary $k > 1$ we take an appropriate k-type $p(\overline{x})$ and repeat the arguments for the case $k = 1$, replacing elements by k-tuples. □

We denote by Σ^1 an arbitrary signature consisting of constant symbols c_i, $i \in I$, as well as 0-ary and unary predicate symbols P_j, $j \in J$.

Theorem 3.4. *Let $\mathcal{M}$ be a structure of a signature Σ^1. Then any lattice $\mathbf{LTD}_k(\mathcal{M})$ is regular iff $\mathcal{M}$ is semantically rigid.*

Proof. In view of [12, Section 8.1] formulae of any signature Σ^1 are represented by Boolean combinations of formulae describing numbers of elements in intersections of literas P^δ of unary predicates P, belonging of constants to these intersections, equalities and inequalities of constants, and satisfiability and unsatisfiability of zero-ary predicates. Thus definable sets are composed as Boolean combinations, Cartesian products and Cartesian sums for unary ones [13]. Considering structures $\mathcal{TD}_k^A(\mathcal{M})$ we just extend the set of language constants by elements of A.

If $\mathcal{M}$ is semantically rigid then by the described basedness of $\mathrm{Th}(\mathcal{M})$ there are no distinct tuples connected by automorphisms. i.e. having same type. It implies that each k-tuple in $\mathcal{M}$ is type-definable implying that $\mathcal{TD}_k^A(\mathcal{M})$ consists of all elements of $\mathcal{P}(M^k)$. Repeating the arguments for Proposition 3.2 we observe that the lattice $\mathbf{LTD}_k(\mathcal{M})$ is regular.

Conversely, if $\mathcal{M}$ is not semantically rigid, we find a complete k-type $p(\overline{x}) \in S(\emptyset)$, realized by several tuples, each of which without distinct coordinates. Now we take an appropriate set A such that $p(\overline{x})$ is extended till a complete type $q(\overline{x}) \in S(A)$ such that $q(\overline{x})$ has finitely many and at least two realizations in $\mathcal{M}$. Repeating the arguments for Proposition 3.3 we obtain the violation of regularity for the lattice $\mathbf{LTD}_k(\mathcal{M})$ □

Let $\mathbf{LTD}_k^{\mathrm{fin}}(\mathcal{M})$ be the restriction of a lattice $\mathbf{LTD}_k(\mathcal{M})$ to the family of sets $\mathcal{TD}_k^A(\mathcal{M})$ with finite A. Since these sets, for a signature Σ^1, can define only their subsets and complements inside definable sets, we have the following possibilities:

1) $\mathcal{M}$ is semantically rigid, with regular singletons $\mathbf{LTD}_k^{\mathrm{fin}}(\mathcal{M})$;

2) $\mathcal{M}$ has a complete 1-type over $\emptyset$ with finitely many and more then one realizations, violating the regularity of $\mathbf{LTD}_k^{\mathrm{fin}}(\mathcal{M})$;

3) any complete 1-types over $\emptyset$ has only one or infinitely many realizations in $\mathcal{M}$, producing the regularity of $\mathbf{LTD}_k^{\mathrm{fin}}(\mathcal{M})$.

Thus we have the following modification of Theorem 3.4:

Theorem 3.5. *Let $\mathcal{M}$ be a structure of a signature Σ^1. Then any lattice $\mathbf{LTD}_k^{\mathrm{fin}}(\mathcal{M})$ is regular iff any complete 1-type over $\emptyset$ has only one or infinitely many realizations in $\mathcal{M}$.*

Now we argue to show that the signature Σ^1 is essential for Theorem 3.5.

