Федеральное государственное бюджетное учреждение науки
Институт математики им. С. Л. Соболева
Сибирского отделения Российской академии наук

Федеральное государственное автономное образовательное
учреждение высшего образования
«Новосибирский национальный исследовательский государственный
университет»

Международная конференция

МАЛЬЦЕВСКИЕ ЧТЕНИЯ

посвященная 75-летию Ю. Л. Ершова

3–7 мая 2015 г.

Тезисы докладов

РФФИ Конференция проведена при финансовой поддержке
Российского фонда фундаментальных исследований
(код проекта 15-01-20155)

Новосибирск • 2015

Sobolev Institute of Mathematics

Novosibirsk State University

International Conference

MAL'TSEV MEETING

dedicated to 75th anniversary of Yuriĭ L. Ershov

May 3–7, 2015

Collection of Abstracts

РФФИ

Supported by
Russian Foundation for Basic Research
(grant 15-01-20155)

Novosibirsk • 2015

Содержание

I. Пленарные доклады

Структурная теория степеней неразрешимости: достижения и открытые проблемы

М. М. Арсланов

В докладе предполагается изложить некоторые важные и интересные достижения последних лет в разработке структурной теории степеней неразрешимости, а также описать наиболее серьезные проблемы, все еще ждущие своего решения.

Казанский (Приволжский) федеральный университет, Казань
E-mail: Marat.Arslanov@kpfu.ru

Алгебраические структуры и конструкции, связанные с косами

В. В. Вершинин

В докладе предполагается сделать обзор алгебраических объектов, связанных с косами, и возникающих при их изучении. Такими объектами являются, например, различные обобщения классических кос: косы на поверхностях, виртуальные косы, косы с особенностями, инверсный моноид частичных кос. Среди конструкций важную роль играет сопоставление алгебры Ли группе крашеных кос по ее нижнему центральному ряду. Эта конструкция используется, в частности, для построения инвариантов конечного типа для групп кос.

ИМ СО РАН, Новосибирск
E-mail: versh@math.nsc.ru

Индексные множества и вычислимость алгебраических структур

И. Ш. Калимуллин

Доклад посвящен ряду результатов и вопросов об алгоритмической сложности индексных множеств в различных нумерациях алгебраических структур и семейств вычислимо перечислимых множеств. Исследуемые в докладе задачи неожиданным образом возникают как при изучении степеней представлений алгебраических структур, так и при описании допустимых множеств, в которых заданная алгебраическая структура имеет Σ-определимое представление.

Казанский (Приволжский) федеральный университет, Казань
E-mail: Iskander.Kalimullin@ksu.ru

Нильтреугольные подалгебры алгебр Шевалле и их обобщения: идеалы и автоморфизмы

В. М. Левчук

Алгебру Шевалле над полем K, ассоциированную с системой корней Φ, характеризуют базисом Шевалле; его дают база подалгебры Картана и элементы e_r $(r \in \Phi)$ [**1**, § 4.4]. Подалгебру $N\Phi(K)$ с базой $\{e_r \mid r \in \Phi^+\}$ называем *нильтреугольной*. Для типа A_{n-1} ее отождествляют с ассоциированной алгеброй Ли $\Lambda(R)$ алгебры $R = NT(n, K)$ нильтреугольных $n \times n$ матриц. В [**2**] алгебры Ли $N\Phi(K)$ классических типов A_{n-1}, B_n, D_n и C_n представлены специальными матрицами с базисом из матричных единиц e_{iv}, где $i \leq n$ и, соответственно,

$$1 \leq v < i, \quad -i < v < i, \qquad 1 \leq |v| < i, \qquad -i \leq v < i,\ v \neq 0.$$

Структурные константы выписаны по теореме Шевалле о базисе в [**2**, Лемма 2].

Канонический базис лиева идеала алгебры $NT(n, K)$ находит Н.Д. Ходюня, решая задачу 2 из [**3**] о числе идеалов алгебр Ли $N\Phi(K)$ с конечным полем K.

Унипотентный радикал $U = U\Phi(K)$ подгруппы Бореля группы Шевалле типа Φ над K представлен в [**2**] присоединенной группой $N\Phi(K)$. Ее нормальные подгруппы тесно связаны с идеалами кольца Ли $N\Phi(K)$ и при $char\ K \neq 2, 3$ образуют даже совпадающие множества. Автор и Г.С. Сулейманова ранее перечислили большие нормальные абелевы подгруппы в U конечных групп G лиева типа и доказали, что их $(Aut\ G)$-образы в U дают все большие абелевы подгруппы в U, за некоторыми исключениями. Мы находим абелевы подалгебры наивысшей размерности в $N\Phi(K)$ с любым полем K; случай $K = C$ см. А.И. Мальцев [**4**]. А.В. Литаврин переносит решение в [**2**] проблемы описания $AutU$ на $AutN\Phi(K)$. Автоморфизмы финитарных обобщений групп U классических типов см. [**6**].

На введенные в [**6**] финитарные обобщения колец Ли $N\Phi(K)$ типов B_Γ, C_Γ и D_Γ для любой цепи Γ удается перенести методы [**5**]. База $\{e_{ij} \mid i, j \in \Gamma,\ i > j\}$ дает финитарное обобщение $R = NT(\Gamma, K)$. Когда кольцо K без делителей нуля, в [**5**] взаимосвязано описаны максимальные абелевы идеалы и автоморфизмы колец R и $\Lambda(R)$ и автоморфизмы присоединенной группы. Оказывается, в случае цепи Γ натуральных чисел все нильтреугольные Γ-матрицы над K дают также радикальное кольцо. На него удается перенести (автор и В. В. Цыганков) методы и результаты [**5**]. Случай поля $|K| > 2$ исследует Р.Словик [**7**].

Список литер туры

[1] *Carter R.* Simple groups of Lie type, Wiley and Sons, New York, 1972.

[2] *Левчук В. М.* Автоморфизмы унипотентных подгрупп групп Шевалле. - Алгебра и логика, т. 29 (1990), No. 3, с. 315-338.

[3] *Egorychev G. P., Levchuk V. M.* Enumeration in the Chevalley algebras. - ACM SIGSAM Bulletin, Vol 35, No. 2, 2001, p. 439-452.

[4] *Mal'cev A. I.* Commutative subalgebras in semisimple Lie algebras. - Izv. Akad. Nauk SSSR. Ser. Mat. 8 (1945) 291-300.

[5] *Левчук В. М.* Некоторые локально нильпотентные кольца и их присоединенные группы. - Математические заметки. 1987. T.42. No. 5. C. 631-641

[6] *Levchuk V. M., Suleimanova G. S.* Automorphisms and Normal Structure of Unipotent Subgroups of Finitary Chevalley Groups. - Proceed. Steklov Inst. Math., 3(2009), p. 118-127.

[7] *Slowik R.* Bijective maps of infinite triangular and unitriangular matrices preserving commutators. - Linear and Multilinear Algebra. 2013. Vol. 61. No. 8. P. 1028-1040.

Сибирский федеральный университет, Красноярск
E-mail: vlevchuk@sfu-kras.ru

Сильно регулярные графы с неглавным собственным значением 4 и их расширения

А. А. Махнев

Мы рассматриваем неориентированные графы без петель и кратных ребер. Для вершины a графа Γ через $\Gamma_i(a)$ обозначим i-окрестность вершины a, то есть, подграф, индуцированный Γ на множестве всех вершин, находящихся на расстоянии i от a. Подграф $\Gamma(a) = \Gamma_1(a)$ называется окрестностью вершины a и обозначается $[a]$, если граф Γ фиксирован.

Дж. Кулен предложил задачу изучения дистанционно регулярных графов, в которых окрестности вершин — сильно регулярные графы с неглавным собственным значением $\leq t$ для данного натурального числа t. Заметим, что сильно регулярный граф с нецелым собственным значением является графом в половинном случае, а вполне регулярный граф, в котором окрестности вершин — сильно регулярные графы в половинном случае, либо имеет диаметр 2, либо являеься графом Тэйлора. Таким образом, задача Кулена может быть решена пошагово для $t = 1, 2, \dots$.

Ранее было получено решение задачи Кулена для $t = 3$ (Махнев А.А., Падучих Д.В. и др. [**1**]-[**3**]). В докладе будет изложена программа изучения дистанционно регулярных графов, в которых окрестности вершин — сильно регулярные графы с неглавным собственным значением r, $3 < r \leq 4$.

Список литер туры

[1] *Карданова М. Л., Махнев А. А.* О графах, в которых окрестности вершин являются графами, дополнительными к графу Зейделя, Доклады академии наук 2010. Т. 434, N 4. С. 447–449.

[2] *Белоусов И. Н., Махнев А. А., Нирова М. С.* Дистанционно регулярные графы, в которых окрестности вершин сильно регулярны с собственным значением 2, Доклады академии наук 2012. Т. 447, N 5. С. 475–478.

[3] *Махнев А. А., Падучих Д. В.* Дистанционно регулярные графы, в которых окрестности вершин сильно регулярны с собственным значением 3, Доклады академии наук 2014. Т. 458, N 2. С. 275–278.

Институт математики и механики УрО РАН (Екатеринбург)
E-mail: makhnev@imm.uran.ru

Первичные вырожденные алгебры

С. В. Пчелинцев

Известны классические теоремы о строении первичных невырожденных алгебр в многообразиях альтернативных алгебр (М. Слейтер), $(-1,1)$-алгебр (И. Хенцель) и йордановых алгебр (Е. И. Зельманов). Проблема о существовании первичных вырожденных алгебр в указанных многообразиях была положительно решена докладчиком. Построенные примеры были названы К. МакКриммоном монстрами. Позже Ю. Медведев, Е. И. Зельманов и И. П. Шестаков указали новые примеры монстров.

Доказано, что построенные $(-1,1)$-монстры над полем характеристики 0 изоморфны; аналогично обстоит дело и в случае йордановых алгебр над полем характеристики 0. Указана также связь монстров с супералгебрами векторного типа и алгебрами Грассмана. Многообразия, порожденный $(-1,1)$ и йордановыми монстрами, являются минимальными многообразиями, содержащими первичные вырожденные алгебры (эти результаты получены совместно с И. П. Шестаковым).

Доказано, что всякая первичная вырожденная альтернативная алгебра A удовлетворяет 2-ому условию Энгеля; структура алгебры A определяется заданием «коммутатора» на подходящей первичной коммутативной альтернативной алгебре.

Для альтернативных алгебр доказано, что существует бесконечно много неизоморфных первичных коммутативных алгебр, а также указаны бесконечные серии тождеств, различающих первичные некоммутативные алгебры.

Финансовый университет при Правительстве Российской Федерации, Москва
E-mail: pchelinzev@mail.ru

Autostability and decidable structures

N. A. Bazhenov, S. S. Goncharov, M. I. Marchuk

A structure $\mathcal{A}$ is autostable relative to strong constructivizations if $\mathcal{A}$ has a decidable copy $\mathcal{B}$ and, for every decidable copy $\mathcal{C}$ of $\mathcal{A}$, there is a computable isomorphism f from $\mathcal{B}$ onto $\mathcal{C}$. In this talk we discuss some recent results on autostability relative to strong constructivizations. The primary focus of the talk is the complexity of the index sets for different classes of structures.

Sobolev Institute of Mathematics, Novosibirsk (Russia)
E-mail: bazhenov@math.nsc.ru, s.s.goncharov@math.nsc.ru, margaretmarchuk@gmail.com

On constructive recognition of finite simple groups

A. A. Buturlakin, A. V. Vasil′ev

Given a finite group G, the set of its element orders is denoted by $\omega(G)$. If $\mathcal{M}$ is some set of positive integers, then a natural question is whether a finite group G with $\omega(G) = \mathcal{M}$ exists, and if so, can one describe all such groups? In our talk we deal with algorithmic aspect of this problem in a special case when G is simple.

Sobolev Institute of Mathematics and Novosibirsk State University, Novosibirsk
E-mail: buturlakin@math.nsc.ru, vasand@math.nsc.ru

Natural language, embodied computation, and "The two cultures"

S. B. Cooper

In his 1959 Rede Lecture in Cambridge, the scientist and writer C. P. Snow described how:

"I believe the intellectual life of the whole of western society is increasingly being split into two polar groups. When I say the intellectual life, I mean to include also a large part of our practical life .... Literary intellectuals at one pole - at the other scientists ... Between the two a gulf of mutual incomprehension - sometimes (particularly among the young) hostility and dislike, but most of all lack of understanding. ... Their attitudes are so different that, even on the level of emotion, they can't find much common ground."

Since 1959, the balance and character of what Snow described has changed, in part due to the increasing ascendancy of algorithmic thinking and the computer. Our understanding of the relationship between computer and more 'human' thinking has benefited from the work of mathematicians such as Alan Turing and his successors. The development of the mathematics of computation and definability has provided a framework within which to clarify Snow's dichotomy between the 'Two Cultures'. More important, the mathematics can point to a practical heuristic, anticipated by Turing, via which one can explore and cohere different styles of mental and machine thinking and learning. Key to this is a focus on the mathematics of typed information, definability, and an already evident revival of interest in 'generalised recursion theory' and its wider significance.

University of Leeds, Leeds (Great Britain)
E-mail: pmt6sbc@leeds.ac.uk

The model theory of transseries

L. van den Dries

Ershov has done fundamental work on the model theory of henselian valued fields. This includes the valued field of Laurent series with real coefficients. When viewed as a valued differential field, however, with termwise differentiation, we run into undecidability in the Laurent series setting. Positive results along the Ax–Kochen–Ershov paradigm can be reestablished by going to a much larger differential field of transseries, which include also logarithmic and exponential terms. This is joint work with Matthias Aschenbrenner and Joris van der Hoeven.

University of Illinois at Urbana-Champaign, Urbana IL (USA)
E-mail: vddries@math.uiuc.edu

Formal ontology and principles of theory formation and modeling

H. Herre

In this talk we present and discuss principles of organization and representation of knowledge which are grounded on formal ontology and the axiomatic method, being unified to establish the onto-axiomatic method. We use the term formal ontology (FO) to name an area of research which is becoming a science similar as formal logic. Formal ontology is concerned with the systematic development of axiomatic theories describing forms, modes, and views of being of the world at different levels of abstraction and granularity; this discipline integrates aspects of philosophy, formal logic, artificial intelligence (computer science), and cognitive science.

We explain the usage of formal ontology by a number of examples. In particular we address following topics: a theory of ontological regions, a new theory of time and space, an ontological analysis of visual perception, an ontology of sets, collectives and categories, aspects of an ontology-bases semantics, an analysis of biological basic notions, and a three ontology method for software development. Finally, we outlook some open problems, among them big problems of formal ontology, but also the need of new theories in various fields, notably in the field of economy.

University of Leipzig, Leipzig (Germany)
E-mail: heinrich.herre@imise.uni-leipzig.de

Computability and uncountable structures

Julia F. Knight

What can we say, using methods from computability, about uncountable structures such as the reals? There are different approaches. Some approaches involve changing the basic notions of computability. Using Hamkin's Infinite-Time Turing machines, or Yue Yang's Master-Slave machines, or definitions from α-recursion theory (with an unpleasant set-theoretic assumption), we see that the ordered field of reals is a computable structure. Noah Schweber defined a notion that lets us compare the computing power of structures of any cardinality, using the standard notions of computability. We say that $\mathcal{A}$ is *Schweber reducible* to $\mathcal{B}$ if after we collapse cardinals so that the two structures become countable, every copy of $\mathcal{B}$ computes a copy of $\mathcal{A}$. I will describe results applying Schweber reducibility to some structures related to the reals.

University of Notre Dame

Finite groups with given properties of their prime graphs

A. S. Kondrat'ev

The prime graph of a finite group is its important arithmetical invariant, having numerous applications. In the talk, we will discuss some results of the study of finite groups by the properties of their prime graphs, obtained by the author and his pupils.

IMM UB RAS, Ekaterinburg (Russia)
E-mail: a.s.kondratiev@imm.uran.ru

The valuation difference rank of a valued difference field

S. Kuhlmann

There are several equivalent characterizations of the valuation rank of a valued field. In this paper, we extend the theory to the case of a valued difference field and introduce the notion of *difference rank*. We characterize the difference rank as the quotient modulo the equivalence relation naturally induced by the automorphism (which encodes its growth rate). In analogy to the theory of convex valuations, we prove that any linearly ordered set can be realized as the difference rank of a valued difference field.

Universität Konstanz, Konstanz (Germany)
E-mail: Salma.Kuhlmann@uni-konstanz.de

Computable Model Theory in the context of the complex and Zilber exponentials

A. Macintyre

I will show that the countable strongly existentially closed exponential fields of Zilber are computable.

Queen Mary University of London, London (UK)
E-mail: a.macintyre@qmul.ac.uk

Bases and generating sets in computable algebra

A. Melnikov

We will survey several recent results in computable algebra that rely on various notions of independence and different choices of generating sets as technics tools. These results can be roughly sub-divided into two kinds.

Results of the first kind study classes in which the respective notions of independence and bases are natural, and it makes sense to study these notions on their own right. Results of this kind go back to the Novosibirsk School of Algebra and Logic and to Mal'cev in particular. As was first noted by Goncharov, results of this sort have interesting applications in the theory of computable categoricity and auto-dimension. Using the notion of a c.e. pregeometry, we develop a general framework of independence in computable commutative structures with new applications to computable differentially closed, difference closed, and real closed fields. We also discuss a long-standing open problem of tree-bases in abelian p-groups.

Results in the second class use special notions of a generating set as a technical tool. With a right choice of a generating set, many complicated arguments become a lot simpler. In fact, several known proofs of this sort would be totally incomprehensible in absence of a good choice of a generating set. Such results are common in computable abelian group theory, but there have been applications to other classes including integral domains.

Massey University (New Zealand)
E-mail: alexander.g.melnikov@gmail.com

The filter of supergeneric sets

Bruno Poizat

This talk presents a paper that was published last year in the *Journal of Algebra 404, p. 240–270*, under the title *Supergénérix*.

Its starting point was the following problem: given a linear group G, embedded in a matrix group $\mathrm{Gl}_m(K)$, what can be said on the trace on G of a constructible subset C (i.e., a boolean combination of a finite number of Zariski-closed sets) of $\mathrm{Gl}_m(K)$? We observe that there is a subgroup H of finite index in G such that, for each coset aH, the intersection $C \cap aH$ is a translate of a supergeneric or of a cosupergeneric subset of H.

Given an arbitrary group G and a subset A of it, we say that A is generic if a finite number of translates of A cover G: $G = a_1A \cup \cdots \cup a_mA$; we say that it is *supergeneric* if any intersection $B = b_1A \cap \cdots \cap b_nA$ of a finite number of translates of A is generic (there are three notions: left, right, two-sided generic and supergeneric). A basic fact is that the supergeneric sets form a filter, the intersection of two supergeneric sets being also supergeneric.

We shall consider some uniformity properties possessed by supergeneric sets which are the traces of the definable subsets of an overgroup Γ of G having nice model-theoric properties (this generalizes the linear case), and also the behaviour of supergenericity with respect to cartesian products in this context. We shall also illustrate the notion with very plain groups, such that the infinite cyclic group and the Prüfer groups, and conclude by a list of open questions.

Université Claude Bernard (Lyon-1), France

Hilbert's Nullstellensatz in algebraic geometry over rigid solvable groups

N. S. Romanovskiĭ

The classical Hilbert's Nullstellensatz says: if K is algebraically closed field and there is a system of polynomial equations over K, $\{f_i(x_1,\dots,x_n)=0 \mid i\in I\}$, then an equation $f(x_1,\dots,x_n)=0$ is a logical consequence of this system (satisfies all the solutions of the system in K^n) if and only if some nonzero power of f belongs to the ideal $(f_i \mid i\in I)$ of the ring $K[x_1,\dots,x_n]$. One can say say that we give an algebraic method for constructing all logical consequences of the given system of equations: f is obtained from f_i $(i\in I)$ using the operations of addition, subtraction, multiplication by elements of $K[x_1,\dots,x_n]$, and extraction of roots.

Our approach to Hilbert's theorem in algebraic geometry over groups is as follows.

1. We should consider some good class of equationally Noetherian groups, let it be a hypothetical class $\mathcal{K}$.

2. In this class, we need to define and allocate an algebraically closed objects and to prove that any group of $\mathcal{K}$ is embedded into some algebraically closed group. Hilbert's theorem should be formulated and proved for algebraically closed in $\mathcal{K}$ groups.

3. Further, let G be an algebraically closed group in $\mathcal{K}$. We think about equations over G as about expressions $v=1$, where v is an element of the coordinate group of the affine space G^n.

4. Since an arbitrary closed subset of G^n is defined in general not by a system of equations, but by a positive quantifier free formula (Boolean combination without negations of a finite set of equations) we should consider as basic blocks not equations, but positive formulas.

5. We should specify and fix some set algebraic rules of deduction on the set of positive formulas over G.

6. If the above conditions Hilbert's theorem will consist in a statement that all logical consequences of given positive formula over G are exactly the algebraic consequences.

We realized this approach in algebraic geometry over rigid solvable groups.

Sobolev Institute of Mathematics SB RAS
E-mail: rmnvski@math.nsc.ru

Problems of unification, admissibility and knowledge representation in transitive and non-transitive temporal linear logics

V. V. Rybakov

We study the linear temporal logic LTL, in particular, its new non-transitive versions. Problems of Unification, Admissibility of Inference Rules, Modeling of AgentTs Knowledge and Knowledge Representation to be considered. We will describe construction of technique to obtain deciding algorithms. Several application areas to be described and discussed.

Manchester Metropolitan University, Manchester (UK)
E-mail: V.Rybakov@mmu.ac.uk

Dialectical systems and quasi-dialectical systems: two approaches to trial-and-error mathematics

A. Sorbi

This is a joint work with J. Amidei, L. San Mauro, D. Pianigiani, and G. Simi.

Dialectical systems were introduced by Roberto Magari in order to describe a trial-and-error approach to mathematical theories, in which axioms may be rejected or accepted through a trial-and-error process: the *final theses*, i.e. the axioms that are eventually accepted, form a Δ^0_2 set. The *dialectical sets* are the sets that consist of the final theses of some dialectical system. When equipped with the deductive machinery of a consistent formal theory T, a dialectical system produces a consistent Δ^0_2 completion of T, so that dialectical systems describe "deductive procedures" that in some sense escape the incompleteness phenomenon; it is also possible to come up with dialectical systems that, among their final theses, have a statement naturally expressing their consistency. The basic ingredient of a dialectical system is that when a proposed axiom seems to produce a contradiction, then we "discard it", and we try with next one. We enrich this mechanism with a "revision" procedure *à la* Lakatos: when an axiom seems inadequate, even if not contradictory, then we replace it with a new one. The enriched systems are called *quasi-dialectical systems*, and the corresponding sets of *final theses* are called *quasi-dialectical sets*, forming a class that extends the class of dialectical sets. We prove that quasi-dialectical sets lie in the same Turing degrees as dialectical sets, namely the c.e. Turing degrees; also the two classes provide the same enumeration degrees, namely the Π^0_1 enumeration degrees. So, in some sense, dialectical systems and quasi-dialectical systems display the same information content. Nevertheless, the class of quasi-dialectical sets is much larger than the class of dialectical sets: every dialectical set can be shown to be ω-c.e., whereas quasi-dialectical sets spread out through all classes of the Ershov hierarchy of Δ^0_2 sets: for every ordinal notation $a \in \mathcal{O}$, with $|a|_{\mathcal{O}} > 0$, there is a quasi-dialectical set $A \in \Sigma^{-1}_a \smallsetminus \bigcup_{b <_{\mathcal{O}} a} \Sigma^{-1}_b$. As to dialectical sets, we show that for every finite $n > 1$ there exist n-c.e. dialectical sets, which are not $(n-1)$-c.e. (the statement is not true of $n = 1$, as already observed by Magari); and there exist ω-c.e. dialectical sets which are not n-c.e., for every finite n.

University of Siena, Siena (Italy)
E-mail: sorbi@unisi.it

Big subsets with small boundaries in a graph with a vertex-transitive group of automorphisms

V. I. Trofimov

The theory of ends of finitely generated groups G and connected locally finite graphs Γ with vertex-transitive groups of automorphisms can be regarded as a theory of the Boolean algebras of subsets of G or the vertex set of Γ with finite boundaries (in locally finite Cayley graphs of G or in Γ), considered modulo finite subsets. We develop a more general approach towards 'ends', replacing infinite subsets with finite boundaries by certain 'big' subsets with 'small' boundaries. This is a joint work with N. Seifter.

IMM UB Russian Acad. Sci., Ekaterinburg
E-mail: trofimov@imm.uran.ru

II. Секция «Алгебро-логические методы в информационных технологиях»

Распознавание аномальных данных с использованием таксономических решающих деревьев

В. Б. Бериков

Одной из актуальных задач анализа данных является распознавание аномальных наблюдений. В качестве примера прикладной задачи можно привести обнаружение необычной активности субъектов на основе анализа информации об их двигательном поведении (замеров датчиков акселерометра, гироскопа, магнетометра и частоты сердечных сокращений). При этом аномальными считаются такие наблюдения, для которых вероятность их возникновения (оцененная по обучающей выборке) меньше определенного порогового значения.

Существует ряд методов детекции аномалий, например, одноклассовый метод опорных векторов, непараметрические оценки плотности и т.д., однако возможности их применения ограничиваются случаем количественных характеристик: при введении расстояний для признаков нечисловой природы возникают серьезные методологические трудности. При наличии разнотипных переменных (булевых, номинальных, порядковых и количественных) для решения задачи предлагается использовать класс логических решающих функций, представленных в виде таксономических деревьев решений. Алгоритмы построения таксономических решающих деревьев [**1**]) позволяют проводить группировку объектов в разнотипном пространстве переменных, формируют иерархическую логическую модель группировки, определяют наиболее информативные для группирования факторы. Логическое правило классификации представляет собой утверждение вида "Если $X_{j_1}(a) \in E_{j_1}$ И ... И $X_{j_m}(a) \in E_{j_m}$, то объект a относится к k-му кластеру", где $X_j(a)$ означает значение переменной X_j для объекта a. Если объект не принадлежит ни к одной из найденных групп, и при этом критерий качества группировки, полученный при включении данного объекта в кластеры, значительно деградирует, то такой объект считается аномальным. Для улучшения точности распознавания применяется также ансамбль алгоритмов кластерного анализа [**2**].

Список литературы

[1] *Berikov V. B.* Grouping of Objects in a Space of Heterogeneous Variables with the Use of Taxonomic Decision Trees // Pattern Recognition and Image Analysis. 2011. Vol. 21, No. 4, P. 591-598.

[2] *Berikov V.* Weighted ensemble of algorithms for complex data clustering // Pattern Recognition Letters. 2014. Vol. 38. P. 99-106.