Lemma 3.6. *If a structure $\mathcal{M}$ has a $\emptyset$-definable equivalence relation E with at least two at least two-element E-classes whose elements are pairwise connected by automorphisms then $\langle \mathbf{TD}_1(\mathcal{M}); \vee, \wedge \rangle$ is not regular.*

Proof. Let Z be a $\emptyset$-type-definable set defined by a complete 1-types realized by the elements in the conjecture. We have pairwise distinct elements $a_1, a_2, a_3, a_4 \in Z$ such that $\models E(a_1, a_2) \wedge E(a_3, a_4) \wedge \neg E(a_1, a_3)$. The formulae $E(a_1, x)$ and $E(a_2, x)$ define the same proper subset of Z whereas Z does not have proper $\emptyset$-type-definable subsets. Thus, $E(a_1) = E(a_2) \in \mathcal{TD}_1^{\{a_1\}}(\mathcal{M}) \cap \mathcal{TD}_1^{\{a_2\}}(\mathcal{M})$ and $E(a_1) = E(a_2) \notin \mathcal{TD}_1^{\emptyset}(\mathcal{M})$, where $\emptyset = \{a_1\} \cap \{a_2\}$. Hence $\langle \mathbf{TD}_1(\mathcal{M}); \vee, \wedge \rangle$ is not regular. □

Using Lemma 3.6 we have the following:

Theorem 3.7. *For any signature Σ each lattice $\mathbf{LTD}_k^{\mathrm{fin}}(\mathcal{M})$, for a structure $\mathcal{M}$ of the signature Σ, without complete k-types over finite $A \subset M$ having $n \in \omega \setminus \{0, 1\}$ realizations, is regular iff Σ has the form Σ^1.*

Proof. If $\Sigma = \Sigma^1$ then each its lattice $\mathbf{LTD}_k^{\mathrm{fin}}(\mathcal{M})$, without without complete k-types over finite $A \subset M$ having $n \in \omega \setminus \{0, 1\}$ realizations, is regular by Theorem 3.6.

Otherwise, Σ has a n-ary predicate symbol P, $n \geq 2$, or a n-ary functional symbol f, $n \geq 1$. Now we reduce $P(x_1, x_2, \ldots, x_n)$ to binary one $E(x_1, x_2) = P(x_1, x_2, \ldots, x_2)$ and write the axioms for the conjecture of Lemma 3.6 violating the regularity of $\mathbf{LTD}_k^{\mathrm{fin}}(\mathcal{M})$. Having a functional symbol f we take the formula $E(x_1, x_2) = \exists y(f(x_1, \ldots, x_1) \approx y \wedge f(x_2, \ldots, x_2) \approx y)$ and again write the axioms for the conjecture of Lemma 3.6 violating the regularity of $\mathbf{LTD}_k^{\mathrm{fin}}(\mathcal{M})$. Thus in any case symbols P and f violate the regularity of $\mathbf{LTD}_k^{\mathrm{fin}}(\mathcal{M})$. □

References

[1] R. Fraïssé, Theory of relations. — Amsterdam : North-Holland, 1986. — 451 p.

[2] D. Marker, Model Theory: An Introduction. — New York : Springer-Verlag, 2002. — Graduate texts in Mathematics. — Vol. 217. — 342 p.

[3] S.V. Sudoplatov, Formulas and properties, their links and characteristics // Mathematics. — 2021. — Vol. 9, Issue 12. — 1391. 16 p.

[4] B. Poizat, A la recherche de la structure intrinsèque de l'univers // Model Theory in Kazakhstan: Collection of scientific works dedicated to the memory of A.D. Taimanov. — Almaty : Eco Sudy, 2006, 448 p. — P. 341–388.

[5] A. Pillay, Stable theories, pseudoplanes and the number of countable models // Ann. Pure and Appl. Logic. — 1989. — Vol. 43, No. 2. — P. 147–160.

[6] S.V. Sudoplatov, Type reduction and powerful types // Siberian Math. J. — 1992. — Vol. 33, No. 1. — P. 125–133.

[7] C. Milliet, On enveloping type-ddefinable structures // The Journal of Symbolic Logic. — 2011. — Vol. 76, No. 3. — P. 1023–1034.

[8] A. Martin-Pizarro, D. Palacín, Stabilizers, Measures and IP-sets // arXiv:1912.07252v5 [math.LO], 2024. — 14 p.

[9] S.J. Surma, On the Origin and Subsequent Applications of the Concept of the Lindenbaum Algebra // Logic, Methodology and Philosophy of Science VI, Proceedings of the Sixth International Congress of Logic, Methodology and Philosophy of Science. Studies in Logic and the Foundations of Mathematics. — 1982. — Vol. 104. — P. 719–734.