Институт математики им. С.Л.Соболева СО РАН, Новосибирск
E-mail: berikov@math.nsc.ru

Реляционная модель логического разграничения доступа для современных информационных систем

В. А. Васенин, В. Ю. Бухонов, А. А. Иткес, К. А. Шапченко

Разграничение доступа к отдельным ресурсам и действиям с ними является важной составляющей современных информационных систем. Большое число пользователей, частое изменение атрибутов и связей ресурсов и пользователей, изменение состава пользователей в таких системах делают неэффективным использование традиционных моделей и механизмов для задания и исполнения правил доступа, в том числе — из-за увеличения количества административных действий по управлению правилами доступа. Декларативное задание правил доступа с использованием логико-языковых средств с высоким уровнем выразительности позволяет обойти ряд ограничений традиционных подходов. Такой способ задания правил применяется, например, в универсальных моделях логического разграничения доступа на основе атрибутов, а также в специализированных моделях, применяемых в системах с элементами социальных сетей.

В рамках указанного декларативного подхода предлагается новая модель логического разграничения доступа, предназначенная для применения в широком классе информационных систем, которые используют реляционные СУБД для хранения данных, на основе которых принимается решение о доступе. Зачастую «отношения»-связи между сущностями в системе хранятся в виде «отношений» в таблицах реляционных СУБД либо простым образом выражаются через них. Такая особенность позволяет использовать терминологию принятой модели данных при задании правил доступа и эффективно вычислять решение о доступе с применением оптимизаций реляционных СУБД.

Предлагаемая модель в своей основе использует так называемые цепочки отношений. Например, для правила «пользователь может иметь доступ к документам сотрудников своего подразделения» может использоваться цепочка отношений «пользователь a работает в подразделении b», «в подразделении b работает пользователь c», «пользователь c является автором документа d», причем положительное решение о доступе принимается при существовании набора значений для соответствующих переменных. За счет комбинирования цепочек отношений и внедрения дополнительных атрибутов удается выразить широкий класс правил доступа. При этом для предлагаемой модели разработан способ оценки ее корректности, необходимой для эффективного вычисления решения о доступе.

Возможность применения предлагаемого подхода на практике апробирована на модели многопользовательской информационно-аналитической системы «Наука-МГУ» («ИСТИНА»). Эта система предназначена для управления наукометрической информацией и рассматривается в МГУ как инструментарий управления научно-педагогической и инновационной деятельностью в университете, как средство повышения его рейтингового потенциала.

НИИ механики МГУ имени М. В. Ломоносова
E-mail: vasenin@msu.ru

Алгебраический подход к оптимизации реконфигурируемых вычислительных систем и сетевых протоколов

В. А. Васенин, В. А. Роганов

Использование свойств таких алгебраических структур, как кольца линейных операторов над полями R, C и Q [**1**], а также над конечными полями давно занимает почетное место как в современной теории вычислений (криптография, коды исправления ошибок), так и в ее перспективных направлениях (реверсивные, квантовые вычисления). Активно развивается аппаратная поддержка соответствующих операций. К числу активно внедряемых сегодня расширений относятся: векторные инструкции и фрагменты раундов шифра AES в микропроцессорах, быстрая арифметика для полей Галуа в специализированных микросхемах [**2**].

Определенным вызовом научному и инженерному сообществу является появление реконфигурируемых вычислительных систем, а также специализированных многоядерных сопроцессоров. Максимальное использование их вычислительных возможностей требует, как правило, значительной модификации численных методов и алгоритмов. Классическое определение вычислительной сложности как совокупного количества необходимых примитивных операций для таких устройств перестает быть адекватной мерой их производительности. Возможность же реконфигурации аппаратуры и вовсе переносит вопрос в новую плоскость, поскольку динамические синтез и оптимизация вычислительной схемы или среды передачи данных становятся основополагающими факторами обеспечения эффективного функционирования системы [**3**].

В качестве примеров задач, в решении которых существенную помощь оказывают алгебраические методы, можно привести следующие:

(1) Обеспечение отказоустойчивости параллельных алгоритмов для решения систем линейных уравнений с большими разреженными матрицами;
(2) Создание высоконадежных протоколов для информационного обмена в реальном масштабе времени через глобальные сети передачи данных и радиоканалы;
(3) Построение систем логических правил для быстрого синтеза квазиоптимальных вычислительных систем с использованием информации о специфике полугруппы операций для интересующей нас предметной области.

Иллюстрацией эффективности применения алгебраического подхода могут служить следующие утверждения:

Теорема. *Параллельный алгоритм решения системы линейных алгебраических уравнений с разреженной матрицей, имеющей трехмерную конфигурацию ненулевых элементов, можно сделать отказоустойчивым для практически любой доли отказов* $k < 1$*, сохранив вычислительную эффективность при малых* k*.*

Теорема. *Эффективная оптимизация параметров протокола избыточного блочного кодирования на базе использования матриц Коши над полем* $GF[2, k]$ *для сети с активной ретрансляцией может быть выполнена за время* $O(n)$*, где* n *– количество узлов сети.*

Список литературы

[1] *Васенин В. А., Роганов В. А.* Применение полей Q и F(X) в параллельных вычислениях и для верификации программ. Мальцевские чтения, Новосибирск, 2013.

[2] *Гашков С. Б., Сергеев И. С.* О сложности и глубине булевых схем для умножения и инвертирования в конечных полях характеристики 2. Дискретная математика, том 25, № 1, 2013, с. 3-32.

[3] *Захаров В. А., Чемерицкий Е. В.* О некоторых задачах реконфигурирования программно-конфигурируемых сетей. Моделирование и анализ информационных систем, том 21, № 6, 2014, с. 57-69.

Механико-математический ф-т. и НИИ Механики МГУ им. Ломоносова, г.Москва
E-mail: vasenin@msu.ru, var@msu.ru

Формализация естественной классификации и систематики через неподвижные точки предсказаний

Е. Е. Витяев, В. В. Мартынович

В настоящее время известно множество подходов к построению классификаций: основанных на компактности и различных мерах близости в признаковых пространствах; на сравнении с эталонами; разделении смесей распределений и т.д. В отличии от вышеперечисленных подходов, задачей «естественной» классификации является обнаружение классификации как закона природы, удовлетворяющего определённым требованиям, сформулированным естествоиспытателями. Смысл этого закона в сжатии информации за счет выделения закономерных структур объектов с помощью неподвижных точек предсказания свойств.

Задача стояла в таком определении понятия вероятностного правила (закона), чтобы неподвижные точки, полученные логическим выводом по этим правилам были непротиворечивы (не содержали одновременно литеру и ее отрицание).

Для решения этой задачи было использовано и формализовано требование максимальной специфичности вероятностных правил. В результате были решены следующие задачи:

(1) Формально определено требование максимальной специфичности.
(2) Определены максимально специфические правила, которые удовлетворяют требованию максимальной специфичности и не подвержено проблеме статистической двусмысленности.
(3) Доказано, что максимально специфические правила при построении неподвижных точек непротиворечивы (не содержат литеру и ее отрицание)
(4) Дано определение "естественной" классификации и систематики на основании неподвижных точек.
(5) Разработан метод обнаружения максимально специфических правил и ¡ естественной¿ классификации и систематики.

Основной теоретичекий результат состоит в следующем.

Теорема. *Неподвижные точки оператора прямого вывода по множеству максимально специфических законов для совместного набора литер L совместны и непротиворечивы.*

Разработанный метод работает с зашумленными данными. Проведен компьютерный эксперимент, в котором по выборкам сайтов связывания транскрипционных факторов распознается их класс. Полученный метод классификации последовательностей оказывается эффективнее общепринятого метода классификации сайтов на основе весовых матриц.

Институт математики им. С.Л.Соболева, Новосибирск
НГУ, Новосибирск
E-mail: evgenii.vityaev@math.nsc.ru; vilco@ya.ru

Иерархические Σ-спецификации дискретных систем реального времени

В. Н. Глушкова

Поведение многих систем реального времени характеризуется неограниченной последовательностью $St_1,\ldots$ $St_n,\ldots$ переходов между состояниями. В идеологии "model checking" они описываются конечными временными автоматами с циклами без финальных состояний, расширенных множеством переменных-локальных часов. Формулы темпоральных логик формализуют циклически повторяющиеся свойства, проверяемые на деревьях вычислений, порождаемых автоматами.

Язык Σ- формул [**1**] более выразительный, он расширяет возможности ИП 1-го порядка введением переменных сорта "list" (которыми легко представить деревья) и допускает явное использование переменных сорта "time". Для построения формальной модели системы будем использовать теорию Th из Δ_0 - формул специального вида. Иерархизируем списки в соответствии с правилами вида $St \to \{Act\}^+St$(грамматики G), где Act, St– имена действий и состояний. Безкванторная часть формулы – квазитождество с отрицаниями вида:

$$\varphi(x_1,\ldots x_n, y_1,\ldots y_m) \to \psi(x_1,\ldots x_n, y_1,\ldots y_m)$$

φ (ψ)- конъюнкция атомарных формул или их отрицаний вида p, $f=\tau$, $\tau_1=\tau_2$, p, f, τ- символы предикатов, функций и термов соответственно. В префиксе формулы используются кванторы $\forall x_i \dot{\in} y_j$, $\forall x_i \prec y_j$, $\dot{\in}$- транзитивное замыкание отношения $\in$, $\prec$- отношение "левее" для элементов списка. Теория Th – это система определений функций и отношений, заданных на узлах дерева. При определенных ограничениях на теорию она имеет многосортную константную модель для дерева грамматики G. Полиномиальный (относительно "размера" дерева) алгоритм построения модели реализует прямой логический вывод для заданной теории. Предикаты, функции, аксиомы теории, сорта переменных согласованы с символами и правилами G, которые применяются к исходному дереву в процессе вычисления. На полученном дереве можно проверять истинность произвольных Δ_0- формул.

Для практики существенным является выразительность Δ_0-формул: какие именно свойства системы можно формализовать и верифицировать. Легко формализовать причинно-следственные связи событий с конкретными временными значениями. Для анализа систем с неопределенным временем наступления событий необходимо расширить класс формул и допустить использование термов, не сводимых к константам в процессе вычислений. Это приведет к идеологии смешанных вычислений на термальных моделях.

Список литературы

[1] *Goncharov S. S., Ershov Yu. L., Sviridenko D. I.* Semantic programming // Information processing. 1986. V. 11. № 10 p. 1093–1100.

ДГТУ, Ростов-на-Дону
E-mail: lar@aaanet.ru

Экспертная системы оценки рисков при лекарственных назначениях

А. А. Дергунов

Экспертная система предназначена для помощи врачу в принятии медицинских решений, а именно - в оценке рисков при лекарственных назначениях. Основа системы - база знаний, содержащая прецеденты. Эти данные могут включать в себя результаты анализов, внешние факторы, сведения о прописанных медицинских препаратах и схему лечения по ним.

Задача кластеризации заключается в разбиении множества событий на подмножества (кластеры) таким образом, чтобы кластер состоял из подобных объектов, но при этом различные кластеры отличались друг от друга. Из-за специфики предметной области, объект не может относиться однозначно к одному кластеру. По этой причине, в качестве алгоритма применяется метод нечеткой кластеризации c-средних (Fuzzy c-means clustering) [**1**].

Пациент рассматривается как набор признаков, которыми он обладает. Это могут быть как количественные признаки, так и качественные: возраст, вес, заболевания, лекарственные препараты, которые он принимает в настоящий момент и.т.п. У этих признаков должен быть разный вес, так как не все они влияют в равной степени. Для сравнения признаков между собой необходимо нормализовать значения признаков.

В базе знаний экспертной системы содержится состояние пациента до применения и состояние после применения лекарственного средства. В качестве решения задачи восполнения пропущенных данных используется замена пропуска средним из ближайших.

Результат работы системы представляет из себя упорядоченный по удаленности от центров набор кластеров, к которым относится текущий прецедент.

Используя описанный подход, в рамках работы была построена математическая модель предметной области, проведена формулировка и анализ требований к экспертной системе, разработана архитектура экспертной системы. На данный момент реализован прототип системы.

Список литературы

[1] *Berks G., Keyserlingk D.G.V., Jantzen J., Dotoli M., Axer H.* (2000) Fuzzy clustering - a versatile mean to explore medical databases. In: Proceedings of European Symposium on Intelligent Techniques clustering // Pattern Recognition Letters. 2014. Vol. 38. P. 99-106.

Новосибирский государственный университет, Новосибирск
E-mail: dergunov.alexander@gmail.com

О существовании классифицирующей функции для произвольного разбиения N-мерного куба на два класса

В. П. Добрица, Д. Н. Нургабал, Н. С. Уалиев

Рассмотрим n-мерный куб как n-ю степень отрезка $[0,1]$. В этом случае каждой вершине соответствует код из 0 и 1 длины n.

Теорема 1. *Для произвольного разбиения вершин n-мерного куба на два класса, отмеченных 0 и 1 соответственно, существует непрерывная функция $f(x_1,\ldots,x_n)$ такая, что аргументы и она сама изменяются в пределах отрезка $[0,1]$ и во всех вершинах, отмеченных 1, она принимает значение 1, а в вершинах, отмеченных 0, она принимает значение 0.*

На основании этой теоремы доказан следующий результат.

Теорема 2. [**1**] *Для произвольного разбиения вершин n-мерного куба на два класса существует нейронная сеть, распознающая эти классы.*

Эта теорема дает теоретическое обоснование для нейросетевого шифратора текстов [**2**].

Список литературы

[1] *Добрица В. П., Нургабыл Д. Н., Уалиев Н. С.* Существование классифицирующей нейронной сети для произвольного разбиения n-мерного куба на два класса // Нейрокомпьютеры: разработка, применение. - 2014, №6. - с.12,48 - 15,52.

[2] *Добрица В. П., Липунов А. А.* Нейросетевой шифратор текстов // Наукоемкие технологии. Научно-технический журнал. - 2012, №9, т.13. - с.13-15.

ЮЗГУ, Курск; ЖГУ, Талдыкорган
E-mail: dobritsa@mail.ru; kebek.kz@mail.ru; n.ualiev@gmail.com

Термальное исчисление и его семантики

Б. Н. Дроботун

В работе [**1**] была конкретизирована, применительно к исчислению высказываний (ИВ), общая схема построения семантических интерпретаций пропозициональных исчислений, определено термальное исчисление $Term$, как строго формализованный вариант ИВ, в рамках которого обеспечивается возможность наиболее последовательного разделения синтаксической и семантической составляющих этого исчисления.

В исчислении $Term$ формулы ИВ представляются термами сигнатуры

$$\lambda = \langle G_1^2;\ G_2^2;\ G_3^2;\ G_4^1;\ d_1;\ d_2\rangle$$

над множеством $\{X_1; X_2; :; X_t; :\}$ - пропозициональных переменных. В соответствии с этим, интерпретации η исчисления $Term$ определяются алгебрами

$$\boldsymbol{I} = \langle M;\ {}^{\eta}G_1^2;\ {}^{\eta}G_2^2;\ {}^{\eta}G_3^2;\ {}^{\eta}G_4^1;\ {}^{\eta}d_1;\ {}^{\eta}d_2\rangle,$$

основные операции и выделенные элементы которых являются термальными операциями и выделенными элементами некоторых алгебраических систем $\boldsymbol{M} = \langle M;\ P_1^{m_1};\ ...;\ P_k^{m_k};\ f_1^{n_1};\ ...;\ f_l^{n_l};\ a_1;\ a_r\rangle$, выступающих в роли полей означивания этих интерпретаций. Интерпретации $\boldsymbol{I}$, удовлетворяющие ряду дополнительных условий [1], и будут представлять собой различные семантики ИВ. Одним из таких условий является следующее: значения термальных операций алгебры $\boldsymbol{I}$, соответствующих аксиомам исчисления $Term$, должны принадлежать определенному подмножеству S множества M. В работе [**2**], следуя этой схеме, была определена нетрадиционная семантика ИВ, названная теоретико-кольцевой, т.к. в качестве поля означивания, при ее построении, было взято (произвольное) булево кольцо с единицей.

В данной работе, отправляясь от булевой решетки $\boldsymbol{M} = \langle M;\ P_1^2;\ f_1^2;\ f_2^2;\ f_3^1;\ 0;\ 1\rangle$, как поля означивания, где P_1^2 - отношение частичного порядка; $f_1^2(x;y) = sup(x;y)$; $f_2^2(x;y) = inf(x;y)$; $f_3^1(x)$ - дополнение элемента x; 0 и 1 - наименьший и наибольший элементы множества M, определяется «порядковая» семантика ИВ.

Предложение 1. *Пусть* $\boldsymbol{M}$ *- произвольная булева решетка. Интерпретация* η *сигнатуры* λ *на множестве* M*, определенная по правилам:* ${}^{\eta}G_1^2(a;b) = f_1^2(a;b)$*;* ${}^{\eta}G_2^2(a;b) = f_2^2(a;b)$*;* ${}^{\eta}G_3^2(a;b) = f_1^2(f_3^1(a);b)$*;* ${}^{\eta}G_4^1(a) = f_3^1(a)$*;* ${}^{\eta}d_1 = 0$*;* ${}^{\eta}d_2 = 1$*, для любых* $a;b \in M$*, является семантикой ИВ с полем означивания* $\boldsymbol{M}$ *и выделенным подмножеством* $S = \{1\}$.

Список литературы

[1] *Дроботун Б. Н., Джарасова Г. С., Егимбаева Н. Б.* О семантиках исчислений высказываний \\ Вестник Тверского государственного университета. №2, 2014г. С. 148-165.

[2] *Дроботун Б. Н.* О семантиках пропозициональных исчислений. Материалы международной научной конференции «Алгебра и математическая логика: теория и приложения», Казань, 2014, С. 52

Павлодарский государственный университет им. С. Торайгырова, г. Павлодар.
E-mail: drobotun.nina@mail.ru

Реализация условных вопросов в вероятностной вопросно-ответной системе

А. А. Карманова, Г. Э. Яхъяева

В рамках программного комплекса «RiskPanel» [**1**], для предметной области информационной безопасности была разработана вопросно-ответная система «QA-RiskPanel» [**2**]. Данная система основана на прецедентном подходе к моделированию предметных областей; база знаний при данном подходе моделируется в виде обобщенной нечеткой модели. Так как знания, представленные в базе, могут быть неполными или неточными, ответы на поставленные вопросы будут носить вероятностный характер. Для вопросов, которые могут быть заданы такой системе, была разработана классификация, состоящая из нескольких вопросных типов; возможность получать ответы на составные вопросы реализуется посредством основных операций классической логики.

В общем случае, внутреннюю логику вопроса, действительно, можно описать посредством основных операций классической логики. Однако проблема возникает, когда семантику вопроса на естественном языке нельзя описать средствами логических операций конъюнкции, дизъюнкции, отрицания и импликации. Любой реальный вопрос обычно имеет входные данные, то есть предварительные знания о предмете вопроса. Учет этих знаний позволяет получить наиболее точный ответ. Возможность усложнять конструируемый вопрос путем надстраивания условия позволяет учесть предварительные знания о предмете.

В данной работе для поиска ответа на условные вопросы был разработан алгоритм, учитывающий вероятностные характеристики базы знаний. Пользователи формируют условие в виде логического выражения, которое должно выполняться для базы знаний. Кроме того, пользователи задают для этого выражения интервал вероятностей, с которыми данное условие должно выполняться. Таким образом, мы получаем подмодели, на которых условие выполнено, а значит, предварительные знания были учтены. Последующее вычисление ответа ведется на этих подмоделях с дальнейшим обобщением результатов.

Список литературы

[1] *Пальчунов Д. Е., Яхъяева Г. Э., Хамутская А. А.* Программная система управления информационными рисками RiskPanel. Программная инженерия. 2011. № 7. С. 29-36.

[2] *Яхъяева Г. Э., Ясинская О. В., Карманова А. А.* Вероятностная вопросно-ответная система в области компьютерной безопасности // Вестник НГУ. Серия: Информационные технологии. 2014. Т. 12, вып. 3. с. 132-145.

Новосибирский государственный университет, Новосибирск
E-mail: anast.karmy.aa@gmail.com, gulnara@mail.ru

Обратный метод Маслова в его секвенциальной интерпретации

А. В. Лялецкий

Рассматривается обратный метод установления выводимости С.Ю. Маслова в его формулировке из [**1**] для классической логике 1-го порядка без равенства. Дается его описание в виде специфического исчисления так называемых благоприятных секвенций. Заметим, что при рассуждениях по выполнимости одна из наиболее удачных трактовок обратного метода дана в [**2**], а [**3**] содержит наиболее оригинальное "погружение" обратного метода в чисто резолюционную технику.

Известно, что посредством скулемизации и логических преобразований установление выводимости в генценовском исчислении LK любой секвенции можно свести к установлению выводимости *стартовой* секвенции S вида $\to D_1, \ldots, D_n$, где $D_1, \ldots, D_n$ – формулы в дизъюнктивной нормальной форме с опущенными кванторами, причем по умолчанию считается, что все их свободные переменные неявно связаны кванторами существования, стоящими перед $D_1, \ \ldots, \ D_n$.

Следуя правилу **А** из [**1**], с S связывается *исходная благоприятная* секвенция $C_1, \ldots, C_m \to D_1, \ldots, D_n$, обозначаемая S_f, в которой $C_1, \ldots, C_m$ являются определенными дизъюнкциями литер, строимыми из литер формул $D_1, \ldots, D_n$ таким образом, что каждая из них содержит как атомарную формулу, так и ее отрицание. Правило **Б** из [**1**] интерпретируется как секвенциальное правило, которое преобразует уже порожденную *благоприятную* секвенцию в новую *благоприятную* секвенцию, у которой в сукцеденте находятся $D_1, \ldots, D_n$, а в антецедент добавляется новая дизъюнкция литер, порождаемая на основании анализа $D_1, \ldots, D_n$ и дизъюнкций литер из антецедента рассматриваемой секвенции.

Теорема. *Стартовая секвенция S выводима в классическом секвенциальном исчислении LK тогда и только тогда, когда исчислении благоприятных секвенций из S_f по правилу* **Б** *выводима (благоприятная) секвенция, содержащая в своем антецеденте дизъюнкцию без литер (т.е. пустую дизъюнкцию).*

В заключении отметим, что приведенная интерпретация обратного метода обладает рядом положительных свойств по отношению как к компьтерно-ориенти- рованным секвенциальным исчислениям, так и к методам резолюционного типа.

Список литературы

[1] *Маслов С. Ю.* Обратный метод установления выводимости в классическом исчислении предикатов. ДАН СССР, Т. 159, № 1, 1964, С. 17-20.

[2] *Lifschitz V.* What is the inverse method? Journal of Automated Reasoning, V. 5, No. 1, 1989, P. 1-23.

[3] *Degtyarev A.*, *Voronkov A.* Equality elimination for the inverse ethod and extension procedures. Technical Report No. 92, Uppsala University, 1994.

Киевский национальный университет имени Тараса Шевченко, Киев
E-mail: lav@unicyb.kiev.ua

Формализованное доказательство корректности теории типов Хоара

Е. М. Макаров, К. Скалка

Мы доказываем корректность теории типов Хоара (ТТХ) [**1**], являющейся расширением логики Хоара для функционального языка программирования с побочными эффектами (присваиванием). Данное доказательство формализовано в интерактивной системе доказательств Coq.

Поведение чисто функциональных программ описывается с помощью известных выразительных систем типов. Однако методы верификации программ высшего порядка с побочными эффектами не так хорошо изучены. Свойства императивных программ можно доказывать с помощью логики Хоара. Она содержит суждения вида $\{P\}M\{Q\}$, где M — программа, а P и Q — пре- и постусловие, соответственно. Сепарационная логика расширяет логику Хоара, позволяя говорить о поведении указателей. ТТХ использует сепарационную логику для описания функциональных программ. Доказательство корректности ТТХ довольно сложное и использует модели реализуемости.

Наше доказательство более простое и основано на сохранении типов. В отличие от предыдущего, оно было полностью формализовано в Coq. Более того, нашу формализацию можно использовать для верификации программ. Формализация логического исчисления содержит кодирование синтаксиса, которое может привести к тому, что программы, подлежащие верификации, превращаются в труднопонимаемые синтаксические объекты. Наша формализация позволяет писать чистые фрагменты программ на языке Coq, который сам является теорией типов, похожей на чистый фрагмент ТТХ, и использовать новые конструкции только для операций с побочными эффектами, отсутствующих в Coq.

В результате мы имеем единую систему, корректность которой доказана в Coq и которую можно использовать на практике для доказательства правильности программ. Для каждой верифицированной программы имеется полное формальное доказательство того, что программа ведет себя согласно спецификации.

ТТХ была ранее реализована в Coq в проекте Ynot [**2**], однако эта реализация не содержала формализации синтаксиса и доказательства корректности. Наша реализация является более надежной, поскольку не использует аксиомы, несовместимые с классической логикой.

Список литературы

[1] *Chlipala A., Malecha G., Morrisett G., Shinnar A. and Wisnesky R.* Effective interactive proofs for higher-order imperative programs. In ICFP '09.

[2] *Chlipala A. et al.* Ynot project. `http://ynot.cs.harvard.edu`.

Нижегородский государственный университет имени Н.И. Лобачевского,
Университет Вермонта, США
E-mail: emakarov@gmail.com

LPACA: облачный сервис описания предметных областей

А. А. Малых, А. В. Манцивода, О. А. Романова

Доклад посвящен представлению облачного сервиса LPACA, ориентированного на поддержку работы пользователя по формированию, накоплению и развитию структурированной информации, имеющей строгую логическую семантику. Хорошо известно, что логические методы с большим трудом осваиваются массовым пользователем интернета. Это является одной из основных проблем для продвижения семантически строгих подходов к обработке данных и знаний в интернете. Опыт развития Semantic web показал, что эту задачу нельзя решить чисто математическими средствами – проблема является междисциплинарной, затрагивающей вопросы интерфейсов, сценариев работы, а также психологическую компоненту.

Логической основой проекта LPACA являются объектные теории над списочными настройками [**2**], разработанные на основе теории GES [**1**]. Технологическая основа разрабатывалась нами в рамках предыдущих проектов – Онтобокс и Мета-2 [**3**]. Однако, в проекте LPACA эти методы и технологии дополнены специализированными интерфейсами визуализации данных и принципиально новыми сценариями взаимодействия пользователя и сервиса.

С нашей точки зрения LPACA представляет собой принципиально новый вид web-сервиса, в котором накопление информации является побочным эффектом и добавленной стоимостью каждодневной деятельности индивидуального пользователя или пользовательских коллабораций. LPACA представляет собой универсальный инструмент, который в отличие от блогов и форумов, ориентирован не на хронологический процесс публикации, а на постепенное развитие, уточнение, масштабирование единой среды данных. Эксперементы с LPACA показывают, что данный сервис доступен самому широкому кругу пользователей и позволяет им в привычных для себя терминах строить логически корректные описания предметных областей.

Список литературы

[1] *Ershov Yu. L., Goncharov S. S., Sviridenko D. I.* Semantic Programming, Information processing, Proc. IFIP 10th World Comput. Congress (Dublin, 1986), IFIP congress series, 10, 1093-1100

[2] *Малых А. А., Манцивода В. П.* Списочные надстройки и семантика итераторов // Вестн. НГУ. Сер. матем., мех., информ., 13:2 (2013), 61-78

[3] *Малых А. А., Манцивода А. В.* Мета2: онтологии как ядро Интернет-сервисов // Научный сервис в сети Интернет: решение больших задач: Труды всерос. науч. конф. 22-27 сентября 2008 г., Новороссийск. - М.: Изд-во МГУ, 2008. - С.425-428.