[10] A. Tarski, Logic, Semantics, and Metamathematics — Papers from 1923 to 1938 // Ed. J. Corcoran. — Hackett Pub. Co., 1983.

[11] W.J. Blok, D. Pigozzi, Algebraizable logics // Memoirs of the AMS. — 1989. 77 (396).

[12] Yu.L. Ershov, E.A. Palyutin, Mathematical logic. — Moscow : Fizmatlit, 2011. — 356 p. [in Russian]

[13] S.V. Sudoplatov, Arities and arizabilities of first-order theories // Siberian Electronic Mathematical Reports. — 2022. — Vol. 19, No. 2. — P. 889–901.

[14] S.V. Sudoplatov, Variations of rigidity // Bulletin of Irkutsk State University. Series Mathematics. — 2024. — Vol. 47. — P. 119–136.

РАНГИ ЭКВАЦИОНАЛЬНОСТИ ДЛЯ СЕМЕЙСТВ ФОРМУЛ

А.В. Васенёва

Новосибирский государственный университет,
ул. Пирогова, 1, Новосибирск, Россия
e-mail: a.vaseneva@g.nsu.ru

В работе рассматривается обобщение ранга нётеровости [1] до ранга эквациональности, применимого к эквациональным теориям [2].

Определение. Семейство C подмножеств множества X называется *нётеровым*, если оно удовлетворяет следующим двум условиям:

1) C замкнуто относительно конечных пересечений и содержит само множество X;

2) C имеет условие нисходящей цепи (DCC): любая нисходящая цепь $C_0 \supset C_1 \supset \ldots \supset C_n \supset \ldots$, где $C_n \in C$ для $n \in \omega$, стабилизируется на некотором конечном шаге, то есть найдется $n_0 \in \omega$ такой, что для любого $n \geq n_0$ выполнено $C_{n+1} = C_n$.

Элемент C_0 из семейства C называется *неприводимым*, если он не является пустым и не может быть представлен в виде конечного объединения $C_0 = C_1 \cup C_2 \cup \ldots \cup C_n$, где каждый C_k строго содержится в C_0 и принадлежит C, $k \geq 1$.

Определение. [1] Пусть C — нётерово семейство подмножеств множества X. Определим порядковый ранг $Rk_C(Y)$ для каждого подмножества Y из X следующим образом. Для неприводимых множеств C это фундаментальный ранг, то есть:

1. $Rk_C(C) \geq 0$ выполнено всегда;
2. $Rk_C(C) \geq \alpha + 1$ тогда и только тогда, когда $Rk_C(D) \geq \alpha$ для некоторого неприводимого $D \subsetneq C$;
3. $Rk_C(C) \geq \alpha$ с предельным ординалом α тогда и только тогда, когда $Rk_C(C) \geq \beta$ для каждого β меньше α.

Также ранг замкнутого множества — это наибольший ранг его неприводимых компонент, а ранг пустого множества определим $Rk_C(\emptyset) = -\infty$.

Пусть T — произвольная полная теория, M — модель теории T, $\varphi(x, a)$ — формула теории T с набором параметров $a \in M$, Δ — множество формул теории T.

Определение. Будет говорить, что формула $\varphi(x, y)$ является *уравнением*, если совокупность конечных пересечений копий $\varphi(M, a)$ формулы $\varphi(x, y)$ имеет DCC. Теория T *эквациональна*, если каждая формула теории T эквивалентна булевой комбинации уравнений.

Определение. *Рангом эквациональности* $\mathrm{ER}(\varphi(x, a))$ формулы $\varphi(x, a)$ (относительно модели M) называется минимальная длина вложенных цепей пересечений $\bigcap\limits_i \varphi(M, a_i)$, в которые входит $\varphi(M, a)$. По определению любое значение $\mathrm{ER}(\varphi(x, a))$ либо конечно, либо является бесконечным ординалом, зависящим от модели M. *Рангом эквациональности* семейства формул Δ будем называть величину $\mathrm{ER}(\Delta) = \sup\{\mathrm{ER}(\varphi(x, a)) \mid \varphi(x, y) \in \Delta, a \in M, l(a) = l(y)\}$.