Иркутский государственный университет, Иркутск
E-mail: olga@baikal.ru

О разложении идеалов некоторых дедекиндовых колец в произведение максимальных идеалов

К. А. Петухова

В [**1**] было описано обобщение известного криптографического алгоритма RSA, в котором вместо натуральных чисел использованы идеалы дедекиндовых колец. Для того, чтобы практически реализовать данный алгоритм и обосновать его криптостойкость, необходимо выбрать способ представления информации о кольце и его идеалах и оценить сложность алгоритмов разложения этих идеалов в произведение максимальных. Мы используем для этого технику работ [**2**] - [**4**].

В докладе будут описаны некоторые виды дедекиндовых колец (прежде всего некоторых колец целых алгебраических чисел), для которых упомянутые выше задачи могут быть в том или ином виде решены. В частности, обсуждается алгоритм, который определяет, содержится или нет нетривиальный идемпотент в конечном фактор-кольце R/I, где R — дедекиндово кольцо, I — его идеал. Дается оценка сложности данного алгоритма.

Список литературы

[1] *Tronin S. N., Petikhova K. A.* RSA cryptosystem for Dedekind rings // Материалы конференции “Алгебра и математическая логика: теория и приложения” (г.Казань, 2-6 июня 2014 г.) и сопутствующей молодежной летней школы “Вычислимость и вычислимые структуры”. - Казань: Изд-во Казан. ун-та, 2014. - С.148-149.

[2] *Huang D., Deng Y.* Deterministic polynomial-time tests for prime ideals of a finite rank Dedekind domain // arxiv:1406.3523v3. — 2014. — 14 p.

[3] *Staromiejski M.* Polynomial-time locality tests for finite rings // Journal of Algebra. — 2013. — V. 379. — P. 441–452.

[4] *Kayal N., Saxena N.* Complexity of ring morphism problems // Computational complexity — 2007. — V. 15. — P. 342–390.

Казанский федеральный университет, Казань
E-mail: ksenypet@mail.ru

Автоматизированные методы порождения фраз, имеющих заданную психосемантику

П. А. Сазонова

Работа посвящена методам автоматизированного порождения фраз с заданной психосемантикой. Предполагается порождение фраз как с определенным пропозициональным содержанием, так и с заданной эмоциональной составляющей. Психосемантика фраз определятся при помощи теории речевых действий (ТРД)[**1**]. Это подход к формализации языка, основанный на представлении целей участников речевого общения. Согласно ТРД, каждая фраза естественного языка рассматривается как речевое действие: композиция пропозиционального содержания P и иллокутивной силы F(P). Ту часть речевого действия, которая выражает эмоционально-психологическую составляющую фразы, будем называть психосемантикой фразы. Психосемантика задается речевой целью говорящего, лингвистической структурой фразы, смыслом фразы, связанным с уровнями потребностей человека по Маслоу. В данной работе рассматриваются 2 вида потребностей - физические и социальные. Для осуществления процесса порождения фраз были сформированы размеченные словари иллокутивных глаголов, а также словари глаголов, связанных с физическими или социальными потребностями. Был разработан словарь шаблонов лингвистических структур, в котором представлено более 350 шаблонов. На первом этапе автоматизированного порождения фразы подбирается лингвистическая структура предложения на основании модели ситуации. На втором этапе осуществляется поиск слов в размеченных словарях в зависимости от выбранного типа речевого действия, интенсивности речевого действия и от заданного пропозиционального содержания фразы. На третьем этапе происходит подстановка подобранных слов в лингвистическую структуру: слова приводятся к заданным формам (род, вид, число, падеж и др.) и выстраиваются в нужном порядке. Алгоритм реализован на языке Python 3.4, с использованием сторонней библиотеки морфологического анализатора pymorphy2. Указанные методы предполагается применить, в частности, для проведения психофизиологических исследований. Ранее было показано, что фразы с различной психосемантикой оказывают на слушателей различное психофизиологическое воздействие [**2**].

Список литературы

[1] *Pal'chunov D. E.* Algebraische Beschreibung der Bedeutung von Aeusserungen der natuerlichen Sprache. // In: GABEK. Verarbeitung und Darstellung von Wissen. Innsbruck-Wien: STUDIENVerlag, 1999, 310-326.

[2] *Савостьянов А. Н., Богомаз С. А., Пальчунов Д. Е., Будакова А. В., Залешин М. С., Гуляев А. С., Сапрыгин А. Е.* ЭЭГ реакции в условиях распознавания предложений с различным отношением к личностной оценке испытуемого // Теоретическая и экспериментальная психология, т. 5, № 3 - 2012. - с. 48-55.

Новосибирский государственный университет, Новосибирск
E-mail: psazonova@gmail.com

Поиск определений терминов и связей между ними для построения онтологий при помощи языка описания лингвистических шаблонов

П. А. Степанов

В последнее время особенно важными задачами стали задачи, связанные с анализом текстов естественного языка, а также извлечением из них онтологических знаний. Часто анализ текстов проводится с целью построения онтологий предметных областей, сложно осуществимый вручную.

Задачей, в рамках которой проводилась данная работа, был анализ текстов медицинских справочников, статей и других научных трудов. Реализована программная система, осуществляющая помощь эксперту в построении онтологии предметной области. По заданному множеству терминов осуществлялся поиск всех участков текста, которые могут содержать определение данных терминов или онтологические отношения между ними. Данный инструмент позволяет отфильтровать значительные объёмы текста и сэкономить время, которое эксперт затратит на извлечение определений терминов и формализацию связей между ними. Следует отметить, что разработанный инструмент предназначен для помощи эксперту в извлечении онтологических знаний, отличия которых от знаний общего характера приведены в статье [**1**].

Текст анализировался с привлечением языка описания лингвистических шаблонов [**2**], который позволяет проводить поиск участков текста, удовлетворяющих заданным грамматическим и синтаксическим условиям. Также при анализе текста применялся подход множеств интерпретаций [**3**], который позволяет на всех стадиях анализа текста корректно обрабатывать все возможные результаты, рассматривая их в качестве альтернатив.

На первом этапе поиска возможных определений термина разработанный инструмент производил поиск вхождений этого термина в стандартные «определяющие» конструкции, выраженные в виде лингвистических шаблонов. На втором этапе поиска отношений между терминами производился поиск вхождений терминов в конструкции связей. В результате тестирования разработанного инструмента были получены удовлетворительные результаты. Точность поиска определений составила 74%, полнота - 92%. Производился поиск связей типа «общее-частное», «часть-целое», а также связей «осложнение заболевания» и «симптом заболевания». Точность поиска связей между терминами составила 67%, полнота - 87%. При этом было отфильтровано 94% исходного текста, что, несомненно, упростило бы работу эксперта.

Список литературы

[1] *Пальчунов Д. Е., Степанов П. А.* Применение теоретико-модельных методов извлечения онтологических знаний в предметной области информационной безопасности // Программная инженерия, 2013, № 11, с. 8-16.

[2] *Степанов П. А.* Язык описания лингвистических шаблонов // Материалы Всероссийской конференции с международным участием "Знания-Онтологии-Теории". - 2013. - Том 2. - С. 136-145.

[3] *Степанов П. А.* Автоматизация обработки текстов естественного языка // Вестник НГУ. Серия: Информационные технологии. - 2013. - Том 11; № 2. - С. 106-112.

Новосибирский государственный университет, Новосибирск
E-mail: stefan.nsk@gmail.com

Автоматическая оценка криптостойкости алгебраически гомоморфных криптосистем, основанных на факторизации чисел

А. В. Трепачева

Гомоморфная криптосхема – это четверка алгоритмов KeyGen, Encrypt, Decrypt, Evaluate, имеющих фиксированную спецификацию [**3**]. Эти алгоритмы могут быть заданы в виде семейств (параметризованных некоторым параметром уровня криптостойкости λ) так называемых схем из функциональных элементов (СФЭ) представляющих собой наборы полиномиальных формул от многих переменных.

Желание построить полностью гомоморфную криптосхему на основе задачи факторизации чисел возникло довольно давно и не потеряло актуальность до сих пор [**3**]. Однако имеющиеся попытки не показали высокой криптостойкости по ряду схожих причин – некоторым их свойствам, которые можно выделить на основе их криптоанализа [**2, 1, 5, 4, 6**].

Рассматривается следующая задача: по формальному описанию криптосхемы (с криптостойкостью, обоснованной через факторизацию чисел) на специализированном языке (синтаксис которого будет описан), установить справедливость для неё некоторых свойств.

Рассматриваемую задачу можно назвать *автоматическим символьным криптоанализом* (или автоматическим формальным криптоанализом).

Работа выполнена при поддержке гранта РФФИ №15-07-00597 А «Разработка и исследование алгоритмов полностью гомоморфного шифрования»

Список литературы

[1] *Trepacheva A.* Cryptanalysis of polynomial based homomorphic encryption. In *Proceedings of the 7th International Conference on Security of Information and Networks*, page 205. ACM, 2014.

[2] *Trepacheva A. and Babenko L.* Known plaintexts attack on polynomial based homomorphic encryption // In Proceedings of the 7th International Conference on Security of Information and Networks, p. 157. ACM, 2014.

[3] *Vaikuntanathan V.* Computing blindfolded: New developments in fully homomorphic encryption // In Foundations of Computer Science (FOCS), 2011 IEEE 52nd Annual Symposium on, p. 5–16. IEEE, 2011.

[4] *Vizár D. and Vaudenay S.* Analysis of chosen symmetric homomorphic schemes // In Central European Crypto Conference, number EPFL-CONF-198992, 2014.

[5] *Трепачева А. В.* Криптоанализ шифров, основанных на гомоморфизмах полиномиальных колец // Известия Южного федерального университета. Технические науки, 157(8):96–107, 2014.

[6] *Трепачева А. В.* Улучшенная атака по известным открытым текстам на гомоморфную криптосистему Доминго-Феррера // Труды Института системного программирования РАН, 26(5):83–98, 2014.

Южный федеральный университет, Ростов-на-Дону
E-mail: alina1989malina@ya.ru, atrepacheva@sfedu.ru

О представлении корневых деревьев множеством последовательностей

Г. В. Чернышев

Существуют различные способы представления деревьев в виде вложенных последовательностей, множеств. Мы рассматриваем корневое дерево как множество последовательностей объектов (вершин) от фиксированного объекта (корня) до других объектов.

Формальное описание базируем на языке теории категорий, вводим: класс объектов $O = \{v_1, v_2, \ldots, v_i, \ldots\}$; множество морфизмов $M(v_i, v_j) = \langle v_i, v_{i_1}, \ldots v_j \rangle$ для $v_i, v_j \in O$; композицию морфизмов ($\circ$), определяемую правилом конкатенации последовательностей; единичные морфизмы $1_v = \langle v \rangle$ для каждого $v \in O$.

В докладе будут изложены результаты исследований свойств данной категории и прикладные аспекты их использования в информационных технологиях, базирующихся на иерархических структурах.

В частности, будет показано, что подмножество характеристических морфизмов χ_{v_t} вида $M(v_R, v_t)$, где v_R — фиксированный объект, а v_t — терминальный объект, является образующим для категории.

Для приложений важной является

Теорема. *Для произвольных объектов $a, b \in O$*

$$M(a,b) = (\chi_a \ominus \chi_{a\times b}) \circ (\chi_b \ominus \chi_{a\times b})^{-1},$$

где $a \times b$ — произведение объектов a и b, $\ominus$ — операция разности харктеристических морфизмов, $M^{-1}(a,b) = M(b,a)$.

Формула, приведенная в формулировке теоремы, подсказывает процедуру вычисления путей между произвольными вершинами дерева.

Рассматриваемое представление деревьев позволяет также определить структурные свойства деревьев, связанные с реулярностями различных типов.

ФГБУН Институт информатики и проблем регионального управления КБНЦ РАН, г.Нальчик
E-mail: chern_gen@mail333.com

Критические корневые диаграммы и корневые многочлены в полиномиальном синтезе алгоритмов автоматического управления

А. В. Чехонадских

Принципиальные свойства линейной системы автоматического управления (устойчивость, ограниченная колебательность и др.) обеспечиваются расположением в левой комплексной полуплоскости её полюсов $z_1, \ldots, z_n$ - корней характеристического многочлена $f_p(s) = s^n + a_{n-1}(C)s^{n-1} + \ldots + a_1(C)s + a_0(C)$, где $C = c_1; \ldots; c_k$ - вектор параметров регулятора. Для регулятора полного порядка расположение полюсов можно задавать произвольно; для регулятора пониженного порядка задача принимает оптимизационный характер: ищется такое значение C^*, при котором область расположения полюсов типа полуплоскости $\{s \mid \operatorname{Re} s \leq \alpha\}$ или конуса $\{s \mid \operatorname{Re} s + |\operatorname{Im} s| \leq \alpha\}$ смещается как можно дальше влево; величина α при этом минимизируется. Размерность вектора C позволяет достигать k равенств между действительными и мнимыми частями корней, за счёт чего критические (в том числе оптимальные и субоптимальные) расположения характеризуются попаданием на правую границу области максимально возможного количества полюсов. Схематическое расположение граничных полюсов $z_1, \ldots, z_m$ кратностей $r_1, \ldots, r_m$ представляется критическими корневыми диаграммами [**1**]. Их список строится рекуррентно, а число растёт по закону Фибоначчи:

Теорема. *Число различных корневых диаграмм, задаваемых k равенствами, равно $(k+3)$-му числу Фибоначчи φ_{k+3}.*

Корневой диаграмме можно однозначно сопоставить корневой многочлен $p(s) = (s - z_1)^{r_1} \ldots (s - z_m)^{r_m}$, включающий множители с граничными полюсами; с помощью корневых многочленов осуществляется нахождение оптимальных параметров C^* [**1**]. Число $P(k)$ корневых многочленов выражается через разбиения натуральных чисел (начальный отрезок C^* совпадает с последовательностью A036469 частичных сумм разбиений натуральных чисел на нечетные слагаемые [**2**]), а эффективное построение списка осуществляется лексикографически.

Список литературы

[1] *Чехонадских А. В.* Экстремальные расположения полюсов систем автоматического управления с регулятором пониженного порядка // Автоматика и телемеханика. 2014. № 10. С.6-24.

[2] URL: http://oeis.org/A036469

Новосибирский государственный технический университет, Новосибирск
E-mail: alcheh@ngs.ru

О теоретико-модельной формализации многошаговых компьютерных атак

Г. Э. Яхъяева, А. А. Ершов

Современный этап развития общества характеризуется возрастающей ролью информационной сферы. В связи с этим, проблема информационной безопасности становится все более и более актуальной. Для эффективной защиты от компьютерной атаки необходимо как можно раньше определить, какая именно атака проводится на информационную систему. Если атака проводится в несколько шагов, идентифицировать её становится сложнее, так как симптомы могут не сразу указывать на конечную цель и способ проведения атаки. Таким образом, возникает необходимость в формализациях, способных моделировать и подсчитывать риски в многошаговых кибератаках.

В настоящей работе для моделирования многошаговых компьютерных атак мы рассматриваем конечное множество прецедентов компьютерных атак. Каждый прецедент формализуется в виде класса алгебраических систем заданной сигнатуры. На основе данных прецедентов строится обобщённая нечёткая модель, позволяющая просчитывать риски в одношаговых компьютерных атаках.

На множестве прецедентов кибератак задается бинарное транзитивное отношение. Два прецедента находятся в данном отношении, если реализация первого прецедента открывает уязвимость, приводящую к возможности проведения второй атаки. Множество прецедентов с данным отношением образуют обобщённую структуру Крипке, позволяющую, с учётом неполноты знаний о прецедентах атак, описывать многошаговые кибератаки. Модальности в данной структуре интерпретируются как «возможность» и «необходимость» событий в многошаговых атаках. Фазификация такой структуры приводит к обобщённой нечёткой модели, позволяющей просчитывать риски в многошаговых атаках.

В рамках данной работы был разработан алгоритм вычисления интервальных значений истинности модальных предложений на заданной обобщённой нечёткой модели. Данный алгоритм осуществляет постфиксный обход графа в глубину и базируется на алгоритме маркировки [**1**] и на алгоритме подсчёта интервальных значений истинности предложений, не содержащих модальностей [**2**].

Список литературы

[1] *Handbook* of Modal Logic // P. Blackburn et al. (Editors), Elsevier, 2007, 1231 p.

[2] *Яхъяева Г. Э., Ясинская О. В.* Методы согласования знаний по компьютерной безопасности, извлечённых из различных документов. // Вестник НГУ. Серия: Информационные технологии. 2013. Т. 11, вып. 3. с. 63-73.

Новосибирский государственный университет, Новосибирск
E-mail: gul_nara@mail.ru, alaershov@gmail.com

Прецедентный подход к формализации знаний о предметной области

Г. Э. Яхъяева, О. В. Ясинская

В данной работе мы рассматриваем логику предикатов без равенства. Пусть у нас имеется некоторая предметная область Δ . Сигатура σ — это множество понятий, на языке которых описывается предметная область Δ, A — множество объектов предметной области Δ. Аналитическая теория предметной области Δ является непротиворечивой теорией T_Δ сигнатуры σ [**1**]. Тогда класс моделей $K_\Delta = \{\mathfrak{A} = \langle A, \sigma\rangle | \mathfrak{A} \models T_\Delta\}$ назовем множеством *потенциальных прецедентов* предметной области Δ.

В работах [**2**], [**3**] были введены понятие *прецедентной модели* $\mathfrak{A}_E$, порожденной конечным множеством прецедентов $E \subseteq K_\Delta$ и понятие *обобщенной нечеткой модели*, порожденной классом прецедентных моделей. Были доказаны теоремы, утверждающие, что значениями истинности предложений на обобщенных нечетких моделях, порожденных нечеткими (интервальными) означиваниями являются интервалы рациональных чисел из отрезка $[0, 1]$.

Однако на практике, мы часто сталкиваемся с неполными описаниями прецедентов предметной области. В этом случае мы вынуждены формализовывать прецеденты не как отдельные модели, а как классы моделей.

Определение. *Рассмотрим непротиворечивую теорию $T \in S(\sigma)$, такую, что $T_\Delta \subseteq T$. Тогда класс моделей $K = \{\mathfrak{A} \in K_\Delta | \mathfrak{A} \models T\}$ назовем обобщенным прецедентом, порожденным теорией T.*

Теорема. *Рассмотрим обобщенные прецеденты $K_1, ..., K_n$, порожденные теориями $T_1, ..., T_n$ соответственно. Пусть $\boldsymbol{K} = \{\mathfrak{A}_E | E \in K_1 \times ... \times K_n\}$ класс прецедентных моделей, порожденный обобщенными прецедентами $K_1, ..., K_n$ и $\mathfrak{A}_{\mathbf{K}}$ — обобщенная нечеткая модель, порожденная классом $\boldsymbol{K}$. Тогда для любого предложения $\varphi \in S(\sigma)$ значением истинности на модели $\mathfrak{A}_{\mathbf{K}}$ является множество $\{\frac{\alpha}{n} |\ \alpha \in N$ и $a \leq \alpha \leq 1 - b\}$, где $a = \|\{i | \varphi \in T_i\}\|$ и $b = \|\{i | \neg\varphi \in T_i\ \}\|\}$.*

Разработан алгоритм вычисления значений истинности бескванторных предложений на обобщенной нечеткой модели $\mathfrak{A}_{\mathbf{K}}$, порожденной конечным множеством обобщенных прецедентов. Данный алгоритм имеет полиномиальную сложность.

Список литературы

[1] *Пальчунов Д. Е.* Моделирование мышления и формализация рефлексии: Ч.1. Теоретико-модельная формализация онтологии и рефлексии // Философия науки, № 4, 2006, с. 86-114.

[2] *Palchunov D. E., Yakhyaeva G. E.* Interval fuzzy algebraic systems // Proceedings of the Asian Logic Conference 2005. World Scientific Publishers. 2006, pp. 23-37.

[3] *Пальчунов Д. Е., Яхъяева Г. Э.* Нечеткие алгебраические системы // Вестник НГУ. Серия: Математика, механика, информатика. 2010. Т.10, вып. 3. С. 75-92

Новосибирский государственный университет, Новосибирск
E-mail: gulnara@mail.ru; yasinskaya.olga@gmail.com

Knowledge representation and undecidability

A. V. Bessonov

In computer science it is commonplace truth that the degree of felicity and adequacy of a chosen way of knowledge representation has a direct bearing on success in solving a posed problem. It turns out that this truth applies also to evaluation of undecidability results.

In proving the incompleteness theorems, K. Gödel represents provability in PA using the provability predicate $\mathrm{Pr}(x, y)$ (which is satisfied iff x is the Gödel number of a formula and y is the Gödel number of its proof) and some arithmetical formula $\mathrm{Prov}(x, y)$ 'expressing' that predicate in PA. But this formula is not the best candidate to represent the *unprovability* in PA. The following is a simple consequence of the second Gödel's theorem showing inadequacy of Gödel's representation of unprovability:

Theorem 2+. (1) *If* PA *is consistent, then, for any formula A, a formula* $\forall y \neg \mathrm{Prov}(\ulcorner A \urcorner, y)$ *that 'expresses' the unprovability of A is unprovable in* PA.

(2) *If* PA *is ω-consistent, then, for any formula A unprovable in* PA, *a formula that 'expresses' the unprovability of A is undecidable in* PA.

Theorem 2+ implies that the formula $\forall y \neg \mathrm{Prov}(\ulcorner \neg(\mathbf{0} = \mathbf{0}) \urcorner, y)$, which 'expresses' the unprovability of a formula $\neg(\mathbf{0} = \mathbf{0})$, is undecidable and, hence, is unprovable in PA. In fact, however, a proof (by contradiction) that $\neg(\mathbf{0} = \mathbf{0})$ is unprovable is quite elementary, provided PA is consistent.

If PA is consistent, and $\neg A$ is a formula provable in PA, then A is obviously unprovable by the definition of consistency. Consider the *unprovability* predicate $\mathrm{NPr}(x, y)$ which is satisfied iff x is the Gödel number of some formula and y is the Gödel number of a proof of its *negation*. (The extension of this predicate does not include all formulas unprovable in PA, but we need only prove a formula 'expressing' unprovability of at least one formula in PA.) Clearly, this predicate is 'expressible' in PA via some formula $\mathrm{NProv}(x, y)$. Let n be the Gödel number of a derivation of the formula $\neg\neg(\mathbf{0} = \mathbf{0})$. The definition of a predicate $\mathrm{NPr}(x, y)$ implies that $\mathrm{NPr}(\ulcorner \neg(0 = 0) \urcorner, n)$ is true. In view of the 'expressibility' conditions, therefore, $\mathrm{NProv}(\ulcorner \neg(\mathbf{0} = \mathbf{0}) \urcorner, \mathbf{n})$ is provable in PA. If existential generalization is applied to this formula, then we are led to a derivation of $\exists y \mathrm{NProv}(\ulcorner \neg(\mathbf{0} = \mathbf{0}) \urcorner, y)$ which 'expresses' the unprovability of a formula $\neg(\mathbf{0} = \mathbf{0})$. (If existential generalization is applied twice, then we arrive at a derivation of $\exists x \exists y \mathrm{NProv}(x, y)$ that 'expresses' the existence of an unprovable formula in PA. Thus PA can well prove its own consistency!)

Hence an informal statement "$\neg(\mathbf{0} = \mathbf{0})$ is unprovable in PA, provided PA is consistent," which is undecidable in PA via Godel's representation, turns out provable in PA via another representation. This implies that the available undecidability results should be re-evaluated with due regard for variability of ways for representing informally formulated problems.

Institute of Philosophy and Law, Siberian Branch, Russian Academy of Sciences,
Novosibirsk State University, Novosibirsk (Russia)
E-mail: trt@academ.org

Boolean models of some nonlinear dynamic systems

V. P. Golubyatnikov, M. V. Kazantsev

We consider n-dimensional nonlinear dynamical systems

$$\dot{x_1} = f_1(x_n) - x_1, \qquad \dot{x_i} = f_i(x_{i-1}) - x_i, \qquad i \in \{2 \dots n\}, \qquad x_j \geq 0 \tag{1}$$

as gene network models. All the functions f_i here are non-negative and smooth or piecewise constant. We assume that all of them are monotonically non-increasing (L-functions) or monotonically non-decreasing (Γ-functions). This corresponds, respectively, to negative and positive feedbacks in gene networks. Let x^* be an equilibrium point of the system (1) surrounded by an invariant parallelepiped Q. We decompose Q by hyperplanes containing x^* and parallel to coordinate hyperplanes. The constructed smaller 2^n parallelepipeds $\{\varepsilon_1, \dots, \varepsilon_n\}$ of this decomposition are enumerated by boolean indices: $\varepsilon_i = 0$ if $0 \leq x_i \leq x_i^*$, $\varepsilon_i = 1$ if $x_i^* < x_i$.

Let G be the oriented graph (**domain graph**) such that its vertices correspond to the parallelepipeds of the decomposition of Q, and directions of arcs correspond to directions of trajectories of the system (1), cf. [**1**].

For the system (1) we define *characteristic vector* Ψ of length n. $\Psi_i = 1$ if f_i is a Γ-function and $\Psi_i = 0$ if f_i is an L-function. Given n, there are 2^n systems with different characteristic vectors.

We call the system (1) **even** if $\sum \Psi_i = 0 \pmod 2$ and **odd** if $\sum \Psi_i = 1 \pmod 2$.

We define inversion operator $\Phi = Inv_i(\Psi)$ as follows:

$$\Phi_i = \Psi_i | i \notin \{i-1, i\}, \qquad \Phi_i = \Psi_i \oplus 1 | i \in \{i-1, i\}$$

We assume that $\Psi_0 = \Psi_n, \Psi_{n+1} = \Psi_1$ etc. Here $\oplus$ denotes addition (mod 2).

Operators Inv_i obviously preserve parity of system for any i. Moreover, applying sequence of operators Inv_i with different i any characteristic vector may be transformed into any other vector with same parity.

Lemma 1. *A loop in G exists on its every potential level except n and 0.*

Lemma 2. *Domain graphs of systems with characteristic vectors Ψ and $Inv_i(\Psi)$ are isomorphic for any i.*

Theorem. *Domain graphs of all dynamic systems of same dimension and same parity are isomorphic to each other.*

The work was supported by RFBR, grant 15-01-00745.

References

[1] *Akinshin A. A., Golubyanikov V. P.* On cycles in symmetric dynamical systems // Bull. NSU. 2012. V. 12. N. 2 P. 3–12.

Sobolev Institute of Mathematics, Novosibirsk,Russia;
Altai state technical university, Barnaul, Russia
E-mail: glbtn@math.nsc.ru, markynaz.astu@gmail.com

Formalized Proof of Soundness of Hoare Type Theory

E. Makarov, C. Skalka

We prove the soundness of the Hoare Type Theory (HTT) [**1**], an extension of Hoare logic for a functional programming language with side effects (assignment). Our proof is formalized in the proof assistant Coq.

The behavior of pure functional programs can be specified and proved using expressive type systems. However, research progress in verification of higher-order programs with side effects has been slower despite the importance of this topic. Imperative, as opposed to functional, programs can be proved using Hoare logic. It uses judgments of the form $\{P\}M\{Q\}$, where M is a program and P and Q are pre- and postconditions, respectively. Separation logic extends Hoare logic by making it possible to talk about pointers. In turn, HTT adapts separation logic to functional programs. Soundness of HTT was proved using a rather complicated argument using a realizability model.

We developed a simpler proof of HTT soundness based on preservation of types. Unlike the previous proof, ours was fully verified in the Coq proof assistant. Moreover, this formalization can be used for writing and verifying programs. Formalizing a logical calculus involves an encoding of syntax, which can turn programs subject to verification into hard-to-understand syntactic objects. Instead, our formalization allows writing pure parts of programs directly in Coq, which itself is a type system similar to the pure fragment of HTT, and to use new constructs only for effectful operations, which are not available in Coq.

The result is a single system whose soundness is proved in Coq and that can be used in practice for proving programs. For each verified effectful program we have a complete Coq proof that the program behaves according to its specification.

HTT was previously implemented in Coq in the Ynot project [**2**]. However, that implementation does not formalize syntax and does not prove HTT soundness. Our Coq implementation is also more robust because it does not use axioms that conflict with classical logic.

References

[1] *Chlipala A., Malecha G., Morrisett G., Shinnar A. and Wisnesky R.* Effective interactive proofs for higher-order imperative programs. In ICFP ’09.

[2] *Chlipala A. et al.* Ynot project. `http://ynot.cs.harvard.edu`.

Lobachevsky State University of Nizhni Novgorod, Russia
The University of Vermont, USA
E-mail: emakarov@gmail.com

Metric space $P_{k_1} \times P_{k_2} \times ... \times P_{k_m}$ in regard to Hamming distance

Seymur Meshaik

Under the direct product of Post algebras we shall understand their product as graded algebras [**1**]:

$$P_{k_1} \times ... \times P_{k_m} =< \bigcup_{n=1}^{\infty} P_{k_1}^{(n)} \times ... \times P_{k_m}^{(n)}; \zeta, \tau, \Delta, \nabla, * >,$$

where P_{k_i} are complete Post algebras on sets $E_{k_i} = \{0, 1, ..., k_i - 1\}$.

We define a Hamming distance $d\,(A,\, B)$ between sequences $A = (a_1,\, a_2,\, ...,\, a_n)$ and $B = (b_1,\, b_2,\, ...,\, b_n)$ of the size n as a number of pares of components a_i and b_i, such that $a_i \neq b_i$ [**2**].

Let $f =< f_1,\, f_2,\, ...,\, f_m >$ and $g =< g_1,\, g_2,\, ..., g_m >$ be functions of n variables in $P_{k_1} \times P_{k_2} \times ... \times P_{k_m}$. The expressions $d\,(f,\, g) = n\,(A_1 \bigcup A_2 \bigcup ... \bigcup A_m)$ define the Hemming distance $d\,(f,\, g)$ between the functions f and g, where A_i are the set of pares of the values of the functions f and g which differs one from another by i-th component. If $d\,(f_i,\, g_i) = \chi_i$ then

$n\,(A_i) = \chi_i \cdot \prod_{j=1}^{m} k_j^n$; $n\,(A_{i_1} \bigcap A_{i_2}) = \chi_{i_1} \cdot \chi_{i_2} \cdot \prod_{j=1}^{m} k_j^n$; ... ; $n\,(A_1 \bigcap A_2 \bigcap ... \bigcap A_m) = \prod_{i=1}^{m} \chi_i$ and

$$d\,(f,\, g) = n\left(A_1 \bigcup A_2 \bigcup ... \bigcup A_m\right) = \delta_1 - \delta_2 + ... + (-1)^m\, \delta_m$$

where $\delta_1 = \sum_i n\,(A_i)\,,\;\; \delta_2 = \sum_{i_1,\, i_2} n\,(A_{i_1} \bigcap A_{i_2})\,,\;\; ...,\;\; \delta_m = n\,(A_1 \bigcap A_2 \bigcap ... \bigcap A_m)$.

Theorem. The Hamming distance between functions from the product $P_{k_1} \times P_{k_2} \times ... \times P_{k_m}$ *is a metric, and the corresponding set of functions* $P_{k_1} \times P_{k_2} \times ... \times P_{k_m}$ *is a metric space defined by Hamming distance* $d\,(f,\, g)$.

References

[1] *Maltsev A. I., Maltsev I. A.* Iterative Post algebras (rus). Novosibirsk, 2009.
[2] *Berlecamp E.* Algebraic theory of coding (rus). Moscow, 1971.
[3] *Meshaik S.* Hamming distance between the functions of direct product of Post algebras (rus). "Natural and Technical sciences", N 3, Moscow.

Ganja State University, Ganja, Azerbaijan
E-mail: seymur_meshaik@inbox.ru

A generalization of the Feistel cipher

V. A. Nosov, A. E. Pankratiev

The Feistel cipher [**1**] is a widely used encryption scheme which transforms plaintext blocks splitted into two equal pieces, (L_0, R_0), into blocks of ciphertext by the rule

$$\begin{cases} L_1 = R_0 \\ R_1 = L_0 \oplus F(R_0, K_0), \end{cases}$$

(K_0 is a key). This scheme is usually iterated with an appropriate key schedule.

We consider a cipher that applies to bit strings of length $n = 2^k$ and transforms the plaintext block $x = (x_1, x_2, \ldots, x_n)$ into the block $y = (y_1, y_2, \ldots, y_n)$ by the rule

$$y_j = x_j + f_j(p_1(x_1), p_2(x_2), \ldots, p_n(x_n)) \qquad j = \overline{1, n}, \tag{1}$$

where p_i, and f_i, $i = \overline{1, n}$, are Boolean functions of 1 and n variables, respectively.

We find conditions on the family $F_0 = \{f_1, f_2, \ldots, f_n\}$ under which the mapping (1) is bijective for any choice of $p_1, p_2, \ldots, p_n$.

Theorem. *The mapping* (1) *is bijective for any functions* p_i, $i = \overline{1, n}$, *if and only if the family* F_0 *is proper* [**2**] *(that is, for any distinct* n*-tuples* $x' = (x'_1, x'_2, \ldots, x'_n)$ *and* $x'' = (x''_1, x''_2, \ldots, x''_n)$ *one can find an index* α *such that* $x'_\alpha \neq x''_\alpha$ *and* $f_\alpha(x') = f_\alpha(x'')$*).*

Now we split the input bit string into digrams $(x_1, x_2, \ldots, x_n) \to (x'_1, x'_2, \ldots, x'_{n/2})$, $x'_i = (x_{2i-1}, x_{2i})$, and define the transformation $x' \to y'$ of the digram string:

$$y'_j = x'_j + f'_j(p'_1(x'_1), p'_2(x'_2), \ldots, p'_{n/2}(x'_{n/2})), \qquad j = \overline{1, n/2}. \tag{2}$$

Here p'_i, and f'_i, $i = \overline{1, n}$, are functions of 4-valued logic.

Further partitioning of the input string into digrams and thereby doubling the set of the values gives at step $(k-1)$ two half-blocks $x_1^{(k-1)} = (x_1, x_2, \ldots, x_{2^{k-1}})$, $x_2^{(k-1)} = (x_{2^{k-1}+1}, x_{2^{k-1}+2}, \ldots, x_{2^k})$, which are transformed by the rule

$$y_j^{(k-1)} = x_j^{(k-1)} + f_j^{(k-1)}(p_1^{(k-1)}(x_1^{(k-1)}), p_2^{(k-1)}(x_2^{(k-1)})), \qquad j = 1, 2. \tag{$k-1$}$$

Theorem. *The mapping* $(k-1)$ *is bijective for any* $p_1^{(k-1)}, p_2^{(k-1)}$ *if and only if the family* $\{f_1^{(k-1)}, f_2^{(k-1)}\}$ *is proper; in the case of two functions it means that one of them is constant and the other one does not depend on the same-name argument.*

It is easily seen that we arrive at the original Feistel cipher.

Thus, in this work we suggest generalizing the Feistel cipher by splitting the input block into more than two parts, fixing a proper family of functions $\{f_j\}$, and using transformations (1), (2), ..., $(k-1)$ with functions p_j treated as changeable keys.

References

[1] *Feistel H.* Cryptography and Computer Privacy
Scientific American, 228 (5), 1973, 15–23.

[2] *Nosov V. A., Pankratiev A. E.* Latin squares over Abelian groups, J. Math. Sci., 2008, **149** (3), 1230–1234.

Lomonosov Moscow State University, Moscow (Russia)
E-mail: anton.pankratiev@gmail.com

III. Секция «Теория вычислимости»

Об A–вычислимых нумерациях

С. А. Бадаев, А. А. Исахов

Неопределяемые нами понятия можно найти в монографии Ю.Л. Ершова [**1**].

Вычислимые нумерации семейств арифметических множеств привлекают внимание многих авторов. Основные направления исследований таких нумераций и многие нерешенные к концу прошлого века проблемы были сформулированы в обзоре [**2**]. Позже в работе [**3**] было замечено, что равномерные перечисления, вычислимые относительно тьюринговых скачков пустого множества, свойственные вычислимым нумерациям семейств арифметических множеств, во многих случаях могут быть обобщены на конструкции с использованием произвольных оракулов. В связи с этим в [**3**] были сформулированы естественные вопросы о вычислимых нумерациях над произвольными оракулами. На некоторые из них ответы сформулированы ниже.

Определение. Пусть A – произвольное множество натуральных чисел. Нумерация ν семейства A–вычислимых множеств S называется A–вычислимой, если универсальное множество этой нумерации $\{< x, n >: x \in \nu(n)\}$ является вычислимо перечислимым относительно оракула A.

Теорема 1. *Для любого A всякое конечное семейство A–вычислимо перечислимых множеств, содержащее наименьшее по включению множество, имеет A-вычислимую универсальную нумерацию.*

Теорема 2. *Пусть A – произвольное множество и пусть S – бесконечное A-вычислимое семейство всюду определенных функций. Тогда, с точностью до эквивалентности, если S имеет две A-вычислимых фридберговых нумераций, то S имеет бесконечно много таких нумераций.*

Список литературы

[1] *Ершов Ю. Л.* Теория нумераций, М.: Наука, Москва, 1977.

[2] *Badaev S. A., Goncharov S. S.* Theory of numberings: open problems. Computability Theory and its Applications. P. Cholak, S. Lempp, M. Lerman and R. Shore eds. Contemporary Mathematics, American Mathematical Society, Providence, 257, 23–38 (2000).

[3] *Badaev S. A., Goncharov S. S.* Обобщенно вычислимые универсальные нумерации. Алгебра и логика, 53, No. 5, 555–569 (2014).

Казахский национальный университет им. аль-Фараби, Алматы
E-mail: serikzhan.badaev@kaznu.kz, asylissakhov@mai.ru

Структура m-степеней внутри Q-степеней

И. И. Батыршин

Одним из основных вопросов в теории вычислимости, касающихся различных типов алгоритмических сводимостей, является вопрос о структуре степеней более сильной сводимости внутри степени более слабой сводимости.

Пусть r_1 и r_2 - такие алгоритмические сводимости, что для всех множеств A и B выполняется $A \leq_{r_1} B \Rightarrow A \leq_{r_2} B$, тогда каждая r_2-степень состоит из некоторой совокупности r_1-степеней. Возникает естественный вопрос, существует ли такая r_2-степень, которая состоит ровно из одной r_1-степени, или ровно из $n \in \omega$ r_1-степеней? Какова ситуация с вычислимо перечислимыми (в.п.) степенями: существует ли такая в.п. r_2-степень, которая состоит ровно из одной в.п. r_1-степени?

Классическим результатом в сфере изучения структуры в.п. степеней одной алгоритмической сводимости внутри в.п. степени другой алгоритмической сводимости является результат Дегтева [**1**], который показал, что существует в.п. не вычислимая tt-степень, состоящая из единственной в.п. m-степени (т.е. существует такое в.п. невычислимое A, что для всех в.п. множеств W_i, если $B \equiv_{tt} A$, то $B \equiv_m A$).

В работе [**2**] Доуни и Чолак обобщили этот результат, показав, что для любого $n \in \omega$ существует в.п. tt-степень, состоящая ровно из n в.п. m-степеней.

Оманадзе [**3**] показал, что результат Доуни и Чолака не имеет места для Q-сводимости, и поставил вопрос [**4**], верен ли для Q-сводимости результат Дегтева, а именно существует ли невычислимая в.п. Q-степень, состоящая ровно из одной в.п. m-степени?

В докладе будут подробно проанализирована проблематика структур степеней более сильных сводимостей внутри степеней более слабых сводимостей и дан положительный ответ на поставленный выше вопрос, а именно будет построена такая невычислимая в.п. Q-степень, которая состоит ровно из одной в.п. m-степени.

Теорема. *Существует в.п. не вычислимое множество A, такое что для всех в.п. W_i, если $W_i \equiv_Q A$, то $W_i \equiv_m A$.*

Список литературы

[1] *Дегтев А. Н.* tt- и m-степени // Алгебра и Логика. Т. 12 (2), 1973, с. 143-161.

[2] *Cholak P., Downey R. G.* Recursively enumerable m - and tt -degrees, III. Realizing all finite distributive lattices // J. London Math. Soc. 1994. V. 50. № 3. P. 440–453.

[3] *Оманадзе Р. Ш.* Соотношения между некоторыми сводимостями // Алгебра и логика. 1994. Т. 33. №6. С. 681–688.

[4] *Omanadze R.Sh., Chitaia I.O.* Q1-degrees of c.e. sets // Arch. Math. Logic. 2012. V. 51. N 5-6. P. 503–515.

Казанский (Приволжский) федеральный университет, Казань
E-mail: batyrshin@gmail.com

Об одной сводимости Σ^0_2-множеств и последовательностей из Σ^0_2-множеств

Д. Х. Зайнетдинов

Работа посвящена исследованию предельно монотонных функций, предельно монотонных множеств, а также изучению свойств предельно монотонной сводимости (иначе, lm-сводимости) между Σ^0_2-множествами. Основные определения можно найти, например, в работах [1] и [2].

Понятие предельно монотонной последовательности было введено в работе [3]. Основные результаты, полученные при исследовании предельно монотонных функций и множеств приведены в обзорной работе [4].

В представленной работе также будет введено определение lm-сводимости между двумя последовательностями, состоящими из Σ^0_2-множеств, которое опирается на понятие Σ-сводимости на семействах подмножеств натуральных чисел, введенное в работе [5]. Кроме того, будет рассмотрена lm-сводимость между данным множеством и парой множеств.

В работе получены следующие основные результаты:

Теорема 1. *Пусть дана произвольная последовательность $\mathcal{C} = \{C_n\}_{n\in\mathbb{N}}$, состоящая из бесконечных Σ^0_2-множеств, которая не является предельно монотонной. Тогда существует такое Σ^0_2-множество A, что A не предельно монотонно и $\mathcal{C} \not\leq_{lm} A$.*

Теорема 2. *Пусть $\mathcal{A} = \{A_n\}_{n\in\mathbb{N}}$ – это произвольная бесконечная последовательность, состоящая из бесконечных Σ^0_2-множеств. Тогда существует такое Σ^0_2-множество B, что $B \not\leq_{lm} \mathcal{A}$.*

Работа выполнена при финансовой поддержке РФФИ, проект № 14-01-31200.

Список литературы

[1] *Faizrahmanov M., Kalimullin I., Zainetdinov D.* Maximality and minimality under limitwise monotonic reducibility // Lobachevskii Journal of Mathematics. 2014. V. 35, No 4. P. 333–338.

[2] *Зайнетдинов Д. Х., Калимуллин И. Ш.* О предельно монотонной сводимости Σ^0_2-множеств // Учен. зап. Казан. гос. ун-та. Сер. Физ.-матем. науки. 2014. Т. 156, № 1. С. 220–30.

[3] *Kalimullin I., Khoussainov B., Melnikov A.* Limitwise monotonic sequences and degree spectra of structures // Proc. Amer. Math. Soc. 2013. V. 141, No 9. P. 3275–3289.

[4] *Downey R. G., Kach A. M., Turetsky D.* Limitwise monotonic functions and their applications // Proceedings of the Eleventh Annual Asian Logic Conference, World Sci. Publ., Hackensack, NJ (2012), pp. 59–85.

[5] *Калимуллин И. Ш., Пузаренко В. Г.* О сводимости на семействах // Алгебра и логика. 2009. Т. 48, № 1. С. 31–53.

Казанский (Приволжский) федеральный университет, Казань
E-mail: damir.zh@mail.ru

Префиксная и Бюхи разрешимость сверхслов при автоматных преобразованиях

Н. Н. Корнеева

В работе рассматривается действие конечных автоматов Мили и конечных асинхронных автоматов на префиксно разрешимые и разрешимые по Бюхи сверхслова над конечным алфавитом. Сверхслово называется префиксно разрешимым ([1]), если для любого регулярного языка можно определить, существует ли префикс сверхслова, принадлежащий этому языку. Сверхслово называется разрешимым по Бюхи ([1]), если для любого регулярного языка можно определить, бесконечно ли пересечение данного языка и множества префиксов сверхслова. Разрешимые по Бюхи сверхслова являются, очевидно, префиксно разрешимыми.

Теорема 1. *Пусть* $(S, \Sigma, \Sigma', \delta, \omega, s_0)$ *– конечный инициальный автомат Мили или конечный инициальный асинхронный автомат,* $x \in \Sigma^\infty$ *– префиксно разрешимое сверхслово. Тогда* $\omega(s_0, x) \in (\Sigma')^\infty$ *– префиксно разрешимое сверхслово.*

Аналогичный результат для разрешимых по Бюхи сверхслов доказан в работах [2] и [3] для конечно и асинхронно автоматной сводимости соответственно.

Конечно и асинхронно автоматные сводимости на множестве сверхслов естественным образом индуцируют отношения эквивалентности на этом множестве. В данной работе показано существование атомов из сверхслов со свойством префиксной и Бюхи разрешимости в возникающих частично упорядоченных множествах степеней.

Теорема 2. *Существует атом структуры степеней конечно–автоматных преобразований и существует атом структуры степеней асинхронно автоматных преобразований, состоящие из префиксно разрешимых, но неразрешимых по Бюхи сверхслов.*

Теорема 3. *Существует атом структуры степеней асинхронно автоматных преобразований, состоящий из разрешимых по Бюхи сверхслов.*

Существование атома структуры степеней конечно–автоматных преобразований, состоящего из разрешимых по Бюхи сверхслов, было показано в [2].

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований 14-01-31200 мол_а.

Список литературы

[1] *Вялый М. Н., Рубцов А. А.* Алгоритмическая разрешимость задач о поведении автоматов на сверхсловах. Дискретный анализ и исследование операций. 2012. Т. 19. № 2. С. 3–18.

[2] *Байрашева В. Р.* Степени автоматных преобразований почти периодических сверхслов и сверхслов с разрешимой монадической теорией. Казань, 1989. 29 с. Деп. в ВИНИТИ 11.05.1989 № 3103–В89.

[3] *Корнеева Н. Н.* Об автоматных преобразованиях и монадических теориях бесконечных последовательностей. Известия вузов. Математика. 2011. № 8. С. 90–93.

Казанский (Приволжский) федеральный университет, Казань
E-mail: Natalia.Korneeva@kpfu.ru

Сложность проблемы вхождения в члены верхнего центрального ряда вычислимых групп

И. В. Латкин

Автором в [1] построена нильпотентная ступени n группа G_l без кручения, для которой по любому набору $e_2, \ldots, e_n$ вычислимо перечислимых тьюринговых степеней можно подобрать такую вычислимую нумерацию α, что при $2 \leqslant j \leqslant n$ проблема вхождения в j-й член нижнего центрального ряда (централ) $\gamma_j G_l$ имеет сложность e_j, т.е. $T(G_l, \gamma_j G_l, \alpha) = e_j$. В [2] описана нильпотентная ступени n группа G_u без кручения, у которой при любом наборе $d_1, \ldots, d_{n-1}$ вычислимо перечислимых тьюринговых степеней существует такая вычислимая нумерация β, что при $1 \leqslant j \leqslant n-1$ проблема вхождения в j-й член верхнего центрального ряда (гиперцентр) $\zeta_j G_u$ имеет сложность d_j, т.е. $T(G_u, \zeta_j G_u, \beta) = d_j$. В [2] также доказано, что для любых наборов $d_1, \ldots, d_{n-1}$ и $e_2, \ldots, e_n$ вычислимо перечислимых степеней у прямого произведения G групп G_l и G_u имеется вычислимая нумерация μ такая, что $T(G, \zeta_i G, \mu) = d_i$ и $T(G, \gamma_j G, \mu) = e_j$ $(1 \leqslant i \leqslant n-1,\ 2 \leqslant j \leqslant n)$, кроме того, группа G обладает вычислимым порядком, не зависящим от вычислимой нумерации. В [1] построена также не автоустойчивая нильпотентная ступени n группа H_l, у которой при каждой вычислимой нумерации ν $T(H_l, \gamma_j H_l, \nu) = e_j$, где $e_2, \ldots, e_n$ — заданный набор вычислимо перечислимых степеней.

В [2] спрашивается: имеется ли нильпотентная группа без кручения со свойствами группы H_l, а также возможна ли подобная ситуация для гиперцентров. На второй вопрос найден частичный ответ.

Теорема. *Для любых данных наборов $d_1, \ldots, d_{n-1}$ и $e_2, \ldots, e_n$ вычислимо перечислимых тьюринговых степеней найдётся нильпотентная ступени n группа H, у которой при каждой вычислимой нумерации проблема вхождения в j-й гиперцентр при $1 \leqslant j \leqslant n-1$ (или централ для $2 \leqslant j \leqslant n$) равна d_j (или e_j), а фактор группа по нему вычислима тогда и только тогда, когда $d_j = 0$ (или $e_j = 0$); при этом если $d_j \neq 0$, то и сам гиперцентр не вычислим. По всякой р.п. степени b можно построить вычислимую нумерацию β группы такую, что $T(H, \tau H, \beta) = b$, поэтому H — не автоустойчивая, где τH — периодическая часть группы H.*

Список литературы

[1] *Латкин И. В.* Алгоритмическая сложность проблемы вхождения в коммутанты и члены нижнего центрального ряда // Сиб. Матем. Ж. 1987. Т. 28, № 5. С. 102–110.

[2] *Csima B. F., Solomon R.* The complexity of central series in nilpotent computable groups // Annals of Pure and Applied Logic. 2011. No 162. P. 667–778.

Восточно-Казахстанский государственный технический университет им. Д. Серикбаева, г. Усть-Каменогорск, Казахстан
E-mail: lativan@yandex.ru

О проведении корректных вычислений при решении нечетких задач

А. А. Лялецкий

Предлагается подход к решению вопроса о том, как, умея совершать какие-то вычислительные действия алгоритмического характера с произвольной совокупностью событий, следует совершать аналогичные действия на нечетких множествах, представляющих прогнозы относительно этих событий. При этом проводится уточнение того, что следует понимать под решением «нечеткой версии» конечно параметризованной задачи, для которой известна алгоритмическая функция вычисления ее «точного» решения.

Для достижения этой цели вводится специальный понятийный аппарат, определяется, какой информации достаточно для нахождения решения «нечеткой версии», и указывается процедура получения этого решения. Проводится математическое обоснование корректности процедуры.

Предлагаемая процедура может быть программно реализована, что делает возможным ее применение в широком спектре практических приложений, имеющих дело с нечеткими множествами и сталкивающихся с задачей нахождения корректного решения нечетких задач.

Киевский национальный университет имени Тараса Шевченко, Киев
E-mail: foraal@mail.ru

Фридберговы нумерации классов всех частично вычислимых функционалов заданного конечного типа

С. С. Оспичев

Р. М. Фридберг в 1958 году показал, что семейство всех одноместных частично вычислимых функций обладает вычислимой нумерацией без повторений. Этот результат породил целое направление исследований в теории нумераций. Было получено множество результатов, доказывающих существование или отсутствие однозначной нумерации семейств различных объектов. Результатом данной работы является переход в классическом результате Фридберга от частично вычислимых функций к функционалам более высоких типов.

Все основные определения и обозначения могут быть найдены в книге Ю. Л. Ершова "Теория нумераций". Отметим лишь некоторые из них.

Определим понятие *типа функционала*. Множество всех типов будем обозначать T.

1. $0 \in T$;
2. Если σ,τ есть типы, то $(\sigma \times \tau)$ и $(\sigma|\tau)$ тоже являются типами;
3. T - наименьшее множество, удовлетворяющее условиям 1 и 2.

Теперь перейдем к определению *частично вычислимых функционалов*. Обозначим через C_σ - семейство всех частично вычислимых функционалов типа σ. Полагаем $C_0 \rightleftharpoons \mathcal{C}$, где $\mathcal{C}$ – семейство всех одноместных частично вычислимых функций. Если C_σ и C_τ уже определены, то полагаем $C_{(\sigma\times\tau)} \rightleftharpoons C_\sigma \times C_\tau$, а $C_{(\sigma|\tau)} \rightleftharpoons \mathfrak{Mor}(C_\sigma, C_\tau)$.

Отметим, что для любого $\sigma \in T$ семейство C_σ обладает главной вычислимой нумерацией. Основным результатом работы является

Теорема. *Для любого $\sigma \in T$ семейство C_σ обладает вычислимой фридберговой нумерацией.*

Работа выполнена при финансовой поддержке Совета по грантам Президента РФ для государственной поддержки ведущих научных школ (проект НШ-860.2014.1). Исследование выполнено при финансововй поддержке РФФИ в рамках научного проекта № 14-01-00376.

ИМ СО РАН, Новосибирск
E-mail: ospichev@math.nsc.ru

О генерической неполноте формальной арифметики

А. Н. Рыбалов

Знаменитая теорема Геделя о неполноте утверждает, что если формальная арифметика непротиворечива, то она неполна, то есть в ней существует недоказуемое и неопровержимое утверждение относительно любой рекурсивной системы аксиом. Возникает вопрос, а если ограничиться не всеми утверждениями, а «почти всеми», что можно сказать о такой генерической полноте формальной арифметики? Другими словами, верно ли, что для «почти любой» (случайной) замкнутой формулы арифметики выводима из некоторого рекурсивного списка аксиом либо сама формула, либо ее отрицание? В данной работе доказывается, что даже если ограничиться некоторым классом множеств «почти всех» арифметических формул, неполнота арифметики сохранится. Другими словами, в любом таком множестве «почти всех» формул (они называются строго генерическими множествами) существует формула, которая сама не выводима и не выводимо ее отрицание. Так же как и теорема Геделя, подобный результат можно получить для любой формальной системы, которая содержит арифметику.

Теорема. *Не существует строго генерического множества арифметических формул $\mathcal{G}$ такого, что для любой формулы $\Phi \in \mathcal{G}$ либо Φ, либо $\neg\Phi$ выводится из фиксированного рекурсивного множества аксиом.*

Институт математики им. С.Л.Соболева СО РАН, г. Омск
E-mail: alexander.rybalov@gmail.com

Экстремальные элементы полурешеток Роджерса обобщенно вычислимых нумераций

М. Х. Файзрахманов

В докладе рассматриваются вопросы об описании оракулов, относительно которых каждое конечное семейство в.п. множеств обладает универсальной нумерацией, каждая универсальная нумерация является предполной, каждое вычислимое семейство имеет минимальную нумерацию.