Примеры. 1. Формулы $x = c$, задающие константы, всегда имеют ранг эквациональности, равный 1.

2. Атомные формулы $P(x)$ одноместных предикатов P также всегда имеют ранг эквациональности, равный 1.

3. Линейные порядки дают конечное значение ранга эквацинальности тогда и только тогда, когда они являются конечными. При этом формулы $x \leq y$ позволяют реализовать произвольные конечные ранги эквациональности.

4. Рассмотрим ациклический граф, обозначим через $Q(x, y)$ множество вершин $x \in M$ в которые можно попасть из вершины y. Пусть $Q(M, b) = \{a_1, a_2\}$, $Q(M, a_1) = \{b, c_1, c_2\}$, $Q(M, a_2) = \{b, c_3\}$. Нетрудно заметить, что ранг эквациональности для ациклических графов всегда будет равен 1.

Определение. *Рангом эквациональности* типа $p \in S(A)$ называется величина $\mathrm{ER}(p) = \sup\{\mathrm{ER}(\varphi(x, a)) \mid \varphi(x, y) \in p, a \in A, l(a) = l(y)\}$.

Следующее определение дает эквивалентную переформулировку понятий уравнения и эквациональной теории из работы [2].

Определение. Формула $\varphi(x, y)$ теории T называется *уравнением*, если каждая формула $\varphi(x, a)$ имеет конечный (и ограниченный при подстановке параметров a) ранг эквациональности. Теория T называется *эквациональной*, если любая формула теории T является T-эквивалентной некоторой булевой комбинации формул из Δ, где Δ состоит из уравнений.

Определение [3]. Теория T называется Δ-*базируемой*, где Δ — некоторое множество формул без параметров, если любая формула теории T эквивалентна в T некоторой булевой комбинации формул из Δ.

Для Δ-базируемых теорий T также говорят, что T имеет *элиминацию* или *сокращение кванторов* с точностью до множества Δ.

Теорема 1. 1. *Для любого натурального $n \geq 1$ существует Δ_n-базируемая эквациональная теория T_n, для которой* $\mathrm{ER}(\Delta_n) = n$.

2. *Для любого положительного ординала α существует Δ_α-базируемая теория T с моделью M_α такая, что* $\mathrm{ER}(\Delta_\alpha) = \alpha$ *относительно модели M_α.*

Доказательство. 1. Рассмотрим двудольный граф $G = (X, Y, E)$, X и Y — доли двудольного графа. Обозначим через $Q(x, y)$ множество вершин $x \in X$ в которые можно попасть из вершины y. Для $n = 1$ достаточно рассмотреть граф, в котором для любого $y \in Y$ существует единственный $x \in X$ такой, что y и x — смежные вершины G, так как $\forall y_1, y_2 \in Y\ Q(M, y_1) \cap Q(M, y_2) = \emptyset$ и $\forall y \in Y\ |Q(M, y)| = 1$.

Для $n = k+1$ построим граф следующим образом. Пусть $Q(M, y_1) = \{x_1, x_2, \ldots, x_{k+1}\}$, $Q(M, y_2) = \{x'\} \cup Q(M, y_1) \setminus \{x_{k+2}\}$, где $x' \notin Q(M, y_1)$, то есть для каждой следующей вершины y_{i+1} множество $Q(M, y_{i+1})$ строим из $Q(M, y_i)$ путем удаления одного из элементов множества $Q(M, y_i) \cap Q(M, y_1)$ и добавления одного нового элемента $x \in X$, $1 \leq i \leq k$. При таком построении пересечение $Q(M, y_1) \cap Q(M, y_2) \cap \ldots \cap Q(M, y_{k+1})$ состоит из одного элемента $\{x_{j_1}\}$, а ранг будет в точности равен $n = k + 1$.