Казанский (Приволжский) федеральный университет, Казань
E-mail: marat.faizrahmanov@gmail.com

О нильпотентных группах без кручения конечных размерностей

Н. Г. Хисамиев, И. В. Латкин

Пусть μ_n означает некоторую гёделевскую нумерацию группы $UT_n(\mathbb{Q})$, т.е. по данному $m \in \omega$ эффективно определяется матрица $\mu_n m$, и наоборот, по любой матрице из $UT_n(\mathbb{Q})$ находится её μ-номер. Напомним, что максимальная система линейно независимых элементов абелевой группы без кручения называется её базисом, а мощность базиса называется размерностью абелевой группы. Будем говорить, что размерность нильпотентной группы без кручения конечна, если существует её центральный ряд, все секции которого имеют конечную размерность. В [**3**] получены критерии вычислимости нильпотентных групп без кручения конечных размерностей.

Теорема. *Нильпотентная группа без кручения G конечной размерности вычислимо перечислимо определена тогда и только тогда, когда она изоморфна вычислимо перечислимой подгруппе группы $\langle UT_n(\mathbb{Q}), \mu_n \rangle$ при некотором n.*

Следствие. *Вычислимо перечислимо определённая нильпотентная группа без кручения конечной размерности — вычислима.*

В [**4**] доказано, что для нильпотентных групп без кручения бесконечной размерности следствие и теорема не верны.

Список литературы

[1] *Гончаров С. С., Ершов Ю. Л.* Конструктивные модели, Новосибирск: Научная книга, 1999.

[2] *Каргаполов М. И., Мерзляков Ю. И.* Основы теории групп, М., Наука, 1996.

[3] *Нуризинов М. К., Тюлюбергенов Р. К., Хисамиев Н. Г.* Вычислимые нильпотентные группы без кручения, Сибирский математический журнал, 55, №3 (2014), 580–591.

[4] *Латкин И. В.* Арифметическая иерархия нильпотентных групп без кручения, Алгебра и логика, 35, №3 (1996), 308–313.

Восточно-Казахстанский государственный технический университет им. Д. Серикбаева, Усть-Каменогорск

E-mail: hisamiev@mail.ru, lativan@yandex.ru

Categorical and locally finite p-time structures

P. E. Alaev

Let Σ be a finite alphabet and let Σ^* be the set of words in Σ. Below, we consider only structures on subsets of Σ^* for some Σ, i.e., structures $\mathfrak{A} = (A, \ldots)$, where $A \subseteq \Sigma^*$. The definition of a computable structure is standard. We say that $\mathfrak{A}$ is *computable in polynomial time* (*p-time, p-computable*) if A and all functions and predicates of $\mathfrak{A}$ are computable in polynomial time. Remind that a function $f : A \to \Sigma^*$, where $A \subseteq \Sigma^*$, is *p-computable* if there exist a Turing machine T and constants $c, m \in \mathbb{N}$ such that $f(x)$ is computed by T in no more than $c|x|^m$ steps for $x \in A$, $|x| \neq 0$.

If the language of $\mathfrak{A}$ is infinite, for example, $\mathfrak{A} = (A, \{P_i\}_{i\in\mathbb{N}}, \{F_i\}_{i\in\mathbb{N}}, \{c_i\}_{i\in\mathbb{N}})$, then we require that a machine T for computing P_i or F_i and corresponding constants c, m can be found uniformly in $i \in \mathbb{N}$, without any limitation of time. Similarly, we require that the sequence $\{c_i\}_{i\in\mathbb{N}}$ is computable.

Theorem 1. *Let $\mathfrak{A} = (A, F_0, \ldots, F_n, \{P_i\}_{i\in\mathbb{N}}, \{c_i\}_{i\in\mathbb{N}})$ be a computable structure with finitely many functions. Suppose that $(A, F_0, \ldots, F_n)$ is locally finite, i.e., every its finitely generated substructure is finite. Then $\mathfrak{A}$ is computably isomorphic to a p-computable structure.*

Formerly, this fact was proved by D. Cenzer and J. Remmel for structures without functions, for Boolean algebras and for torsion Abelian groups.

Let $\mathfrak{A}$ be a p-computable structure. We say that $\mathfrak{A}$ is *p-categorical* if for every p-computable structure $\mathfrak{B} \cong \mathfrak{A}$, there exists an isomorphism $f : \mathfrak{A} \to \mathfrak{B}$ such that f, f^{-1} are p-computable.

Theorem 2. *Let $\mathfrak{A}$ be a p-computable structure. Then the following are equivalent:*
a) $\mathfrak{A}$ is p-categorical;
b) $\mathfrak{A}$ is finite.

Formerly, this fact was proved by D. Cenzer and J. Remmel for structures without functions, and by E. I. Latkin for p-computable structures $\mathfrak{A}$ such that $A \subseteq \mathrm{Tal}(\mathbb{N})$, where $\mathrm{Tal}(\mathbb{N}) = \{\mathrm{tal}(n) \mid n \in \mathbb{N}\}$, $\mathrm{tal}(n) = 1^n$ for $n \neq 0$ and $\mathrm{tal}(0) = 0$.

Corollary 1. *Let $\mathfrak{A}$ be an infinite p-computable structure. Then there exists a computable sequence of its p-computable presentations $\{\mathfrak{A}_n\}_{n\in\mathbb{N}}$ such that for every $n < k$, there is a p-computable isomorphism $f : \mathfrak{A}_k \to \mathfrak{A}_n$ and there is no p-computable injection $g : A_n \to A_k$.*

Theorem 3. *Let $\mathfrak{A}$ be an infinite p-computable structure, locally finite in the sense of Theorem 1. Then there exists a computable sequence of its p-computable presentations $\{\mathfrak{A}_n\}_{n\in\mathbb{N}}$ such that for every $n < k$, there is a p-computable isomorphism $f : \mathfrak{A}_k \to \mathfrak{A}_n$ and there is no primitive recursive injection $g : A_n \to A_k$.*

Formerly, this fact was proved by D. Cenzer and J. Remmel for structures without functions.

Since the notion of a p-categorical structure is degenerated, we consider its weaker version. Let $\mathfrak{A}$ be a structure and $R \subseteq A^n$. Then R is *invariant* if for every automorphism $f : \mathfrak{A} \to \mathfrak{A}$, $f(R) = R$. Note that if R is invariant then for every $\mathfrak{B} \cong \mathfrak{A}$, we can say about its image R^B in $\mathfrak{B}$.

Let $\mathfrak{A}$ and $\mathfrak{B}$ be computable structures. We say that $\mathfrak{A} \leqslant_{\mathrm{cr}} \mathfrak{B}$ ($\mathfrak{A}$ *is reducible to* $\mathfrak{B}$ *with respect to computable relations*) if for every computable invariant $R \subseteq B^n$, its image R^A in $\mathfrak{A}$ is computable. The notation $\mathfrak{A} \equiv_{\mathrm{cr}} \mathfrak{B}$ means that $\mathfrak{A} \leqslant_{\mathrm{cr}} \mathfrak{B}$ and $\mathfrak{B} \leqslant_{\mathrm{cr}} \mathfrak{A}$, and $\dim_{\mathrm{cr}}(\mathfrak{A})$ is the number of computable presentations of $\mathfrak{A}$ up to $\equiv_{\mathrm{cr}}$. Formerly, this notion was sometimes called algebraic reducibility.

Replacing “computable” by “p-computable” in the previous paragraph, we obtain definitions for $\mathfrak{A} \leqslant_{\mathrm{pr}} \mathfrak{B}$ ($\mathfrak{A}$ *is reducible to* $\mathfrak{B}$ *with respect to p-computable relations*), $\mathfrak{A} \equiv_{\mathrm{pr}} \mathfrak{B}$ and $\dim_{\mathrm{pr}}(\mathfrak{A})$.

Corollary 2. *Let* $\mathfrak{A}$ *be an infinite p-computable structure, locally finite in the sense of Theorem 1. Then* $\dim_{pr}(\mathfrak{A}) \geqslant \dim_{cr}(\mathfrak{A})$.

Example. *Let* $\mathfrak{A}$ *be a computable Boolean algebra with computable sets of atoms (or a computable linear ordering with computable set of adjacent pairs). Then the following are equivalent:*
a) $\dim_{pr}(\mathfrak{A}) = 1$*;*
b) $\dim_{cr}(\mathfrak{A}) = 1$*;*
c) $\mathfrak{A}$ *is computably categorical, i.e., has only finitely many atoms (finitely many adjacent pairs).*

Formerly, the equivalence of b) and c) for Boolean algebras was proved by S. T. Fedoryaev.

Sobolev Institute of Mathematics, Novosibirsk (Russia)
Novosibirsk State University
E-mail: alaev@math.nsc.ru

Degrees of categoricity for linear orderings

N. A. Bazhenov

We study degrees of categoricity for computable structures. The primary focus of this work is computable categoricity for linear orderings.

We recall definitions from [**1**]. Let $\mathbf{d}$ be a Turing degree. A computable structure $\mathcal{A}$ is $\mathbf{d}$-*computably categorical* if, for every computable copy $\mathcal{B} \cong \mathcal{A}$, there is a $\mathbf{d}$-computable isomorphism from $\mathcal{A}$ onto $\mathcal{B}$. The *categoricity spectrum* of $\mathcal{A}$ is the set

$$\mathrm{CatSpec}(\mathcal{A}) = \{\mathbf{d} : \mathcal{A} \text{ is } \mathbf{d}\text{-computably categorical}\}.$$

A Turing degree $\mathbf{d}_0$ is the *degree of categoricity* of $\mathcal{A}$ if $\mathbf{d}_0$ is the least degree in the spectrum $\mathrm{CatSpec}(\mathcal{A})$.

Let α be a computable ordinal. A computable structure $\mathcal{A}$ is Δ^0_α-*stable* if, for every computable $\mathcal{B} \cong \mathcal{A}$, every isomorphism from $\mathcal{A}$ onto $\mathcal{B}$ is Δ^0_α-computable. Ash [**2**] gave a complete characterization of Δ^0_α-stability for the class of computable ordinals. Here we extend this result to the following.

Theorem 1. *Suppose that k is a non-zero natural number, and γ is a computable infinite ordinal. Let α be an ordinal.*

(1) Suppose that $\omega^k \le \alpha < \omega^{k+1}$. Then $\mathbf{0}^{(2k-1)}$ is the degree of categoricity of α.

(2) Suppose that $\omega^\gamma \le \alpha < \omega^{\gamma+1}$. Then $\mathbf{0}^{(2\gamma)}$ is the degree of categoricity of α.

We also obtain some new examples of categoricity spectra for linear orderings.

Theorem 2. *Let k be a natural number such that $k \ge 2$, and let α be a computable infinite ordinal. Suppose that $\mathbf{d}$ is a Turing degree such that one of the following holds:*

(1) $\mathbf{d}$ is c.e. in and above $\mathbf{0}^{(2k)}$,

(2) $\mathbf{d}$ is c.e. in and above $\mathbf{0}^{(2\alpha+1)}$.

Then $\mathbf{d}$ is the degree of categoricity for some linear ordering L.

References

[1] *Fokina E. B., Kalimullin I., Miller R.* Degrees of categoricity of computable structures, Arch. Math. Logic, 49, No. 3 (2010), 51–67.

[2] *Ash C. J.* Recursive labelling systems and stability of recursive structures in hyperarithmetical degrees, Trans. Am. Math. Soc., 298, No. 2 (1986), 497–514.

Sobolev Institute of Mathematics, Novosibirsk (Russia)
E-mail: nickbazh@yandex.ru

Reverse mathematics and countable categoricity

E. Fokina

In this talk we will discuss some properties classically equivalent to countable categoricity from the point of view of reverse mathematics. We will present several new results that deal with the question about the number of models of a theory, in particular the question of existence of the Ryll-Nardzewski function and of a dominating function for the Ryll-Nardzewski function. We will also examine the strength of connected statements about existence of universal and saturated models. This is a joint work with Li Wei and Daniel Turetsky.

Kurt Gödel Research Center, University of Vienna, Vienna (Austria) and Sobolev Institute of Mathematics, Novosibirsk (Russia)
E-mail: ekaterina.fokina@univie.ac.at

Reductions between Types of Numberings

M. Manat

A numbering is a family of sets which can be enumerated or approximated uniformly by index. Numberings are ordered by many-one reduction; here a numbering (A_n) is many-one reducible to (B_n) if there exists a computable function f which translates the indices of the sets in numbering (A_n) into the indices of the same sets in numbering (B_n), i.e. $A_n = B_{f(n)}$ for all n. Rogers initiated the study of the semilattice of numberings under many-one reduction and Ershov [**1, 2, 3**] transferred it in particular to the study of the k-r.e. and, more generally, α-r.e. sets where the sets A_n are approximated uniformly by enumerating and deenumerating elements a limited number of times; this number can either be a constant k or an ordinal which is counted down each time the number is enumerated or deenumerated. An important question investigated is how the numberings on various levels of the hierarchy differ and which types of semilattices can be realised as the semilattice of all α-r.e. numberings with the same range as a given α-r.e. numbering (A_n). The overall goal of this presentation is to show some reductions between various types of numberings:

- If a k-r.e. numbering can realise a certain type of Rogers semilattice, so can a $(k+1)$-r.e. numberings or, more general, every $(\alpha+k)$-r.e. numbering where α is a computable ordinal;
- Every type of Rogers semilattice realised by an r.e. numbering is also realised by an α-r.e. for every computable ordinal α which is not a power of ω and which is not 0 while if α is a power of ω then there is no α-r.e. numbering without minimal numberings in the Rogers semilattice (which stands in contrast to the r.e. case);

This is joint work with F. Stephan and Ian Herbert from National University of Singapore.

References

[1] *Ershov Yu. L.* A certain hierarchy of sets I, Algebra i Logika, 7(1):47–74, 1968.
[2] *Ershov Yu. L.* A certain hierarchy of sets II, *Algebra i Logika, 7(4):15–47, 1968.*
[3] Ershov Yu. L. A certain hierarchy of sets III, Algebra i Logika, 9:34–51, 1970.

School of science and technology, Nazarbayev University, Astana, (Kazakhstan)
E-mail: manat.mustafa@nu.edu.kz

A decision procedure for the theory of atomless probability spaces

S. O. Speranski

Let QPL be the probability logic of [**2**] — hence it can be obtained from a variant of the well-known 'polynomial' quantifier-free logic described in [**1**] by adding *quantifiers over events* — and $\Vdash$ the corresponding satisfiability relation between classical (i.e. countably additive) probability spaces and QPL-formulas.

Recall that a probability space $\mathscr{P}$ is *atomless* iff we have

$$\mathscr{P} \Vdash \forall x\, (\mu\,(x) > 0 \to \exists y\, (0 < \mu\,(y) < \mu\,(x) \wedge \mu\,(\overline{y} \cup x) = 1)).$$

Intuitively such measures are very close to the Lebesgue measure on $[0, 1]$.

Theorem. *All atomless spaces have the same* QPL*-theory. This theory is decidable.*

Let us extend QPL to $\mathsf{QPL}^{\mathrm{r}}$ by adding quantifiers over reals. Then the techniques developed in the proof of the theorem can be applied to get the following:

- *the above results remain true even if we replace* QPL *by* $\mathsf{QPL}^{\mathrm{r}}$*;*
- *the* $\mathsf{QPL}^{\mathrm{r}}$*-theory of the class* $\mathcal{V}$ *of all probability spaces is* Π^1_∞*-bounded.*

So in particular the QPL-theory of $\mathcal{V}$ — which is Π^1_∞-hard, cf. [**2**] — turns out to be Π^1_∞-complete, as well as the $\mathsf{QPL}^{\mathrm{r}}$-theory of $\mathcal{V}$. At the same time both claims stated in the above theorem are false if we pass to weak (i.e. finitely-additive) spaces.

References

[1] *Fagin R., Halpern J. Y., and Megiddo N.* A logic for reasoning about probabilities, Information and Computation, 87:1–2 (1990), 78–128.

[2] *Speranski S. O.* Quantifying over events in probability logic: how Boolean algebras met real-closed fields, Mathematical Structures in Computer Science. Accepted [Cambridge].

Sobolev Institute of Mathematics, Novosibirsk, Russia
E-mail: katze.tail@gmail.com

There are no minimal pairs in $L[\mathbf{d}]$

M. M. Yamaleev

Given 2-computably enumerable (2-c.e.) set D with an effective approximation $\{D_s\}_{s\in\omega}$ such that $|D_s - D_{s-1}| \leq 1$, we say that $L(D) = \{s : \exists\, x \in D_s - D\}$ is the Lachlan's set of D. The Turing degree of $L(D)$ doesn't depend on the approximation (e.g., see Ishmukhametov [**1**]), hence we call $\deg(L(D))$ the Lachlan's degree of D. Let $\mathbf{d}$ be a 2-c.e. Turing degree, we define $L[\mathbf{d}] = \{\deg(L(B)) : B$ is 2-c.e and $B \equiv_T D\}$, elements of $L[\mathbf{d}]$ we also call as Lachlan's degrees of $\mathbf{d}$. Clearly, elements of $L[\mathbf{d}]$ are c.e. degrees, moreover, for any $\mathbf{w} \in L[\mathbf{d}]$ we have $\mathbf{w} \leq \mathbf{d}$ and $\mathbf{d}$ is computably enumerable relative to $\mathbf{w}$.

In a joint work with Fang C., Liu J. and Wu G. we obtained the following results.

Theorem 1. *Given 2-c.e. sets $A, B \in \mathbf{d}$, there exists 2-c.e. set $D \in \mathbf{d}$ such that $L(D) \leq_T L(A), L(B)$.*

If $\mathbf{d}$ has a proper 2-c.e. degree then $L[\mathbf{d}]$ contains only nonzero elements. Hence, as a corollary of Theorem 1, it cannot contain a minimal pair. Note that, if $\mathbf{d}$ would have a c.e. degree then $L[\mathbf{d}] = [0, \mathbf{d}]$ and it could contain a minimal pair.

By induction on Theorem 1, we can see that any finite number of elements from $L[\mathbf{d}]$ have lower bound from $L[\mathbf{d}]$. However, for the case of whole $L[\mathbf{d}]$ we can prove

Theorem 2. *There exists a 2-c.e. degree $\mathbf{d}$ such that $L[\mathbf{d}]$ doesn't have a nonzero lower bound.*

Based on this, in the talk we will discuss possible approaches in distinguishing properly 2-c.e. degrees from c.e. degrees in the class of all 2-c.e. degrees. Also we will discuss a generalization of $L[\mathbf{d}]$ for the case of weak truth-table degrees, particularly we will show that a weak truth-table analogue of $L[\mathbf{d}]$ can contain a minimal pair, if $\mathbf{d}$ has a proper 2-c.e. degree.

The work is supported by The President grant of Russian Federation (project NSh-941.2014.1), by Russian Foundation for Basic Research (projects 14-01-31200, 15-01-08252), by Kazan Federal University and by the subsidy allocated to Kazan Federal University for the project part of the state assignment in the sphere of scientific activities.

References

[1] *Ishmukhametov Sh.* On the predececcors of d.r.e. degrees // Arch. Math. Logic. 1999. V. 38. P. 373–386.

Lobachevsky Institute of Mathematics and Mechanics, Kazan Federal University, Kazan
E-mail: mars.yamaleev@kpfu.ru

IV. Секция «Теория групп»

О периодизуемости замощений плоскости

С. В. Августинович, И. С. Думанский

Несмотря на значительные усилия исследователей, сложностной статус проверки замощаемости плоскости произвольной односвязной фигурой до сих пор не определен. Кроме того неясно, всегда ли будет существовать периодическое замощение, если некоторое замощение существует. Один из возможных подходов к этой проблеме заключается в том, чтобы вместо поисков периодических замощений доказывать их периодизуемость, т.е. находить последовательность локальных свитчингов, приводящих к периодическому варианту.

Пусть некоторая конечная односвязная плоская область О замощена копиями фигуры Ф двумя разными способами. Замену одного способа на другой будем называть свитчингом. Если в каждом из упомянутых замощений некоторые копии Ф остаются на своих местах, то свитчинг будем называть локальным. Область О, допускающую несколько замощений, назовем свитчингово связной если от любого ее замощения к любому другому можно перейти с помощью серии локальных свитчингов. В противном случае такую область назовем элементарной. Множество всех элементарных областей для Ф назовем Ф-базовым множеством. Таким образом можно утверждать, что любые два различных замощения произвольной области переводятся друг в друга композицией свитчингов элементарных областей.

Обозначим через D прямоугольник 1x2 (домино).

Теорема. *Базовое множество для D состоит ровно из одного элемента, а именно - квадрата 2x2.*

Список литературы

[1] *Puzynina S. A.* On periodicity of generalized two-dimensional infinite words. Information and Computation 207:11, 2009, p. 1315–1328.

[2] *Puzynina S. A., Avgustinovich S. V.* On periodicity of two-dimensional words. Theoretical Computer Science 2008 (391), p. 178–187.

ИМ СО РАН, Новосибирск
E-mail: avgust@math.nsc.ru, ilyadumnsk@gmail.com

Элементы конечного порядка и подгруппы, порождаемые инволюциями в целочисленных групповых кольцах некоторых 2-групп

Д. М. Агеев

В работе изучаются обратимые элементы конечного порядка и подгруппы, порождаемые инволюциями в целочисленных групповых кольцах диэдральных групп D_8, D_{16} порядков 8 и 16 и обобщённой группы кватернионов Q_{16} порядка 16.

Под *тривиальными* элементами целочисленного группового кольца группы G, как обычно, понимаются элементы, которые имеют вид $\pm g$, где $g \in G$.

С использованием подходов из [1]–[3] получены следующие результаты.

Теорема 1. *Пусть $D_8 = \langle a, b | a^4 = b^2 = 1, bab = a^{-1} \rangle$. Тогда нетривиальные элементы конечного порядка из нормализованной мультипликативной группы кольца $\mathbb{Z}D_8$ имеют вид:*

(1) *если элемент имеет порядок 2, то это или u_{2n} или $a^2 u_{2n}$, где $n = 0, 1$*

$$u_{20} = a^2 b + (1 - a^2)(ya + xb + zab)$$
$$u_{21} = a^3 b + (1 - a^2)(ya + zb + xab)$$

при условии $x(x-1) = y^2 - z^2$,

(2) *если элемент имеет порядок 4, то это или u_4 или $a^2 u_4$, где*

$$u_4 = a^3 + (1 - a^2)(xa + yb + zab)$$

при условии $x(x-1) = y^2 + z^2$,

Аналогичные описания получены для случаев групп D_{16} и Q_{16}, но они более громоздки.

Как следствие получается положительное решение гипотезы Цассенхауза для групп D_8, D_{16} и Q_{16}.

Исследованы некоторые подгруппы группы единиц группового кольца, порождаемые парой инволюций для диэдральных групп порядков 8 и 16 и доказана теорема:

Теорема 2. *Пусть $b \in \pm G$, $x \in V(\mathbb{Z}G)$ и $b^2 = x^2 = 1$, тогда:*

(1) *если $G = D_8$ и $\langle b, x \rangle \cong D_8$, то x тривиальна,*

(2) *если $G = D_{16}$, то существуют подгруппы, изоморфные D_8 или D_{16}, не все элементы которых тривиальны.*

Список литературы

[1] *Luthar I. S., S.Passi I. B.* Zassenhaus conjecture for A_5 // Proc. Indian Acad. Sci. Math. Sci. – 1989. – № 9. – С. 1–5.

[2] *Берман С. Д.* Об уравнении $x^m = 1$ в целочисленном групповом кольце // Украинский математический журнал. – 1955. – Т. VII. – № 3. – С. 253–261.

[3] *Cohn J. A., Livingstone D.* On the structure of group algebras I // Canad. J. Math. – 1965. – № 17. – С. 583–593.

Южно-Уральский государственный университет, г. Челябинск
E-mail: feuerrader92@mail.ru

Индуктивный подход к описанию групп единиц целочисленных групповых колец циклических 2-групп

Р. Ж. Алеев, О. В. Митина, В. Н. Пузач

Пусть $G = \langle x\rangle$ — циклическая группа порядка $2^n \geqslant 16$ (для порядков 2 и 4 тривиально, а для 8 хорошо известно). Пусть $\mathrm{V}(\mathbf{Z}G)$ — нормализованная группа единиц целочисленного группового кольца $\mathbf{Z}G$ группы G. Пусть ζ — первообразный корень степени 2^n из 1 и $\mathrm{U}(\mathbf{Z}[\zeta])$ — группа единиц кольца $\mathbf{Z}[\zeta]$.

Пусть $\chi_0 = 1_G$, $\chi_1,\ldots,\chi_{2^n-1}$ — неприводимые комплексные характеры группы G, где $\chi_j(x^k) = \zeta^{jk}$ для любых j и k. Для любого $j \in \{0, 1, \ldots, 2^n-1\}$ пусть e_j — минимальный центральный идемпотент комплексной групповой алгебры $\mathbf{C}G$, соответствующий характеру χ_j. Тогда групповым гомоморфизмом является $\varphi : \mathrm{V}(\mathbf{Z}G) \to \mathrm{U}(\mathbf{Z}[\zeta])$, где $\varphi\Big(\sum_{k=0}^{2^n-1}\beta_k e_k\Big) = \beta_1$.

В [**1**] была построена подгруппа конечного индекса группы $\mathrm{V}(\mathbf{Z}G)$ на основе локальных подгрупп [**2**]. Однако, индекс этой подгруппы был очень большим. Здесь на основе индуктивных соображений предлагается другой подход для построения подгруппы группы $\mathrm{V}(\mathbf{Z}G)$, который даст такую подгруппу значительно меньшего индекса.

Положим $\ker\varphi = V_0$ и для любого натурального t через σ_t обозначим автоморфизм кругового поля $\mathbf{Q}(\zeta)$, продолжающий отображение $\zeta \mapsto \zeta^{2t+1}$. Тогда пусть

$$V_1 = \Big\{1 + \sum_{t=0}^{2^{n-1}-1}(\sigma_t(\lambda)-1)e_{2t+1}\Big|\lambda \in \mathrm{U}(\mathbf{Z}[\zeta])\Big\} \cap \mathrm{V}(\mathbf{Z}G).$$

Теорема. *При введённых ранее обозначениях имеем:*

$$|\mathrm{V}(\mathbf{Z}G) : \langle\zeta\rangle \times V_0 \times V_1| < \infty.$$

*Кроме того, V_0 изоморфна подгруппе $\big(1 + 2\mathbf{Z}\langle x^2\rangle\big) \cap \mathrm{V}(\mathbf{Z}\langle x^2\rangle)$ группы $\mathrm{V}(\mathbf{Z}\langle x^2\rangle)$. При условии положительного решения проблемы Вебера о числе классов [**3**] и описания $\mathrm{V}(\mathbf{Z}\langle x^2\rangle)$ имеем:*

$$|\mathrm{V}(\mathbf{Z}G) : \langle\zeta\rangle \times V_0 \times V_1| \leqslant 2^{2^{n-2}-1}.$$

Список литературы

[1] *Алеев Р. Ж., Пузач В. Н.* Группы единиц целочисленных групповых колец циклических 2-групп. Межд. конф. «Мальцевские чтения» (10–13 ноября 2014 г.). Тезисы докладов. Новосибирск. 2014. с. 51.
URL: www.math.nsc.ru/conference/malmeet/14/Malmeet2014.pdf

[2] *Алеев Р. Ж.* Единицы полей характеров и центральные единицы целочисленных групповых колец конечных групп. Матем. труды, 3, № 1(2000), с. 3–37.

[3] *Miller John C.* Class numbers of totally real fields and applications to the Weber class number problem. Acta Arithmetica 164, no. 4 (2014), 381-397.

Южно-Уральский ГУ (НИУ), Челябинск; Челябинский ГУ, Челябинск; Костанайский филиал ЧелГУ, Костанай (Казахстан)
E-mail: aleev@csu.ru; ovm@csu.ru; puzach1984@mail.ru

Сравнения по модулю 2 круговых единиц в кольцах вычетов колец целых круговых полей

Р. Ж. Алеев, О. В. Митина, В. Н. Пузач

Пусть ζ — первообразный корень степени $2^n > 4$ из 1. При изучении единиц целочисленного группового кольца циклической группы порядка 2^n возникает задача исследования свойств единиц кольца целых $\mathbf{Z}[\zeta]$ кругового поля $\mathbf{Q}(\zeta)$. Проблема Вебера о числе классов [**1**] в совокупности с [**2**] утверждает, что все единицы кольца $\mathbf{Z}[\zeta]$ будут круговыми. Уточнением результата из [**3**] служит следующая лемма.

Лемма. *Для любого натурального j положим*

$$t_j = 1 + \zeta^{2j+1} + \zeta^{-2j+1} + \alpha^{4j+1} + \alpha^{-4j+2} \quad \text{и} \quad T(j) = \left\langle t_{2j+1}, t_{2^{n-1}-2j-1} \right\rangle.$$

Тогда группа круговых единиц равна

$$\langle\zeta\rangle \times \langle t_0\rangle \times \prod_{j=1}^{2^{n-3}-1} T(j).$$

Продвижением результатов из [**4**] является следующая теорема.

Теорема. *Для натурального j*

$$T_j \cap (1 + 2\mathbf{Z}[\zeta]) = \left\langle t_{2j+1} \cdot t_{2^{n-1}-2j-1}^{2^{n-2}-1} \right\rangle \times \left\langle t_{2^{n-1}-2j-1}^{2^{n-2}} \right\rangle.$$

Список литературы

[1] *Miller John C.* Class numbers of totally real fields and applications to the Weber class number problem. Acta Arithmetica 164, no. 4 (2014), pp. 381-397.

[2] *Sinnott W.* On the Stickelberger ideal and circular units of a cyclotomic field., Ann. of Math., Vol. 108, no. 1(1978), pp. 107–134.

[3] *Алеев Р. Ж., Такшеева В. С.* Порождающие группы круговых единиц. Вестник ЧелГУ. Математика. Механика. Информатика. Выпуск 10. № 6 (107), 2008, С. 121–129.

[4] *Алеев Р. Ж., Митина О. В., Пузач В. Н.* Круговые единицы в кольцах вычетов колец целых круговых полей. Межд. конф. «Мальцевские чтения» (10–13 ноября 2014 г.). Тезисы докладов. Новосибирск. 2014. с. 50.
URL: www.math.nsc.ru/conference/malmeet/14/Malmeet2014.pdf

Южно-Уральский ГУ (НИУ), Челябинск; Челябинский ГУ, Челябинск; Костанайский филиал ЧелГУ, Костанай (Казахстан)
E-mail: aleev@csu.ru; ovm@csu.ru; puzach1984@mail.ru

О конечных разрешимых группах, графы Грюнберга—Кегеля которых не содержат треугольников

О. А. Алексеева, А. С. Кондратьев

Графом простых чисел (или графом Грюнберга—Кегеля) $\Gamma(G)$ конечной группы G называется граф, в котором вершинами служат простые делители порядка группы G и две различные вершины p и q смежны тогда и только тогда, когда G содержит элемент порядка pq. Через $l_F(G)$ обозначается фиттингова длина конечной разрешимой группы G, т. е. наименьшая длина нормальных рядов группы G, все факторы которых нильпотентны.

Лючидо [**1**] исследовала конечные группы G такие, что связные компоненты графа $\Gamma(G)$ являются деревьями, т. е. связными графами, не содержащими циклы. Мы рассматриваем более общую задачу описания строения конечной группы G такой, что граф $\Gamma(G)$ не содержат треугольников, т. е. 3-циклов. В [**2**] мы определили все конечные почти простые группы с таким свойством. В данной работе мы продолжаем эти исследования, рассматривая строение конечных разрешимых групп с таким свойством. Доказана

Теорема. *Пусть G – конечная разрешимая группа. Если граф $\Gamma(G)$ не содержит треугольников, то выполняются следующие утверждения:*

(1) *если граф $\Gamma(G)$ несвязен, то G — группа Фробениуса или 2-фробениусова группа и граф $\Gamma(G)$ имеет точно две компоненты связности, каждая из которых является 1- или 2-цепью;*

(2) *если граф $\Gamma(G)$ связен, то граф $\Gamma(G)$ является либо n-цепью для $1 \leq n \leq 4$, либо 4-циклом, либо 5-циклом;*

(3) *если граф $\Gamma(G)$ является 2-цепью, то число $l_F(G)$ может быть сколь угодно большим;*

(4) *если граф $\Gamma(G)$ не является 2-цепью, то $l_F(G) \leq 6$.*

Работа выполнена при финансовой поддержке РФФИ (проект 13-01-00469), Комплексной программы фундаментальных исследований УрО РАН (проект 15-16-1-5) и в рамках проекта повышения конкурентоспособности (Соглашение между Министерством образования и науки Российской Федерации и Уральским федеральным университетом от 27.08.2013, №02.A03.21.0006).

Список литературы

[1] *Lucido M. C.* Groups in which the prime graph is a tree // Boll. Unione Mat. Ital. (8), 2002. V. 5-B, N 1. P. 131–148.

[2] *Алексеева О. А., Кондратьев А. С.* Конечные почти простые группы, графы Грюнберга—Кегеля которых не содержат треугольников // Межд. конф. "Мальцевские чтения". Тез. докл. Новосибирск: ИМ и НГУ, 2014. С. 50.

Русско-Британский институт управления, Челябинск; Институт математики и механики им. Н. Н. Красовского УрО РАН;
Уральский федеральный университет, Екатеринбург
E-mail: Alekseeva.O.A@rbiu.ru, a.s.kondratiev@imm.uran.ru

Формульная определимость кольца R в частично коммутативной нильпотентной R-группе

М. Г. Амаглобели, А. А. Мищенко, А. В. Трейер

Пусть Γ — конечный простой граф отличный от полного графа и G_Γ — частично коммутативная двуступенно нильпотентная R—группа, где R — биномиальное евклидово кольцо. В докладе будет показано, что класс частично коммутативных двуступенно нильпотентных R–групп и класс биномиальных евклидовых колец являются синтаксически эквивалентными классами (определение в статье [**1**]). Другими словами, для любой элементарной формулы в групповом языке выполненной на R-группе G_Γ можно построить формулу кольцевого языка, которая будет выполнена на кольце R и наоборот.

Существует несколько работ где в конечно порожденных нильпотентных группах интерпретируется центроид группы — максимально определимое кольцо для данной группы. Особенность нашего подхода состоит в том, что, используя специфику частично коммутативных нильпотентных R-групп, мы интерпретируем непосредственно кольцо R.

Список литературы

[1] *Мальцев А. И.* Об одном соответствии между кольцами и группами, Матем. сб., 1960, том 50(92), 3, 257–266

Тбилисский государственный университет, Тбилиси, Грузия. Инстиут математики СО РАН. Инстиут математики СО РАН
E-mail: alexei.mishenko@gmail.com, alexander.treyer@gmail.com

О пересечении сопряженных разрешимых подгрупп в симметрической группе

А. А. Байкалов

Пусть группа G действует на множестве Ω. Элемент $x \in \Omega$ называется *регулярной точкой* , если $|xG| = |G|$, т.е. если $G-$орбита элемента x регулярна. Определим действие группы G на Ω^k правилом:

$$g : (i_1, \dots, i_k) \mapsto (i_1 g, \dots, i_k g).$$

Если группа G действует точно и транзитивно на Ω, то минимальное k такое, что Ω^k имеет регулярную точку, называется *базой* группы G и обозначается через $b(G)$. Для любого натурального m число $G-$регулярных орбит обозначается через $Reg(G, m)$ (это число равно нулю, если $m < b(G)$). Если H — подгруппа группы G и группа G действует на множестве Ω правых смежных классов по H умножением справа, то G/H_G действует точно и транзитивно на Ω, где $H_G = \cap_{g\in G} H^g$. В этом случае обозначим $b(G/H_G)$ и $Reg(G/H_G, m)$ через $b_H(G)$ и $Reg_H(G, m)$ соответственно.

Таким образом, $b_H(G)$ — это минимальное k такое, что существуют $x_1, \dots, x_k \in G$, для которых справедливо равенство $H^{x_1} \cap \dots \cap H^{x_k} = H_G$.

В данной работе рассматривается вопрос 17.41 из ¡ ¡ Коуровской тетради¿ ¿ [**1**]:

Пусть S — разрешимая подгруппа конечной группы G, не содержащей нетривиальных разрешимых подгрупп. Всегда ли найдётся пять подгрупп, сопряженных с S, пересечение которых тривиально?

Проблема сведена в [**2**] к случаю почти простой группы G. А именно, в работе [**2**], в частности, доказано, что если для любой почти простой группы G и её разрешимой подгруппы H справедливо неравенство $Reg_H(G, 5) \geq 5$, то и в любой конечной неразрешимой группе G для любой разрешимой подгруппы H справедливо неравенство $Reg_H(G, 5) \geq 5$.

В настоящей работе доказана теорема:

Теорема 1. *Пусть группа $G = S_n$ или A_n, где $n \geq 5$. Тогда если S — разрешимая подгруппа группы G, то $Reg_S(G, 5) \geq 5$. В частности $b_S(G) \leq 5$.*

Исследование выполнено за счет гранта Российского научного фонда (проект No14-21-00065)

Список литературы

[1] *Коуровская тетрадь*; Издание 18-е, Новосибирск 2014.

[2] *Vdovin E. P.* On the base size of a transitive group with solvable point stabilizer; Journal of Algebra and Application, v. 11 (2012), N 1, 1250015 (14 pages)

Новосибирский государственный университет, Новосибирск
E-mail: anton188@bk.ru

Группа сопрягающих базис автоморфизмов — нормальное строение и автоморфизмы

В. Г. Бардаков, М. В. Нещадим

Одной из фундаментальных групп в комбинаторной теории групп является группа автоморфизмов свободной группы F_n. Не смотря на огромное число публикаций, посвященных этой теме, многие вопросы до сих пор остаются открытыми. В частности, непонятно, как устроена группа $IA(F_n)$ – группа IA-автоморфизмов свободной группы F_n при $n > 2$. Группа $IA(F_2)$, как хорошо известно, изоморфна группе внутренних автоморфизмов группы F_2, а потому изоморфна самой F_2. S. Krstic и J. McCool (1997) доказали, что группа $IA(F_3)$ не является конечно определенной.

Группа Cb_n — группа сопрягающих базис автоморфизмов, состоит из тех автоморфизмов свободной группы F_n, которые на стандартных порождающих $x_1, ..., x_n$ группы F_n действуют сопряжениями. В частности, группа крашеных кос P_n является подгруппой в Cb_n, а группа кос B_n является подгруппой в группе C_n, которая порождается Cb_n и перестановками порождающих $x_1, ..., x_n$. J.McCool (1986) нашел систему порождающих и соотношений для Cb_n. Дальнейшие результаты о строении группы Cb_n можно найти в работах А.Г.Савушкиной (1996), В.Г.Бардакова (2003), F.R.Cohen, J.Pakianathan, V.V.Vershinin (2005).

В предлагаемой работе мы находим некоторое представление группы Cb_n. При $n = 3$ это представление нашел O.Chein (1969). Также мы определяем ее алгебру Ли в новых порождающих. Отметим, что группа Cb_{n-1} естественным образом вложена в группу Cb_n. На основе этого в группе Cb_n определяется последовательность подгрупп и доказывается, что Cb_n является последовательным полупрямым произведением этих подгрупп. Кроме того, определяется группа *частично внутренних автоморфизмов* I_n, которая является подгруппой Cb_n и имеет простое строение. В частности, она является поли-свободной группой, т. е. строится из свободных при помощи нескольких последовательных полупрямых расширений.

Напомним, что автоморфизм произвольной группы называется нормальным, если он оставляет на месте все её нормальные подгруппы. Множество $Aut_N\, G$ всех нормальных автоморфизмов группы G — нормальная подгруппа группы $\mathrm{Aut}\, G$, содержащая подгруппу её внутренних автоморфизмов $\mathrm{Int}\, G$.

Нормальные автоморфизмы исследовались для многих классов групп: свободных групп, свободных разрешимых групп, свободных нильпотентных групп, конечных p-групп, свободных бернсайдовых групп, свободных разрешимых про-p-групп и т.д. Известно, что нормальные автоморфизмы групп кос, групп крашеных кос внутренние, М.В.Нещадим (1993). В настоящей работе мы доказываем, что нормальные автоморфизмы группы Cb_n внутренние и находим пересечение групп I_n и групп крашеных кос P_n.

ИМ СО РАН, Новосибирск
E-mail: bardakov@math.nsc.ru, neshch@math.nsc.ru

Группы автоморфизмов антиподальных дистанционно регулярных графов с числом вершин, не большим 1000

И. Н. Белоусов, А. А. Махнев

Мы рассматриваем неориентированные графы без петель и кратных ребер. Для вершины a графа Γ через $\Gamma_i(a)$ обозначим i-окрестность вершины a, то есть, подграф, индуцированный Γ на множестве всех вершин, находящихся на расстоянии i от a. Подграф $\Gamma(a) = \Gamma_1(a)$ называется окрестностью вершины a и обозначается $[a]$, если граф Γ фиксирован.

В работе [**1**] найдены массивы пересечений дистанционно регулярных локально циклических графов с числом вершин не большим 1000.

Предложение 1. *Пусть Γ является дистанционно регулярным графом диаметра, большего 2, на $v \le 1000$ вершинах. Если $\lambda = 2$ и $\mu > 1$, то верно одно из утверждений:*

(1) Γ — *примитивный граф с массивом пересечений* $\{15, 12, 6; 1, 2, 10\}$, $\{19, 16, 8; 1, 2, 8\}$, $\{24, 21, 3; 1, 3, 18\}$, $\{35, 32, 8; 1, 2, 28\}$, $\{51, 48, 8; 1, 4, 36\}$*;*

(2) Γ — *антиподальный граф с* $\mu = 2$ *и массивом пересечений* $\{2r + 1, 2r - 2, 1; 1, 2, 2r + 1\}$, $r \in \{3, 4, ..., 21\} - \{10, 16\}$ *и* $v = 2r(r + 1)$*;*

(3) Γ — *антиподальный граф с* $\mu \ge 3$ *и массивом пересечений* $\{15, 12, 1; 1, 4, 15\}$, $\{18, 15, 1; 1, 5, 18\}$, $\{27, 24, 1; 1, 8, 27\}$, $\{35, 32, 1; 1, 4, 35\}$, $\{45, 42, 1; 1, 6, 45\}$, $\{42, 39, 1; 1, 3, 42\}$, $\{75, 72, 1; 1, 12, 75\}$.

Мы исследуем группы автоморфизмов графов с массивами пересечений из пункта (2). Если $2r + 1$ — степень простого числа, то граф существует. Более того существует единственный реберно симметричный граф, полученный из схемы Р. Мэтона. Заметим, что $2r + 1$ — не степень простого числа для $r = 7, 17, 19$.

Теорема. *Группа автоморфизмов графа с массивом пересечений* $\{15, 12, 1; 1, 2, 15\}$, $\{35, 32, 1; 1, 2, 35\}$ *или* $\{39, 36, 1; 1, 2, 39\}$ *действует интранзитивно на множестве его вершин.*

Работа выполнена при поддержке РНФ (проект 14-11-00061).

Список литературы

[1] *Буриченко В. П., Махнев А. А.* О вполне регулярных локально циклических графах // Современные проблемы математики. Тезисы 42 Всероссийской молодежной конференции. ИММ УрО РАН, Екатеринбург 2011, 11–14.

Институт математики и механики им. Н. Н. Красовского УрО РАН, Уральский федеральный университет, Екатеринбург
E-mail: i_belousov@mail.ru, makhnev@imm.uran.ru

О разрешимости группы с холловыми добавлениями к нормализаторам выделенных подгрупп

Т. В. Бородич

Все рассматриваемые нами группы конечны. Напомним, что подгруппу H группы G называют добавлением к подгруппе K, если группа $G = KH$ и пересечение $K \cap H$ не обязательно единичная подгруппа.

Если в конечной группе G индекс нормализатора каждой силовской подгруппы примарен, то G – разрешимая группа. Этот результат публиковался в работах [**1, 2, 3, 4**].

Позже в работе [**5**] показали, что группа остается разрешимой, если примарными будут только индексы нормализаторов силовских 2- и 3-подгрупп. Развитие данного направления было в [**6**], в ней установлено разрешимость группы G в том случае, когда нормализаторы силовских 2- и 3-подгрупп обладают нильпотентными холловыми добавлениями. В доказательстве последних двух результатов используется классификация конечных простых групп.

В настоящей заметке исследуются группы с ограничениями на количество нормализаторов силовских подгрупп, которые обладают холловыми добавлениями.

Теорема 1. *Пусть G – группа и $p \in \pi(G)$. Если для любого значения $q \in \pi(G) \setminus \{p\}$ нормализатор силовской q-подгруппы обладает нильпотентным холловым добавлением, то группа G разрешима.*

Пример простой группы A_5, показывает, что в теореме 1 нельзя исключить два простых делителя из $\pi(G)$. Пример простой группы $PSL(2,7)$, указывает на то, что в теореме 1 нельзя рассматривать разрешимое добавления к нормализаторам силовских q-подгрупп $q \in \pi(G) \setminus \{3\}$.

Следствие. *Пусть G – группа и $p \in \pi(G)$. Если для любого значения $q \in \pi(G) \setminus \{p\}$ индекс нормализатора каждой силовской q-подгруппы примарен, то группа G разрешима.*

Теорема 2. *Если в $3'$-группе G нормализатор силовской p-подгруппы обладает p-разрешимым холловым добавлением, то группа G — p-разрешима.*

При доказательстве теорем используется классификация конечных простых групп.

Список литературы

[1] *Ведерников В. А.* О признаках разрешимости и сверхразрешимости конечных групп // Сибирский математический журнал. — 1962. — Т. VIII, №6 — С. 1236–1244

[2] *Buchthal D.* On factorized groups // Trans. Amer. Math. Soc. — 1973. — V.183. — P. 425–432.

[3] *Zhang J.* Sylow numbers of finite groups // J. Algebra. — 1995. — V. 176. — P. 111–123.

[4] *Guo W.* Finite groups with given indices of normalizers of Sylow subgroups // Siberian Math. J. — 1996. — V. 37. — P. 207–214.

[5] *Guo W., Shum K. P.* A note on finite groups whose normalizers of Sylow 2-, 3-sugroups are prime power induces // Journal of Applied Algebra and Discrete Structures. — 2005. — V.3, No.1. — P. 1–9.

[6] *Монахов В. С., Бородич Т. В.* О разрешимости группы с холловыми добавлениями к нормализаторам силовских подгрупп // Математические заметки. — 2009. — Т. 85, № 2. — С. 227–233.

УО "Гомельский государственный университет имени Ф. Скорины", Гомель, Беларусь
E-mail: tvborodich@gsu.by

О пересечении $\mathfrak{f}$-абнормальных максимальных подгрупп в разрешимых группах

Е. Н. Бородич, Р. В. Бородич, С. Н. Быков

Рассматриваются конечные группы. Одно из классических направлений в исследовании конечных групп связано с задачей о свойствах пересечений заданных максимальных подгрупп и исследовании влияния этих свойств на строение группы, которое берет начало с работ Г.Фраттини [1], В.Гашюца [2] и в дальнейшем было продолжено в работах многих авторов (см. монографии [3], [4]) В настоящее время к исследованию пересечений максимальных подгрупп и изучению свойств классов групп, все чаще, подходят с позиций теории подгрупповых функторов (см. монографии [4], [5], [6]).

Пусть Θ — m-функтор, выделяющий в каждой группе один класс сопряжённых максимальных подгрупп и саму группу. Тогда $\bar{\Theta}(G)$ — множество всех максимальных подгрупп группы G, которые не сопряжены с некоторой фиксированной максимальной подгруппой M группы G.

Обозначим через $\bar{\Phi}^{\mathfrak{N}}_{\bar{\Theta}_1}(G)$ пересечение ненильпотентных максимальных подгрупп, не сопряженных с некоторой максимальной подгруппой. Всегда полагаем, что пересечение пустого множества подгрупп из G совпадает с самой группой G.

Теорема. *В любой неразрешимой группе G существует нормальная p-подгруппа P такая, что $\bar{\Phi}^{\mathfrak{N}}_{\bar{\Theta}_1}(G)/P \in \mathfrak{N}$.*

Следствие. *В любой неразрешимой группе G подгруппа, равная пересечению ненильпотентных максимальных подгрупп, не сопряженных с некоторой максимальной подгруппой, метанильпотентна.*

Список литературы

[1] *Frattini G.* Intorno alla generasione dei gruppi di operazioni // Atti Acad. Dei Lincei 1885. Vol.1. P.281-285.

[2] *Gaschütz W.* Über die Φ-Untergruppen endlicher Gruppen // Math. Z. — 1953. — Bd. 58. — S. 160–170.

[3] *Шеметков Л. А.* Формации конечных групп. — М.: Наука, 1978. — 267 с.

[4] *Селькин М. В.* Максимальные подгруппы в теории классов конечных групп — Мн.:Беларуская навука, 1997. — 144 с.

[5] *Каморников С. Ф., Селькин М. В.* Подгрупповые функторы и классы конечных групп. — Мн.: Бел. навука, 2003. — 254 с.

[6] *Скиба А. Н.* Алгебра формаций. — Мн.: Беларуская навука, 1997. — 240 с.

Учреждение образования "Гомельский государственный университет имени Ф.Скорины", Гомель
E-mail: Borodich@gsu.by

О доминионах групп в многообразии N_cA

А. И. Будкин

Доминион $\mathrm{dom}_G^{\mathcal{M}}(H)$ подгруппы H группы G относительно квазимногообразия $\mathcal{M}$ — это множество всех элементов $a \in G$, образы которых равны для всех пар гомоморфизмов, совпадающих на H, из G в каждую группу из $\mathcal{M}$, т.е.

$$\mathrm{dom}_G^{\mathcal{M}}(H) = \{a \in G \mid \forall M \in \mathcal{M}\ \forall f, g : G \to M,\ \text{если}\ f\mid_H = g\mid_H,\ \text{то}\ a^f = a^g\}.$$

Здесь, как обычно, через $f, g : G \to M$ обозначены гомоморфизмы группы G в группу M, через $f\mid_H$ — ограничение f на H.

Несложно заметить, что $\mathrm{dom}_G^{\mathcal{M}}(-)$ является оператором замыкания на решетке подгрупп данной группы G, в том смысле, что он экстенсивный (доминион подгруппы H содержит H), идемпотентный (доминион доминиона подгруппы H равен доминиону H) и изотонный (если $H \subset B$, то доминион H содержится в доминионе B). В результате возникает понятие замкнутой подгруппы.

Подгруппа H группы G ($G \in \mathcal{M}$) называется замкнутой в группе G (относительно класса $\mathcal{M}$), если $\mathrm{dom}_G^{\mathcal{M}}(H) = H$.

Информацию о доминионах в абелевых группах можно найти в [1], в нильпотентных многообразиях групп — в [2], в метабелевых группах — в [3,4].

В данной работе исследуются доминионы абелевых подгрупп в группах из многообразия N_cA, состоящего из расширений нильпотентных групп ступени не выше c при помощи абелевых групп.

Теорема. *Пусть $G \in N_cA$ ($c \geq 1$) и $H \leq G$. Если $H \cap G' = (1)$, то подгруппа H замкнута в G относительно многообразия N_cA.*

Ранее [4] аналогичный результат был получен автором для класса метабелевых групп.

Список литературы

[1] *Шахова С. А.* О существовании решетки доминионов в квазимногообразиях абелевых групп, Известия Алтайского государственного университета. 2011. Т. 69, № 1. С. 31-33.

[2] *Magidin A.* Absolutely closed nil-2 groups, Algebra Universalis. 1999. V. 42, № 1-2. P. 61-77.

[3] *Будкин А. И.* О доминионах в квазимногообразиях метабелевых групп, Сиб. матем. журнал. 2010. Т. 51, № 3. С. 498-505.

[4] *Будкин А. И.* Об абсолютной замкнутости абелевых групп без кручения в классе метабелевых групп. Алгебра и логика. 2014. Т. 53, № 1. С. 15-25.

Алтайский госуниверситет, Барнаул
E-mail: budkin@math.asu.ru

О представлении свободных m-произведений в многообразиях m-групп

С. В. Вараксин

Напомним, что m-группой (G,φ) называется алгебраическая система G сигнатуры $m = \langle \cdot, e, ^{-1}, \vee, \wedge, \varphi\rangle$, которая является ℓ-группой и операция φ — автоморфизм второго порядка группы $\langle G, \cdot, e, ^{-1}\rangle$ и антиизоморфизм решетки $\langle G, \vee, \wedge\rangle$. Пусть $\mathcal{V}$ и $\mathcal{M}$ некоторое многообразие и многообразие всех m-групп. Группу G с частичным порядком P и автоморфизмом второго порядка φ называют ч. у. группой с реверсией, если из $x \leqslant_P y$ следует $\varphi(y) \leqslant_P \varphi(x)$. Назовем также m-группу $(F_{\mathcal{V}},\varphi)$ $\mathcal{V}$-свободной над (G,φ) , если $(F_{\mathcal{V}},\varphi)$ содержится в $\mathcal{V}$, (G,φ) вложима в $(F_{\mathcal{V}},\varphi)$ и любой порядковый φ-гомоморфизм $\alpha_0 : (G,\varphi) \to (H,\varphi)$ в m-группу из $\mathcal{V}$ продолжается до m-гомоморфизма $\alpha : (F_{\mathcal{V}},\varphi) \to (H,\varphi)$.

Пусть $\{(G_i,\varphi_i)\}$ — множество m-групп, $*_i^{\mathcal{V}} G_i$ — их $\mathcal{V}$-свободное произведение, F_λ — все гомоморфные образы $*_i^{\mathcal{M}} G_i$ в $\mathcal{V}$, G' — ч.у.подгруппа с инверсией декартова произведения $\overline{\prod}_\lambda F_\lambda$, порожденная образами G_i при индуцированных гомоморфизмах.