2. Рассмотрим отношение $R(x, a)$, заданное формулой $\neg x \approx a$. Пусть b — некоторый кортеж $b_1, b_2, \ldots, b_k$ из M_α , множество экземпляров формулы $\varphi_k(x, y)$ задается как $\{x : \neg x \approx y, l(y) = k\}$, где $1 \leq k \leq \alpha$. Тогда $\Delta_\alpha = \{\varphi_k(x, b) : l(b) = k, b \in M, 1 \leq k \leq \alpha\}$. По построению $\mathrm{ER}(\Delta_\alpha) = \alpha$.

Замечание. Теория T эквациональна тогда и только тогда, когда для каждого конечного множества Δ_0 формул теории T существует конечное множество Δ_1 формул теории T такое, что $\mathrm{ER}(\Delta_1) \in \omega$ и любая формула из Δ_0 T-эквивалентна некоторой булевой комбинации формул из Δ_1.

Определение. *Рангом эквациональности* $\mathrm{ER}(T)$ теории T называется величина $\mathrm{ER}(T) = \inf_\Delta\{\sup\{\mathrm{ER}(\varphi(x, a)) \mid \varphi(x, y) \in \Delta, a \in M, l(a) = l(y)\}\}$.

Рассматриваются семейства формул Δ такие, что они дают Δ-базируемость теорий.

Опишем поведение рангов эквациональности в теориях графов. Для этого рассмотрим $Q(M, x)$ – множество вершин графа, в которые можно попасть из вершины x, для нескольких случаев:

1. Ациклические графы. Ранг эквациональности для ациклических графов всегда будет равен 1 (показали в примере 4).

2. Циклические ориентированные графы. Рассмотрим граф, в котором $Q(M,a) = \{b_1, b_2, a\}$, $Q(M,b_1) = \{c_1, c_2, b_1\}$, $Q(M,b_2) = \{c_3, b_2\}$, $Q(M,c_i) = \{c_i\}$, $i = 1,2,3$. Для двух смежных вершин y и z (ребро графа из y в z) имеем $Q(M,y) \cap Q(M,z) = \{z\}$, для несмежных вершин такое пересечение будет давать пустое множество. Отсюда ранг эквациональности для циклических ориентированных графов всегда будет равен 2.

3. Циклические неориентированные графы. Рассмотрим граф, в котором $Q(M,a) = \{b_1, b_2, a\}$, $Q(M,b_1) = \{c_1, c_2, b_1, a\}$, $Q(M,b_2) = \{c_3, b_2, a\}$, $Q(M,c_i) = \{c_i, b_1\}$, $i = 1,2$, $Q(M,c_3) = \{c_3, b_2\}$. Для трех вершин y, z и k таких, что смежными являются y и z, z и k имеем $Q(M,y) \cap Q(M,z) \cap Q(M,k) = \{z\}$. Тогда ранг эквациональности для циклических неориентированных графов, у которых минимум 3 вершины, всегда будет равен 3.

4. Полные графы. Пусть $\{a_1, ..., a_n\}$ – множество вершин полного графа. При взятии пересечений $Q(M,a_i) \cap Q(M,a_j)$ получим все множество вершин графа без вершин a_i и a_j. Таким образом ранг эквациональности для полных графов с n вершинами будет равен $n-1$.

5. Двудольные графы. В доказательстве Теоремы 1 был использован способ построения двудольного графа так, что для любого натурального n ранг эквациональности равен n.

Таким образом Теорему 1 можно переформулировать для теорий графов.

Теорема 2. *Для любого натурального $n \geq 1$ существует Δ_n-базируемая эквациональная теория графов T_n, для которой* $\mathrm{ER}(\Delta_n) = n$.

Список литературы

[1] A. Martin-Pizarro, M. Ziegler, Noetherian theories, arXiv:2307.16826v1 [math.LO], 2023.

[2] A. Pillay, G. Srour, Closed sets and chain conditions in stable theories // Journal of Symbolic Logic. — 1984. — Vol. 49. — P. 1350–1362.

[3] Y. Zaffe, E.A. Palyutin, S.S. Starchenko, Models of superstable Horn theories // Algebra and logic. — 1985. — T. 24, No 3. — C. 278–326.