Теорема 1. *$\mathcal{V}$-свободное произведение $*_i^{\mathcal{V}} G_i$ изоморфно подрешетке в $\overline{\prod}_\lambda F_\lambda$, порожденной (G',φ).*

Пусть $F_0 = *_i G_i$ — свободное произведение групп G_i в квазимногообразии $\mathcal{Q}_{\mathcal{V}}$ групп, вложимых в m-группы из $\mathcal{V}$, частичный порядок P на F_0 порожден порядками на G_i, а φ — продолжение φ_i на F_0. Для правого порядка R_λ на F_0, содержащего P, обозначим V_λ наименьшую выпуклую подгруппу, для которой m-группа F_λ, порожденная в $(Aut(\overrightarrow{R_{F_0}(V_\lambda)}) \times Aut(\overleftarrow{R_{F_0}(V_\lambda)}), \varphi)$ правым регулярным представлением группы F_0, лежит в $\mathcal{V}$. Пусть H — подрешетка декартова произведения $\overline{\prod}_\lambda F_\lambda$, порожденная длинными константами — образами G_i при индуцированных индуцированных вложениях $\alpha_i : G_i \to F_\lambda$, $J = \langle (\alpha_i(g)^-)^{-1} \wedge \alpha_i(g)^+ | g \in G_i\rangle$ — m-идеал m-группы (H,φ), а F — фактор-группа H/J по этому m-идеалу.

Теорема 2. *m-группа (F,φ) изоморфна $\mathcal{V}$-свободному произведению m-групп (G_i,φ_i) .*

Список литературы

[1] *Giraudet M., Rachůnek J.* Varieties of half lattice ordered groups of monotonic permutations of chains // Czech. Math. J.1999, 49(124), p.743-766.

[2] Holland C., Scrimger E. Free products of lattice-ordered groups // Algebra Univ. 1972, v.2, p. 247-254.

[3] *Вараксин С. В.* О свободных m-группах и свободных m-произведениях // Изв. Алт.ГУ, N 1-1 (2013), 16–18.

[4] *Вараксин С. В.* О представлении свободных m-групп автоморфизмами линейно упорядоченных множеств // Алгебра и логика, 53:2 (2014), 178-184.

Алтайский госуниверситет, Барнаул
E-mail: varaksins@yandex.ru

О конечных группах с обобщенно субнормальным вложением силовских подгрупп

А. Ф. Васильев, Т. И. Васильева, А. С. Вегера

Рассматриваются только конечные группы. Через $\mathfrak{F}$ обозначается непустая формация. Подгруппа H группы G называется:

1) *$\mathfrak{F}$-субнормальной в G* (обозначается H $\mathfrak{F}$-sn G), если либо $H = G$, либо существует максимальная цепь подгрупп $H = H_0 < H_1 < \cdots < H_n = G$ такая, что $H_i^{\mathfrak{F}} \leq H_{i-1}$ для $i = 1, \ldots, n$;

2) *K-$\mathfrak{F}$-субнормальной в G* (обозначается H K-$\mathfrak{F}$-sn G), если существует цепь подгрупп $H = H_0 \leq H_1 \leq \cdots \leq H_n = G$ такая, что либо $H_{i-1} \trianglelefteq H_i$, либо $H_i^{\mathfrak{F}} \leq H_{i-1}$ для $i = 1, \ldots, n$.

Свойства $\mathfrak{F}$-субнормальных и K-$\mathfrak{F}$-субнормальных подгрупп и их приложения активно изучались в различных направлениях и нашли отражение в многочисленных работах, в частности, в монографиях [**1**], [**2**].

В работе [**3**] было начато рассмотрение следующей общей проблемы.

Проблема. *Изучить влияние $\mathfrak{F}$-субнормальных* (K-*$\mathfrak{F}$-субнормальных*) *силовских подгрупп на строение всей группы.*

Пусть π — подмножество множества всех простых чисел $\mathbb{P}$. Введем классы групп:
$\mathrm{w}_\pi\mathfrak{F} = (G \,|\, 1$ $\mathfrak{F}$-sn G и Q $\mathfrak{F}$-sn G для любой $Q \in \mathrm{Syl}_q(G)$ и $q \in \pi \cap \pi(G))$;

$\overline{\mathrm{w}}_\pi\mathfrak{F} = (G \,|\, Q$ K-$\mathfrak{F}$-sn G для любой $Q \in \mathrm{Syl}_q(G)$ и $q \in \pi \cap \pi(G))$.

Для локальной формации $\mathfrak{F}$, ее максимального внутреннего локального экрана h и любого простого p обозначим через $h_\pi^*(p)$ следующий класс групп:

$h_\pi^*(p) = (G \mid 1$ $\mathfrak{F}$-sn G, Q $\mathfrak{F}$-sn G и $Q \in h(p)$ для любой $Q \in \mathrm{Syl}_q(G)$ и $q \in \pi \cap \pi(G))$.

Теорема 1. *Пусть $\mathfrak{F}$ — наследственная насыщенная формация, h — ее максимальный внутренний локальный экран. Тогда $\mathrm{w}_\pi\mathfrak{F} = LF(f)$, где f — максимальный внутренний локальный экран формации $\mathrm{w}_\pi\mathfrak{F}$ такой, что $f(p) = h_\pi^*(p)$, если $p \in \pi(\mathfrak{F})$, и $f(p) = \varnothing$, если $p \in \mathbb{P} \setminus \pi(\mathfrak{F})$.*

Теорема 2. *Пусть $\mathfrak{F}$ — наследственная насыщенная формация, h — ее максимальный внутренний локальный экран и $\pi(\mathfrak{F}) \subseteq \pi$. Тогда $\overline{\mathrm{w}}_\pi\mathfrak{F} \cap \mathfrak{G}_\pi = LF(g)$, где g — максимальный внутренний локальный экран формации $\overline{\mathrm{w}}_\pi\mathfrak{F} \cap \mathfrak{G}_\pi$ такой, что $g(p) = h_\pi^*(p)$, если $p \in \pi(\mathfrak{F})$; $g(p) = \mathfrak{N}_p$, если $p \in \pi \setminus \pi(\mathfrak{F})$; $g(p) = \varnothing$, если $p \in \mathbb{P} \setminus (\pi \cup \pi(\mathfrak{F}))$.*

Список литературы

[1] *Шеметков Л. А.* Формации конечных групп. М.: Наука.

[2] *Ballester-Bolinches A., Ezquerro L. M.* Classes of Finite Groups. Dordrecht: Springer-Verl., 2006.

[3] *Васильев А. Ф.* О влиянии примарных $\mathfrak{F}$-субнормальных подгрупп на строение группы // Вопросы алгебры. 1995. Вып. 8. С. 31–39.

Гомельский государственный университет им. Ф. Скорины,
Белорусский государственный университет транспорта, Гомель
E-mail: formation56@mail.ru, tivasilyeva@mail.ru, vegera.artem@gmail.com

О $\mathfrak{U}\Phi$-гиперцентрально вложенных подгруппах конечных групп

В. А. Васильев

Все рассматриваемые в данном сообщении группы конечны. Напомним, что подгруппа M группы G называется модулярной подгруппой в G, если выполняются следующие условия:

(1) $\langle X, M \cap Z\rangle = \langle X, M\rangle \cap Z$ для всех $X \leq G, Z \leq G$ таких, что $X \leq Z$, и

(2) $\langle M, Y \cap Z\rangle = \langle M, Y\rangle \cap Z$ для всех $Y \leq G, Z \leq G$ таких, что $M \leq Z$.

Отметим, что модулярная подгруппа является модулярным элементом (в смысле Куроша, [**1**, гл. 2, стр. 43]) решетки всех подгрупп группы. Понятие модулярной подгруппы впервые анализировалось в работе Р. Шмидта [**2**] и оказалось полезным в вопросах классификации составных групп. В частности, в монографии Р. Шмидта [**1**, гл. 5] модулярные подгруппы были использованы для получения новых характеризаций различных классов групп.

Напомним, что главный фактор H/K группы G называется фраттиниевым при условии $H/K \leq \Phi(G/K)$. $Z_\Phi(G)$-гиперцентром ($Z_{\mathfrak{U}\Phi}(G)$-гиперцентром) [**3**] группы G называется произведение всех нормальных подгрупп H из G таких, что все нефраттиниевы G-главные факторы группы H являются центральными (имеют простой порядок).

Найдены следующие условия $\mathfrak{U}\Phi$-гиперцентрального вложения подгрупп конечных групп с заданными модулярными примарными подгруппами.

Теорема. *Пусть E — нормальная подгруппа группы G, и p — простой делитель $|E|$. Предположим, что силовская p-подгруппа P из E имеет подгруппу D такую, что $1 < |D| < |P|$ и каждая подгруппа H из P с порядком $|H| = |D|$ и каждая циклическая подгруппа из P порядка 4 (если $|D| = 2$ и P является неабелевой 2-группой), не имеющие p-нильпотентного добавления в G, являются модулярными в G. Тогда справедливы следующие утверждения.*

(I) *Если $(p-1, |G|) = 1$, то $E/O_{p'}(E) \leq Z_\Phi(G/O_{p'}(E))$.*

(II) *Если $(p-1, |E|) = 1$, то $E/O_{p'}(E) \leq Z_{\mathfrak{U}\Phi}(G/O_{p'}(E))$.*

Список литературы

[1] *Schmidt R.* Subgroup Lattices of Groups — Berlin etc: Walter de Gruyter, 1994. — 572 p.

[2] *Schmidt R.* Modulare Untergruppen endlicher Gruppen // J. Ill. Math. — 1969. — Vol. 13. — P. 358–377.

[3] *Shemetkov L. A., Skiba A. N.* On the $\mathfrak{X}\Phi$-hypercentre of finite groups // J. Algebra. — 2009. — Vol. 322. — P. 2106–2117.

Гомельский государственный университет им. Ф. Скорины, Гомель
E-mail: vovichx@gmail.com

Группы Шмидта с перестановочными и обобщенно перестановочными 2-максимальными и 4-максимальными подгруппами

Ю. В. Горбатова

Все группы в данной работе являются конечными. Подгруппы A и B группы G называются перестановочными, если $AB = BA$. Подгруппа H группы G называется X-перестановочной в G или обобщенно перестановочной [1], где X — непустое подмножество группы G, если для любой подгруппы T из G найдется такой элемент x из X, что $HT^x = T^xH$.

Теорема 1. *Пусть $G = [P]Q$ группа Шмидта, где P и Q – силовские p-подгруппа и q-подгруппа группы G соответственно. В том и только том случае в группе G каждая 2-максимальная подгруппа перестановочна со всеми 4-максимальными подгруппами из G, когда либо $|G| = p^\alpha q^\beta$ для $\alpha+\beta \leq 4$, либо G является группой одного из следующих типов:*

(1) G — группа с абелевыми силовскими подгруппами;

(2) $G = [P]Q$, где $|Q| = q^2$, $|\Phi(P)| \leq p^2$ и $\Phi(P)$ –единственная 2-максимальная подгруппа в P;

(3) $G = [P]Q$, где $|Q| = q$, $|\Phi(P)| \leq p^2$ и $P_3 \subseteq \Phi(P)$ для каждой 3-максимальной подгруппы P_3 из P.

Теорема 2. *Пусть $G = [P]Q$ группа Шмидта, где P и Q – силовские p-подгруппа и q-подгруппа группы G соответственно. В том и только том случае в группе G каждая 2-максимальная подгруппа $F(G)$-перестановочна со всеми 4-максимальными подгруппами из G, когда либо $|G| = p^\alpha q^\beta$ для $\alpha + \beta \leq 4$, либо G является группой одного из следующих типов:*

(1) G — группа с абелевыми силовскими подгруппами;

(2) $G = [P]Q$, где $|Q| = q^2$, $|\Phi(P)| \leq p^2$ и $\Phi(P)$ –единственная 2-максимальная подгруппа в P;

(3) $G = [P]Q$, где $|Q| = q$, $|\Phi(P)| \leq p^2$ и $P_3 \subseteq \Phi(P)$ для каждой 3-максимальной подгруппы P_3 из P.

Следствие. *Пусть G - группа Шмидта и $X = F(G)$ — ее подгруппа Фиттинга. Тогда следующие условия эквивалентны:*

(1) каждая 2-максимальная подгруппа группы G перестановочна со всеми ее 4-максимальными подгруппами;

(2) каждая 2-максимальная подгруппа группы G X-перестановочна со всеми ее 4-максимальными подгруппами.

Список литературы

[1] *Skiba A. N.* H-permutable subgroups // Известия Гомельского государственного университета имени Ф. Скорины. — 2003. — №4(19). — С. 37–39.

Российская академия народного хозяйства и государственной службы при президенте Российской Федерации (Брянский филиал), Брянск
E-mail: lucenko_av@mail.ru

Об одном классе модулей над групповыми кольцами разрешимых групп с ограничениями на систему подгрупп с бесконечными коцентрализаторами

О. Ю. Дашкова

В [**1**] – [**2**] изучались модули над групповыми кольцами разрешимых групп с различными кольцами скаляров, у которых некоторые системы подгрупп удовлетворяли определенным условиям конечности. В настоящей работе изучается $\mathbf{R}G$-модуль A, где $\mathbf{R}$ – ассоциативное кольцо с единицей, G – разрешимая группа. Если $H \leq G$, то фактор-модуль $A/C_A(H)$, рассматриваемый как $\mathbf{R}$-модуль, называется коцентрализатором подгруппы H в модуле A [**5**]. Пусть $\mathbf{L}_{nf}(G)$ – система всех подгрупп группы G, коцентрализаторы которых в модуле A бесконечны. Будем говорить, что группа G удовлетворяет условию $max{-}nf$, если $\mathbf{L}_{nf}(G)$ удовлетворяет условию максимальности как упорядоченное множество.

Основным результатом работы является теорема.

Теорема. *Пусть A - $\mathbf{R}G$-модуль, $\mathbf{R}$ - ассоциативное кольцо с единицей, G - разрешимая группа, удовлетворяющая условию $max - nf$. Если фактор-модуль $A/C_A(G)$ бесконечен, а фактор-группа $G/[G,G]$ бесконечно порождена, то справедливы следующие утверждения:*

1) A обладает конечным рядом $\mathbf{R}G$-подмодулей $\langle 0\rangle \leq C \leq A$, таким, что фактор-модуль A/C конечен, а фактор-группа $Q = G/C_G(C)$ - прюферова q-группа для некоторого простого числа q;

2) $H = C_G(C) \cap C_G(A/C)$ - абелева нормальная подгруппа группы G, коцентрализатор которой в модуле A конечен;

3) группа G почти метабелева.

Список литературы

[1] *Kurdachenko L. A., Subbotin I. Ya.* Linear groups with the maximal condition on subgroups of infinite central dimension // Publicacions Mat. – 2006. – V. 50, № 1. – P. 103–131.

[2] *Дашкова О. Ю.* Об одном классе модулей над групповыми кольцами разрешимых групп с ограничениями на некоторые системы подгрупп // Фундаментальная и прикладная математика. – 2008. – Т. 14, вып. 7. – С. 111–119.

[3] *Dashkova Olga Yu.* Modules over group rings of soluble groups with a certain condition of maximality // Cent. Eur. J. Math. – 2011. – V. 9, № 4. – P. 922–928.

[4] *Дашкова О. Ю.* Об одном классе модулей над целочисленными групповыми кольцами разрешимых групп // Доповiдi НАН України. – 2012. – № 3. – С. 19–23.

[5] *Курдаченко Л. А.* О группах с минимаксными классами сопряженных элементов // Бесконечные группы и примыкающие алгебраические структуры. Академия наук Украины. – Киев, 1993. – С. 160–177.

Филиал Московского государственного университета в г. Севастополе, Севастополь
E-mail: odashkova@yandex.ru

О строгой вещественности и рациональности унитреугольной группы над полем характеристики 2

О. В. Дубина, С. Г. Колесников, Н. С. Манагарова

Периодическую группу G назовем *(строго) вещественной*, если каждый её элемент сопряжен (инволюцией) со своим обратным. Если всякий элемент $g \in G$ сопряжен с любой своей степенью взаимно простой с $|g|$, то G назовем *рациональной* группой. В случае конечности G последнее определение эквивалентно определению рациональной группы через значения её комплексных характеров.

В связи с вопросами из [**1**] в [**2**] было установлено, что группа унитреугольных матриц порядка $n \geqslant 13$ над полем из двух элементов $UT_n(2)$ не является вещественной, а группы $UT_n(2)$ при $n \leqslant 6$ рациональны. Отвечая на вопрос 16.76 из [**3**] в [**4**] и двух работах М.А. Газдановой была доказана строгая вещественность групп $UT_n(K)$ при $n \leqslant 7$ над любым полем K характеристики 2. Для доказательства приведенных результатов авторы цитированных работ сопоставляли произвольной матрице $A = ||a_{ij}|| \in UT_n(K)$, $char(K) = 2$, ориентированный граф $\overrightarrow{\Gamma}(A)$ и граф коммутативности $\Gamma(A)$, вершинами которых являются ненулевые недиагональные элементы матрицы A, две вершины a_{ij} и a_{km} соединены ребром (направленным ребром $a_{ij} \to a_{km}$), если $j = k$. Оказалось, что если $\Gamma(A)$ — лес, то A строго вещественная матрица, а если на вершинах $\overrightarrow{\Gamma}(A)$ можно задать такую целочисленную функцию l, что $l(a_{jk}) = l(a_{ij})+1$, когда ребро $a_{ij} \to a_{jk}$ принадлежит $\overrightarrow{\Gamma}(A)$, то A сопряжена с любой своей нечетной степенью. Авторами тезиса доказана

Теорема 1. *Каждый класс сопряжённости группы $UT_n(K)$, $n \leqslant 8$, K — произвольное поле, содержит матрицу, граф коммутативности которой есть лес.*

Из теоремы 1 и возможности задать функцию l на любом орграфе, полученном произвольным выбором ориентации ребер произвольного леса, следует

Теорема 2. *Пусть K — поле характеристики 2. Группа $UT_n(K)$ является строго вещественной и рациональной, если $n \leqslant 8$.*

Также установлен следующий критерий рациональности 2-группы.

Теорема 3. *2-группа G является рациональной тогда и только тогда, когда для любого элемента $x \in G$ найдутся такие $y, z \in G$, что $x^y = x^3$ и $x^z = x^{-1}$.*

Список литературы

[1] *Kirillov A.* Variation on the upper triangular theme // AMS Transl. 1995. Vol. 169, P. 43–73.

[2] *Isaacs I. M., Karagueuzian D.* Conjugacy in groups of upper triagular matrices // J. Algebra. 1998. Vol. 202, P. 704–711. Erratum // J. Algebra. 1998. Vol. 208, P. 722.

[3] *Коуровская тетрадь* // Новосибирск. ИМ СО РАН. 2006.

[4] *Газданова М. А., Нужин Я. Н.* О строгой вещественности унипотентных подгрупп групп лиева типа над полем характеристики 2 // СМЖ. 2006. Т. 47, N 5. С. 1031-1051.

СФУ, СибГАУ, Красноярск
E-mail: sklsnkv@mail.ru

Об автоморфизмах дистанционно регулярного графа с массивом пересечений $\{99, 84, 30; 1, 6, 54\}$

К. С. Ефимов, А. А. Махнев

Мы рассматриваем неориентированные графы без петель и кратных ребер. Для вершины a графа Γ через $\Gamma_i(a)$ обозначим i-окрестность вершины a и положим $[a] = \Gamma_1(a)$.

А.А. Махневым предложена программа изучения дистанционно регулярных графов, в которых окрестности вершин сильно регулярны со вторым собственным значением 3. Сильно регулярный граф с параметрами (99,14,1,2) имеет второе собственное значение 3. В работе [**1**] найдены массивы пересечений дистанционно регулярных графов, в которых окрестности вершин сильно регулярны с параметрами (99,14,1,2):

Пусть Γ — дистанционно регулярный граф, в котором окрестности вершин сильно регулярны с параметрами $(99, 14, 1, 2)$. Тогда либо Γ — антиподальный граф с массивом пересечений $\{99, 84, 1; 1, 14, 99\}$ или $\{99, 84, 1; 1, 12, 99\}$, либо Γ — примитивный граф с массивом пересечений $\{99, 84, 30; 1, 6, 54\}$. В данной работе изучаются автоморфизмы гипотетического дистанционно регулярного графа с массивом пересечений $\{99, 84, 30; 1, 6, 54\}$ и $v = 48 \cdot 47$ вершинами.

Теорема. *Пусть Γ — дистанционно регулярный граф, имеющий массив пересечений $\{99, 84, 30; 1, 6, 54\}$, $G = \mathrm{Aut}(\Gamma)$, g — элемент из G простого порядка p и $\Omega = \mathrm{Fix}(g)$. Тогда $\pi(G) \subseteq \{2, 3, 5, 7, 11, 13\}$ и выполняется одно из следующих утверждений:*

(1) Ω — пустой граф, $p = 2$, $\alpha_1(g) = 42r - 14m + 22s - 30$ и $\alpha_3(g) = 56m - 88s$ или $p = 3$, $\alpha_1(g) = 198n + 18l + 114$ и $\alpha_3(g) = 12l$;

(2) Ω — клика, $p = 11$ и $|\Omega| = 1$, или $p = 7$ и $|\Omega| \in \{2, 9\}$, или $p = 2$ и $|\Omega| \in \{2, 4, ..., 12\}$;

(3) Ω состоит из вершин попарно находящихся на расстоянии 3 в Γ, $|\Omega| > 1$, $p = 3$ и $|\Omega| \in \{3, 6, ..., 21\}$;

(4) Ω является объединением изолированных n-клик, $n = 1, 4, 7, 11$ и $p = 3$;

(5) Ω содержит вершины, находящихся на расстоянии 2 и $p \le 13$.

Ввиду теоремы дистанционно регулярный граф с массивом пересечений $\{99, 84, 30; 1, 6, 54\}$ не является вершинно симметричным.

Список литературы

[1] *Махнев А. А.* О графах, в которых окрестности вершин сильно регулярны с параметрами (99,14,1,2) // Доклады академии наук 2011, т. 439, N 4, 443–447.

Институт математики и механики им. Н. Н. Красовского УрО РАН, Уральский федеральный университет, Екатеринбург

E-mail: konstantin.s.efimov@gmail.com, makhnev@imm.uran.ru

О локально конечных π-разделимых группах

А. Х. Журтов, З. Б. Селяева

Пусть π — некоторое множество простых чисел, π' — его дополнение во множестве всех простых чисел. Группа называется π-группой, если она периодическая и порядок каждого ее элемента делится только на простые числа из π. Группа называется π-разделимой, если она обладает конечным нормальным рядом, каждый фактор которого является π-группой или π'-группой. Такой ряд называется π-рядом, а π-длиной π-разделимой группы называется наименьшее из возможных чисел нетривиальных π-факторов во всех π-рядах этой группы.

Для конечных групп понятие π-разделимой группы ввел С.А.Чунихин [**1**] вместе с определениями π-отделимой и π-разрешимой группой. Согласно Чунихину, конечная группа G называется π-разделимой, если любой ее главный фактор является либо π-группой, либо π'-группой. Конечные π-разделимые группы интенсивно изучались на протяжении всех лет развития теории конечных групп, начиная с классических работ Чунихина [**1**] и Ф.Холла [**2**].

Локально конечные π-разделимые группы, которым посвящена настоящее сообщение, до настоящего времени практически не изучались. Основным нашим результатом является следующая

Теорема. *Пусть G — локально конечная π-разделимая группа и m — натуральное число. Ели π-длина любой конечной подгруппы из G не превосходит m, то π-длина G не превосходит m.*

Список литературы

[1] *Чунихин С. А.* О силовских свойствах конечных групп. Доклады АН СССР, 73, № 1 (1950), с.29–32.

[2] *Hall P.* Theorems like Sylow's. Proc. London, Math. Soc.(3), 6 (1956), p.286–304.

Кабардино-Балкарский госуниверситет, г. Нальчик
E-mail: zhurtov_a@mail.ru

О пересечениях нильпотентных подгрупп в конечных группах со спорадическим простым цоколем

В. И. Зенков

В работе автора [**1**, теорема B] было доказано, что в конечной группе со с порадическим простым цоколем для любой силовской подгруппы найдется сопряженная с ней и такая, что что их пересечение единично. В данной работе эта теорема распространяется на все нильпотентные подгруппы такой группы, а именно, доказана следующая

Теорема. *Пусть G — конечная группа со спорадическим простым цоколем, A и B — нильпотентные подгруппы из G. Тогда $A \cap B^g = 1$ для некоторого элемента $g \in G$.*

Из этой теоремы следует положительное решение задачи 15.40 из [**2**] в классе спорадических простых групп.

Список литературы

[1] *Зенков В. И.* Пересечение нильпотентных подгрупп в конечных группах // Фундамент. и прикл. матем. 1996. Т. 2, № 1. С. 1–92.

[2] Нерешенные вопросы теории групп. Коуровская тетрадь. 15-е изд. Новосибирск: Новосиб. гос. ун-т, 2002.

ИММ УрО РАН, Екатеринбург
E-mail: v1i9z52@mail.ru

О многообразиях m-групп

А. В. Зенков, О. В. Исаева

Напомним [**1**], что m-группой называется алгебраическая система G сигнатуры $m = \langle \cdot, e, ^{-1}, \vee, \wedge, \ _* \rangle$, где $\langle G, \cdot, e, ^{-1}, \vee, \wedge \rangle$– ℓ–группа и $_*$– автоморфизм второго порядка группы $\langle G, \cdot, e, ^{-1} \rangle$ и антиавтоморфизм решетки $\langle G, \vee, \wedge \rangle$. Стандартно, m-группу G с фиксированным автоморфизмом $_*$ записываем как пару $(G, \ _*)$. Через M обозначим многообразие всех m–групп. Относительно теоретико-множественного включения M является частично упорядоченным множеством. Более того, M есть решетка относительно естественно определенных операций пересечения и объединения многообразий m–групп.

Через $\mathcal{I}$ обозначим многообразие m-групп, определяемое тождеством $x_* = x^{-1}$, которое является наименьшим нетривиальным элементом M. Для каждого натурального n определим $\mathcal{I}^n = \underbrace{\mathcal{I} \cdot \ldots \cdot \mathcal{I}}_{n\text{-раз}}$. В [**1**], в частности, доказано, что $\mathcal{I}^n$ определяется тождеством $x_*^{2^{n-1}} = x^{2^{n-1}}$. Мы показываем, что других многообразий, определяемых подобными тождествами, нет. Более точно, если $n = 2^m(2s+1), m \geq 0, s > 0$, то тождество $x_*^n = x^{-n}$ влечет $x_* = x^{-1}$. Многообразие $\mathcal{I}^2$ содержит многообразие $\mathcal{S}$, порожденное m-группой $(S,_*)$, где $S = \langle a_1, a_2, b | \ [a_1, a_2] = e, a_1^b = a_2, a_2^b = a_1 \rangle$ и $_* : b \to b^{-1}, a_1 \to a_1^{-1}, a_2 \to a_2^{-1}$. Показано, что $\mathcal{S}$ строго содержится в $\mathcal{I}^2$. Важность $\mathcal{S}$ объясняется тем, что оно является единственным неабелевым накрытием многообразия $\mathcal{I}$ в решетке M.