Abstracts

H. Alhussein, P.S. Kolesnikov, *Hochschild cohomology of the Weyl conformal algebra.*

We compute Hochschild cohomology groups of the Weyl conformal algebra and of the universal conformal envelope $U(3)$ of the Virasoro conformal algebra.

G. Czédli, *Four generators of an equivalence lattice with consecutive block counts.*

For an integer $r > 1$, let $B_{r,0}$ denote the $(2^r + 1)$-element lattice that we obtain from the 2^r-element Boolean lattice by adding a new least element to it. For another integer $k \geq 2$, let $n = n(r, k)$ be the smallest integer such that the k-th direct power $B_{r^k,0}$ of $B_{r,0}$ can be generated by n elements. Motivated by the applicability of large lattices with small generating sets in authentication and cryptology, we give a lower estimate of $n(r, k)$ and an upper estimate of $n(4, k)$. (For $r < 4$, lower estimates have been known.) To reach this goal, we prove a Sperner (type) theorem. With our estimates, we can efficiently determine $n(4, k)$ for most k's up to about $k \leq 10^{299}$; for the rest of k's of this magnitude, we can give two consecutive integers such that $n(4, k)$ is one of them. For example, if $k = 10^{299}$, then $n(4, k) = 1001$.

D.Y. Emelyanov, *Algebras of binary isolating formulas for Cartesian products of graphs.*

We describe in more details the algebras for Cartesian products of graphs.

I.B. Kozhukhov, D.S. Khramchenok, *On axiomatizability of the class of subdirectly irreducible acts over semigroups.*

Let K be a class of all subdirectly irreducible act over a semigroup S. We prove that if the class K is axiomatizable then $|X| \leq 2^{|S^1|}$ for any $X \in K$. Similar inequality is proved for modules over associative rings. Further, we establish that if K is axiomatizable then $|X| \leq n$ for some natural n and all $X \in K$. Finally, we prove that for S being a group the class K is axiomatizable if and only if S is finite.

B.Sh. Kulpeshov, In.I. Pavlyuk, S.V. Sudoplatov, *On pseudo-strongly-minimal formulae, structures and theories.*

Possibilities for approximations of structures and theories by strongly minimal ones are studied.

S.B. Malyshev, *Heritability of pregeometry types by composition relative to the original structures.*

We investigate how the pregeometry that arises from the composition of two structures of a predicate signature inherits the types of pregeometries of the original structures. We establish that in the case of degeneracy, modularity, and local finiteness of the pregeometry of a graph signature, the pregeometry of their composition inherits the corresponding properties. We also provide counterexamples to the converse statement.

A.S. Monastyreva, *The zero-divisor graph of a finite ring.*

We discuss our results concerning the zero-divisor graph of a finite ring. Also, the report is devoted to the main problems and direction of investigations in this area.

B. Poizat, *Parameters in the algebraically closed fields.*

We study the influence of the parameters necessary in the definition of a given structure S definable in an algebraically closed field K, principally on the relations between the group of automorphisms of S and the group of automorphisms of K.

N.L. Polyakov, *On the RK-preorder on C-cones of RK-minimal ultrafilters.*

We describe the Rudin-Keisler preorder on the lower cones of RK-minimal ultrafilters with respect to the Comfort preorder.

A.P. Pozhidaev, *Pre-Lie Witt doubles.*

Let $\mathcal{A}$ be a finite-dimensional associative commutative algebra with a nonzero derivation d over an algebraically closed field F, let $\mathcal{A}$ be d-simple and it not be a field. Modulo the automorphisms of $\mathcal{A}$, which are almost commuting with d, the automorphisms are described of the left-symmetric Witt doubles $\mathcal{A}_d$ and $W_d(\mathcal{A})$ over F.

M.N. Rudometkina, A.V. Chekhonadskikh, *Algebra of finite predicates and flexible processes modeling.*

The survey is devoted to finite predicate tools designed for modeling of artificial intelligence systems. Such systems are used in various areas of practice from complex branched technological processes or business schemes to programs analyzing texts composed of heterogeneous material. We consider the main features of logical networks as a means of parallelizing tasks

while artificial intelligence systems proceed symbolic information. The paper emphasizes process mining abilities as an construction instrumentation of discrete process models based on the structuring of their logs (i.e. traces of its execution with time marks). The authors' attention is drawn to the presentation and modeling of flexible processes for information resources transforming, the scope of which covers software development, information web-search, text and metatext analysis, business processes, engineering design automation. Construction of flexible process models based on log analysis using finite predicate algebra is especially relevant in the identification and design of engineering systems.

A.S. Savin, *Some spectra of spherical orderability of finite groups.*

We describe spectra of spherical orderability for some natural finite groups using an algorithm checking possibilities of coordinated orderability for dimensions at least 3.

M. Shahryari, *On conjugately separability of nilpotent subgroups and equational domains: a survey.*

In this survey, we report some generalizations of Conjugate Separable Abelian Groups and Commutative Transitive Groups. These ideas are generalized in different directions by many people and still can be studied in very extended frames. We review some of the recent progress of this study and its applications.

N.A. Shchuchkin, *Ternary groupoids, closely related to ternary quasigroups.*

We construct an algorithm for transforming words using a set of Latin squares or multiplication tables of groupoids close to quasigroups, in a quantity equal to the number of alphabet symbols. Some properties of ternary groupoids close to ternary quasigroups are given. These properties play an important role in the analysis and design of cryptographic schemes based on the algebras indicated, such as polynomial completeness, the absence of nontrivial congruences.

D.V. Solomatin, *Structure of semigroups admitting generalized outerplanar Cayley graphs.*

We investigate how do the properties of outerplanarity and generalized outerplanarity of Cayley graphs of planar semigroups correlate.

A.A. Stepanova, E.L. Efremov, S.G. Chekanov, *T-pseudofinite acts over abelian groups.*

We introduce the notion of T-pseudofiniteness for a model of a theory T and consider T-pseudofinite acts over group. A model $\mathcal{M}$ of a theory T is called T-pseudofinite if every sentence true in $\mathcal{M}$ has a finite model which is a model of T. It is clear that for every theory T, if a model $\mathcal{M}$ of this theory is T-pseudofinite then $\mathcal{M}$ is pseudofinite, and if a model $\mathcal{M}$ of T is pseudofinite and T is a finite axiomatizable theory then $\mathcal{M}$ is T-pseudofinite. We give necessary and sufficient conditions for T-pseudofiniteness of acts over a group G with a finite number of subgroups of finite index, where T is the theory of all G-acts. As a consequence, we obtain a description of T-pseudofinite acts over divisible group. We show that every G-act is T-pseudofinite, where G is the group of integers.

A.I. Stukachev, *Structures on signatures of structures.*

We present a series of generalized effective models of Montague Intensional Logic, together with natural structures on their signatures, and discuss complexity issues of these structures.

S.V. Sudoplatov, *Algebras for definable and type-definable sets in a structure.*

We study possibilities for algebras of definable and type-definable sets in a given structure. Lattices for families of type-definable sets are defined and some their structural properties are described.

A.V. Vaseneva, *Equational ranks for families of formulae.*

We consider a generalization of Noetherian rank till the equational rank which is applied for equational theories. Values of the equational rank are obtained.

Contents

MODEL THEORY AND ALGEBRA 2024

Collection of papers

Edited by *M. Shahryari, S.V. Sudoplatov*

Technical editor *S.V. Sudoplatov*

Подписано в печать 07.11.2024
Формат 70 × 108 1/16. Бумага офсетная
Уч.-изд. л 17,5. Печ. л. 12,5. Тираж 50 экз.
Изд. № 179. Заказ № 214

Налоговая льгота – Общероссийский классификатор продукции
Издание соответствует коду 95 3000 ОК 005-93 (ОКП)

Издательство Новосибирского государственного
технического университета
630073, г. Новосибирск, пр. К. Маркса, 20
Тел. (383) 346-31-87
E-mail: office@publish.nstu.ru

Отпечатано в типографии
Новосибирского государственного технического университета
630073, г. Новосибирск, пр. К. Маркса, 20