Далее, построены новые идемпотенты решетки M.

Список литературы

[1] *Giraudet M., Rachunek J.* Varieties of half lattice-ordered groups of monotonic permutations of chains// Czech. Math. J. 1999. V.49, №124. P. 743–766.

Алтайский Государственный Аграрный Университет, кафедра математики
Алтайский Государственный Университет, кафедра МЭММБИ, Барнаул
E-mail: alexey_zenkov@yahoo.com, isaeva@econ.asu.ru

О совпадении графов Грюнберга–Кегеля двух конечных простых классических групп лиева типа над полями разных характеристик

М. Р. Зиновьева

Пусть $\pi(n)$ обозначает множество простых делителей натурального числа n. *Граф простых чисел* или *граф Грюнберга–Кегеля* $GK(G)$ конечной группы G определяется как граф с множеством вершин $\pi(|G|)$, в котором различные вершины r и s смежны тогда и только тогда, когда G содержит элемент порядка rs.

В "Коуровской тетради" А. В. Васильев поставил вопрос 16.26 об описании всех пар неизоморфных конечных простых неабелевых групп с одинаковым графом Грюнберга–Кегеля. Хаги (2003) и М. А. Звездина (2013) получили такое описание в случае, когда одна из групп совпадает со спорадической и знакопеременной группой соответственно. Автор [**1**] исследовала этот вопрос для конечных простых групп лиева типа над полями одной характеристики.

В данной работе продолжается исследование, начатое автором в [**1**] и [**2**]. В частности, уточняется результат, полученный автором в [**2**].

Обозначим через $\mathcal{M}$ множество конечных простых классических групп $A_{n-1}^{\pm}(q)$, где $n \geq 7$, $B_n(q)$, где $n \geq 5$, $C_n(q)$, где $n \geq 5$, $D_n^{\pm}(q)$, где $n \geq 5$.

Далее в теоремах $q = p^f$ и $q_1 = {p_1}^{f_1}$, где p, p_1 – различные простые числа и f, f_1 – натуральные числа.

Теорема 1. *Пусть G и G_1 – неизоморфные группы из $\mathcal{M}$ над полями порядков q и q_1 соответственно. Если графы $GK(G)$ и $GK(G_1)$ совпадают, то выполнено одно из следующих утверждений:* (1) $\{G, G_1\} = \{A_{n-1}^{\pm}(q), A_{n_1-1}^{\pm}(q_1)\}$, *где* $n_1 \in \{n-1, n, n+1\}$; (2) $\{G, G_1\} = \{B_n(q), B_n(q_1)\}$; (3) $\{G, G_1\} = \{B_n(q), C_n(q_1)\}$; (4) $\{G, G_1\} = \{C_n(q), C_n(q_1)\}$; (5) $\{G, G_1\} = \{D_7(q), D_8(q_1)\}$; (6) $\{G, G_1\} = \{D_n(q), D_n(q_1)\}$; (7) $\{G, G_1\} = \{{}^2D_7(q_1), D_8(q)\}$; (8) $\{G, G_1\} = \{{}^2D_n(q), {}^2D_n(q_1)\}$; (9) $\{G, G_1\} = \{A_7(q), D_6(q_1)\}$; (10) $\{G, G_1\} = \{{}^2A_7(q), D_6(q_1)\}$; (11) $\{G, G_1\} = \{A_{n-1}^{\pm}(q), D_{n_1}(q_1)\}$, *где* $n_1 \in \{2n/3 - 1/3, 2n/3 - 1\}$ *и* $31 \leq n_1 \equiv 3 \pmod 4$.

Теорема 2. *Пусть $G = A_1(q)$ и $G_1 = A_1(q_1)$ – неизоморфные простые группы. Графы $GK(G)$ и $GK(G_1)$ совпадают тогда и только тогда, когда*

$$\{G, G_1\} = \{A_1(5), A_1(4)\}, \{A_1(9), A_1(4)\}, \{A_1(9), A_1(5)\}, \{A_1(7), A_1(8)\}.$$

Теорема 3. *Пусть $|\pi(q^2-1)| \leq 4$, G – одна из групп $B_3(q)$, $B_n(q)$, где $n \geq 4$ четно, $C_3(q)$, $C_n(q)$, где $n \geq 4$ четно, $D_4(q)$, ${}^2D_n(q)$, где n нечетно, G_1 – неизоморфная группе G конечная группа лиева типа над полем порядка q_1 и $GK(G) = GK(G_1)$. Тогда G_1 не изоморфна группам $B_{n_1}(q_1)$, где $n_1 \geq 3$, $C_{n_1}(q_1)$, где $n_1 \geq 3$, $D_4(q_1)$, ${}^2D_{n_1}(q_1)$.*

Работа выполнена при финансовой поддержке РФФИ (проект 13-01-00469) и Комплексной программы фундаментальных исследований УрО РАН (проект 15-16-1-5).

Список литературы

[1] *Зиновьева М. Р.* Конечные простые группы лиева типа над полем одной характеристики с одинаковым графом простых чисел // Тр. Ин-та математики и механики УрО РАН. 2014. Т. 20, N 2. С. 168-183.

[2] *Зиновьева М. Р.* О графах простых чисел конечных простых классических групп над полями разных характеристик // Алгебра и приложения: Тр. Межд. конф. по алгебре. Нальчик: Изд-во КБГУ, 2014. С. 55-57.

ИММ УрО РАН, УрФУ, Екатеринбург
E-mail: zinovieva-mr@yandex.ru

Об одном примере наследственной сверхрадикальной формации

С. Ф. Каморников

Рассматриваются только конечные группы.

Пусть $\mathfrak{F}$ — непустая формация, т.е. класс групп, замкнутый относительно взятия факторгрупп и конечных подпрямых произведений. Подгруппа H группы G называется $\mathfrak{F}$-субнормальной, если либо $H = G$, либо существует максимальная цепь подгрупп

$$H = H_0 \subset H_1 \subset ... \subset H_n = G$$

такая, что $H_i/Core_{H_i}(H_{i-1}) \in \mathfrak{F}$ для всех i =1, 2, ... ,n.

Понятие $\mathfrak{F}$-субнормальной подгруппы, введенное в классе конечных разрешимых групп Картером и Хоуксом, а в произвольном случае – Л.А. Шеметковым, сформировало в теории конечных групп содержательное направление, связанное с изучением сверхрадикальных формаций.

Формация $\mathfrak{F}$ называется сверхрадикальной, если она удовлетворяет следующим требованиям:

1) $\mathfrak{F}$ — нормально наследственная формация;

2) любая группа $G = AB$, где A и B — $\mathfrak{F}$-субнормальные $\mathfrak{F}$-подгруппы из G, принадлежит $\mathfrak{F}$.

Осознание роли сверхрадикальных формаций в решении целого ряда классификационных проблем привело к проблеме их описания. В 1999 году в "Коуровской тетради" под номером 14.99 Л.А. Шеметковым были сформулированы две задачи:

(а) *Найти все сверхрадикальные локальные формации.*

(б) *Доказать, что всякая наследственная сверхрадикальная формация является разрешимо насыщенной.*

В данной работе приводится пример наследственной сверхрадикальной формации, которая содержит все нильпотентные группы и не является разрешимо насыщенной. В частности, дается отрицательный ответ на вопрос 14.99 б).

Напомним, что формация $\mathfrak{F}$ называется разрешимо насыщенной, если для любой разрешимой нормальной подгруппы N группы G из $G/\Phi(N) \in \mathfrak{F}$ всегда следует $G \in \mathfrak{F}$. Зафиксируем также следующие обозначения: $\mathfrak{S}_\pi$ — формация всех разрешимых π-групп, $\mathfrak{N}_{\pi'}$ — формация всех нильпотентных π'-групп.

Теорема. *Пусть G — группа, изоморфная $Sz(2^3)$, и $\pi = \pi(G) = \{2, 5, 7, 13\}$. Если $\mathfrak{F} = \mathfrak{H}\mathfrak{S}_\pi \times \mathfrak{N}_{\pi'}$, где $\mathfrak{H}$ — формация, порожденная группой G, то справедливы следующие утверждения:*

(1) *Формация $\mathfrak{F}$ является наследственной и сверхрадикальной.*

(2) *Формация $\mathfrak{F}$ не является разрешимо насыщенной.*

Международный университет "МИТСО", Гомель, Беларусь
E-mail: sfkamornikov@mail.ru

О нормально вложенных подгруппах конечных групп

В. Н. Княгина, В. С. Монахов

Рассматриваются только конечные группы. Запись $H \le G$ означает, что H — подгруппа группы G, $|H|$ — порядок подгруппы H, а H^G — наименьшая нормальная в G подгруппа, содержащая H. Нильпотентным корадикалом группы G называется наименьшая нормальная подгруппа в G, фактор-группа по которой нильпотентна. $\pi(G)$ — множество всех простых делителей $|G|$. Подгруппа H группы G называется холлово нормально вложенной в G, если H — холлова подгруппа в H^G, [**1**, определение 1].

Shirong Li и Jianjun Liu предложили следующую задачу [**2**, проблема 1]: Изучить группу G, в которой существует холлово нормально вложенная подгруппа H порядка $|B|$ для каждой $B \le G$. В частности, G разрешима?

Adolfo Ballester–Bolinches и ShouHong Qiao [**3**] решили эту проблему. Они ввели класс $\mathfrak{X}$, состоящий из всех групп G, в которых существует холлово нормально вложенная подгруппа H порядка $|B|$ для каждой $B \le G$.

Теорема. [**3**] *Группа G принадлежит классу $\mathfrak{X}$ тогда и только тогда, когда G разрешима и ее нильпотентный корадикал является циклической подгруппой порядка, свободного от квадратов.*

Подгруппа H называется S-перестановочной в G, если $HP = PH$ для каждой силовской подгруппы P группы G. Пусть класс $\mathfrak{X}_1$ состоит из всех групп G со следующим свойством: для любого $p \in \pi(G)$ и любой подгруппы B из G с силовской p-подгруппой порядка p существует S-перестановочная подгруппа с холловой подгруппой U порядка $|B|$. Ясно, что $\mathfrak{X} \subseteq \mathfrak{X}_1$. Мы доказали, что $\mathfrak{X} = \mathfrak{X}_1$.

Список литературы

[1] *Li Shirong, He Jun, Nong Guoping, Zhou Longqiao.* On Hall normally embedded subgroups of finite groups // Comm. Algebra. 2009. Vol. 37. P. 3360–3367.

[2] *Li Shirong, Liu Jianjun.* On Hall subnormally embedded and generalized nilpotent groups // J. Algebra. 2013. Vol. 388. P. 1–9.

[3] *Ballester–Bolinches Adolfo, Qiao ShouHong.* On a problem posed by S. Li and J. Liu // Arch. Math. 2014. Vol. 102. P. 109–111.

Гомельский инженерный институт МЧС Республики Беларусь, Гомель, Беларусь,
Гомельский государственный университет им. Ф. Скорины, Гомель, Беларусь
E-mail: knyagina@inbox.ru, Victor.Monakhov@gmail.com

Конечные группы с обобщенно субнормальными вторыми и третьими максимальными подгруппами

В. А. Ковалева

Все рассматриваемые в сообщении группы являются конечными. Символом $\pi(G)$ обозначается множество всех простых делителей порядка группы G.

Напомним, что подгруппа H группы G называется 2-максимальной (второй максимальной) подгруппой в G, если H является максимальной подгруппой в некоторой максимальной подгруппе M группы G. Аналогично могут быть определены 3-максимальные подгруппы и т.д.

В 2005 году на Гомельском алгебраическом семинаре Л.А. Шеметковым была поставлена задача изучения групп, все n-максимальные подгруппы которых являются обобщенно субнормальными.

Одним из обобщений субнормальности является понятие K-$\mathfrak{U}$-субнормальной подгруппы. Напомним, что подгруппа H группы G называется *$\mathfrak{U}$-субнормальной в смысле Кегеля* [**1**] или *K-$\mathfrak{U}$-субнормальной* [**2**, с. 236] в G, если существует такая цепь подгрупп $H = H_0 \leq H_1 \leq \cdots \leq H_t = G$, что либо H_{i-1} нормальна в H_i, либо $H_i/(H_{i-1})_{H_i}$ сверхразрешима для всех $i = 1, \ldots, t$.

Нами получено полное описание групп, у которых все вторые либо все третьи максимальные подгруппы являются K-$\mathfrak{U}$-субнормальными. Заметим, что каждая подгруппа сверхразрешимой группы K-$\mathfrak{U}$-субнормальна. Более того, ввиду [**3**, Теорема A], в случае, когда $|\pi(G)| > 4$ и каждая 3-максимальная подгруппа группы G является K-$\mathfrak{U}$-субнормальной в G, группа G сверхразрешима. Поэтому для описание групп с K-$\mathfrak{U}$-субнормальными третьими максимальными подгруппами нам нужно было рассмотреть лишь несверхразрешимые группы с числом простых делителей, равным 2, 3 и 4. При этом оказалось, что в бипримарном случае такая группа может не иметь нормальных силовских подгрупп; в случае, когда $|\pi(G)| = 3$, группа G является ϕ-дисперсивной для некоторого упорядочения ϕ множества $\pi(G)$; и, наконец, в случае, когда $|G|$ имеет четыре простых делителя, G дисперсивна по Оре.

Список литературы

[1] *Kegel O. H.* Zur Struktur mehrfach faktorisierbarer endlicher Gruppen // Math. Z. — 1965. — Vol. 87. — P. 409-434.

[2] *Ballester-Bolinches A., Ezquerro L. M.* Classes of Finite Groups. — Dordrecht: Springer-Verlag, 2006.

[3] *Kovaleva V. A., Skiba A. N.* Finite soluble groups with all n-maximal subgroups $\mathfrak{F}$-subnormal // Journal of Group Theory. — 2014. — Vol. 17. — P. 273-290.

Гомельский государственный университет им. Ф. Скорины, Гомель
E-mail: vika.kovalyova@rambler.ru

О конечных группах, которые имеют несвязный граф простых чисел и композиционный фактор, изоморфный $Sp_4(4)$

В. А. Колпакова, А. С. Кондратьев, И. В. Храмцов

Пусть G — конечная группа. Обозначим через $\pi(G)$ множество всех простых делителей порядка группы G. *Граф простых чисел* (*граф Грюнберга — Кегеля*) $\Gamma(G)$ группы G определяется как граф с множеством вершин $\pi(G)$, в котором две различные вершины p и q смежны тогда и только тогда, когда в G есть элемент порядка pq. Группа G называется n-*примарной*, если $|\pi(G)| = n$.

Второй и третий авторы в статье [**1**] исследовали конечные 4-примарные группы G с несвязным графом простых чисел. В теореме 6 этой статьи был пропущен случай, когда G имеет композиционный фактор, изоморфный $Sp_4(4)$. Мы восполняем этот пробел, доказывая следующую теорему.

Теорема. *Пусть G — конечная группа с несвязным графом простых чисел, $\overline{G} = G/F(G)$ и $Soc(G) \cong Sp_4(4)$. Тогда $\overline{G} \cong Sp_4(4)$, $Sp_4(4):2$ или $Sp_4(4):4$, $F(G) = O_2(G)$ и каждый $2-$главный фактор в G как $GF(2)\overline{G}$-модуль изоморфен одному из следующих модулей:*

(1) *если $\overline{G} \cong Sp_4(4)$ или $Sp_4(4):2$, то одному из двух квазиэквивалентных $GF(2)\overline{G}$-модулей размерности $8, 16$ или 32;*

(2) *если $\overline{G} \cong Sp_4(4):4 \cong Aut(Sp_4(4))$, то одному из единственных $GF(2)\overline{G}$-модулей размерности $16, 32$ или 64.*

Работа выполнена при финансовой поддержке РФФИ (проект 13-01-00469), Комплексной программы фундаментальных исследований УрО РАН (проект 15-16-1-5) и в рамках проекта повышения конкурентоспособности (Соглашение между Министерством образования и науки Российской Федерации и Уральским федеральным университетом от 27.08.2013, №02.A03.21.0006).

Список литературы

[1] *Кондратьев А. С., Храмцов И. В.* О конечных четырепримарных группах, Труды Ин-та математики и механики УрО РАН, 17, № 4 (2011), 142–159.

Институт математики и механики им. Н. Н. Красовского УрО РАН, Уральский федеральный университет, Екатеринбург
E-mail: leralid@mail.ru, a.s.kondratiev@imm.uran.ru, ihramtsov@gmail.com

О главных факторах параболических максимальных подгрупп группы $^3D_4(q^3)$

В. В. Кораблева

Эта работа является продолжением работ [**1, 2, 3**], в которых было получено уточненное описание главных факторов параболической максимальной подгруппы, входящих в ее унипотентный радикал, для всех конечных групп нормального лиева типа, за исключением специальных групп, для скрученных классических групп и для группы $^2E_6(q^2)$. Группа лиева типа называется *специальная*, если характеристика поля $p = 2$ для групп типа B_l, C_l, F_4 и $p \leqslant 3$ для групп типа G_2.

Автор рассматривает конечную простую группу лиева типа $^3D_4(q^3)$ и $P = UL$ — параболическую максимальную подгруппу в ней, где U — унипотентный радикал и L — дополнение Леви в P. Из статьи [**4**] следует, что факторы нижнего центрального ряда группы U являются главными факторами группы P и являются неприводимыми $GF(q)L$-модулями или $GF(q^3)L$-модулями.

Если A и B — нормальные подгруппы группы P, B — подгруппа A и фактор-группа A/B является минимальной нормальной подгруппой в P/B, то A/B называется *главным фактором* группы P.

В настоящей работе для конечной простой группы $^3D_4(q^3)$ уточняется описание главных факторов каждой ее параболической максимальной подгруппы, входящих в унипотентный радикал. Приводится таблица, в которой указываются порядки и порождающие элементы соответствующих главных факторов.

Работа выполнена при финансовой поддержке РФФИ (проект 13-01-00469) и Лаборатории квантовой топологии Челябинского госуниверситета (грант правительства РФ № 14.Z50.31.0020).

Список литературы

[1] *Кораблева В. В.* О главных факторах параболических максимальных подгрупп конечных простых групп нормального лиева типа // Сиб. мат. журн. 2014. Т. 55, № 4. С. 764–782.

[2] *Кораблева В. В.* О главных факторах параболических максимальных подгрупп группы $^2E_6(q^2)$ // Тр. Ин-та математики и механики УрО РАН. Екатеринбург, 2014. Т. 20, № 2. С. 230–237.

[3] *Кораблева В. В.* О главных факторах параболических максимальных подгрупп скрученных классических групп // Мальцевские чтения 2014: тез. докл. Междунар. конф. Новосибирск, 2014. С. 64.

[4] *Azad H., Barry M., Seitz G.* On the structure of parabolic subgroup // Comm. Algebra. 1990. Vol. 18, no. 2. P. 551–562.

Челябинский государственный университет, Челябинск; Институт математики и механики им. Н.Н. Красовского УрО РАН, Екатеринбург

E-mail: vvk@csu.ru

Некоторые свойства производных Фокса

А. Ф. Красников

Пусть $F = (\underset{i\in I}{*} A_i) * G$ — свободное произведение нетривиальных групп A_i $(i \in I)$ и свободной группы G с базой $\{g_j | j \in J\}$. Следуя Романовскому [**1**], обозначим через D_k $(k \in I \cup J)$ производные Фокса кольца $\mathbf{Z}(F)$.

Теорема. *Пусть F — свободное произведение нетривиальных групп A_i $(i \in I)$ и свободной группы G с базой $\{g_j | j \in J\}$, N— нормальная подгруппа в F такая, что $N \cap A_i = 1$ $(i \in I)$, X — множество элементов из F, полученное объединением $\{g_j | j \in J\}$ с множеством элементов групп A_i $(i \in I)$; $u \to \bar{u}$ — функция, выбирающая правые шрайеровы представители F по N, S — множество выбранных представителей; f — функция, отображающая элементы x из X в $I \cup J$: если $x = g_j$ то $f(x) = j$, если $x \in A_i$ то $f(x) = i$; $w \in N$. Если $w = w_1^{k_1} \dots w_l^{k_l}$, где $w_i = s_i x_i \overline{s_i x_i}^{-1} \neq 1$, $s_i \in S$, $x_i \in X$ $(i = 1, \dots, l)$, $k_1, \dots, k_l$ — целые, отличные от нуля числа и элемент w нельзя представить по модулю $[N, N]$ в виде произведения степеней меньшего чем l числа элементов вида $sx\overline{sx}^{-1}$, $s \in S$, $x \in X$, то $D_{f(x_i)}(w) \not\equiv 0 \ mod\ N$ $(i = 1, \dots, l)$.*

Следствие. *Пусть F — свободное произведение нетривиальных групп A_i $(i \in I)$ и свободной группы G с базой $\{g_j | j \in J\}$, N— нормальная подгруппа в F, $N \cap A_i = 1$ $(i \in I)$. Элемент v группы F принадлежит $[N, N]$ тогда и только тогда, когда $D_k(v) \equiv 0 \mod N$, $k \in I \cup J$.*

Следствие равносильно, в случае отсутствия в произведении F множителей A_i $(i \in I)$, вложению Магнуса [**2**] для группы $F/[N, N]$, а в произвольном случае - обобщению вложения Магнуса, полученному Романовским [**1**]:

Пусть F — свободное произведение нетривиальных групп A_i $(i \in I)$ и свободной группы G с базой $\{g_j | j \in J\}$, N— нормальная подгруппа в F такая, что $N \cap A_i = 1$ $(i \in I)$. Пусть T — правый свободный $\mathbf{Z}(F/N)$-модуль с базой $\{t_k | k \in I \cup J\}$. Рассмотрим гомоморфизм

$$\varphi : F \to \begin{pmatrix} F/N & 0 \\ T & 1 \end{pmatrix}$$

определяемый отображением

$$a_i \mapsto \begin{pmatrix} a_i N & 0 \\ t_i(a_i N - 1) & 1 \end{pmatrix} (a_i \in A_i,\ i \in I),\ g_j \mapsto \begin{pmatrix} g_j N & 0 \\ t_j & 1 \end{pmatrix} (j \in J).$$

Тогда $ker\varphi = [N, N]$.

Список литературы

[1] *Романовский Н. С.* О вложении Шмелькина для абстрактных и проконечных групп, Алгебра и логика, 38, N 5 (1999), 598–612.

[2] *Magnus W.* On a theorem of Marshall Hall, Ann. of Math., 40, N 4 (1939), 764–768.

Омский государственный университет, г. Омск
E-mail: phomsk@mail.ru

О графах Кэли двупорожденных групп периода 4

А. С. Кузнецова, А. А. Кузнецов

Графы Кэли находят применение в задачах проектирования топологий многопроцессорных вычислительных систем (МВС) благодаря таким хорошим свойствам как регулярность, вершинно-транзитивность, малые диаметр и степень при достаточно большом количестве вершин в графе. Поэтому изучение графов Кэли различных классов конечных групп является актуальной задачей.

Пусть $\mathbb{X} = \{x_1, x_1^{-1}, x_2, x_2^{-1}\}$, где $x_i^{-1} = x_i^3$, — симметричное порождающее множество некоторой группы G, период которой равен 4. Графом Кэли $\Gamma = Cay(G, \mathbb{X}) = (V, E)$ будет являться неориентированный граф, в котором множество вершин $V(\Gamma)$ соответствует элементам группы G, а множество ребер $E(\Gamma)$ состоит из всех упорядоченных пар (g, hg), где $g \in G$ и $h \in \mathbb{X}$.

Количество вершин Γ равно порядку порождающей группы, т. е. $|V| = |G|$. Граф Кэли является регулярным и его степень s, т. е. количество ребер, выходящее из каждой вершины, равно числу порождающих элементов группы: $s = |\mathbb{X}| = 4$. Диаметр графа Кэли D (средний диметр d), т. е. максимальное (среднее) кратчайшее расстояние от произвольной фиксированной вершины до других вершин графа, равен максимальной (средней) длине минимальных слов группы, записанных через порождающие элементы в лексикографическом порядке.

При рассмотрении графа в качестве топологии МВС берут во внимание следующие характеристики графа: количество вершин, степень (для регулярного графа), диаметр и средний диаметр. В табл. приведены указанные характеристики графов Кэли некоторых двупорожденных групп периода 4, которые были получены при помощи компьютерных вычислений. Порождающие множества были взяты симметричными, поскольку в этом случае графы будут неориентированными. Именно неориентированные графы, как правило, используют при проектировании топологий МВС.

$\|G\|$	s	D	d
2^4	4	4	2
2^5	4	4	$2,5$
2^6	4	6	$\approx 3,4$
2^7	4	8	$\approx 4,1$
2^8	4	8	$\approx 5,2$
2^9	4	10	$\approx 5,9$
2^{10}	4	12	$\approx 6,6$
2^{11}	4	14	$\approx 7,8$
2^{12}	4	16	$\approx 9,0$

Работа выполнена при поддержке Министерства образования и науки РФ (проект Б 112/14), а также гранта Президента РФ (проект МД 3952.2015.9).

СибГАУ, Красноярск
E-mail: alexakulch@rambler.ru, alex_kuznetsov80@mail.ru

Критические группы, изоспектральные группе $U_3(3)$

Ю. В. Лыткин

Множество порядков элементов конечной группы G называется её *спектром* и обозначается $\omega(G)$. Под *секцией* группы G понимаем произвольную факторгруппу H/N, где $N, H \leq G$ и $N \trianglelefteq H$. Группы G и H называются *изоспектральными*, если $\omega(G) = \omega(H)$. Зафиксируем некоторый набор натуральных чисел ω. Следуя [**1**], назовём группу G *критической* относительно ω, если ω совпадает со спектром G и отлична от спектра любой её собственной секции.

Одна из важных задач для неабелевых простых групп состоит в исследовании изоспектральных им критических групп. В работах [**2, 3**] дано полное описание критических групп со спектром как у знакопеременной или спорадической группы, а также как у специальной линейной группы $SL_3(3)$.

В работе изучаются группы, критические относительно спектра проективной специальной унитарной группы $U_3(3)$. В частности, доказывается следующая

Теорема. *Пусть G — конечная группа, изоспектральная $U_3(3)$, содержащая нормальную подгруппу N, для которой $G/N \simeq PGL_2(7)$. Тогда N — 2-группа и любой её G-главный фактор изоморфен 6-мерному модулю группы $PGL_2(7)$. Далее, $G = NH$, где $H \simeq PGL_2(7)$. Если при этом группа G критическая относительно $\omega(U_3(3))$, то $|N| = 2^6$.*

Более того, H имеет представление $\langle a, b, c \mid a^2 = b^3 = c^2 = (ab)^7 = (ac)^2 = (bc)^2 = [a, b]^4 = 1\rangle$, и если рассмотреть N как векторное пространство над полем $GF(2)$, то можно выбрать базис в N такой, что действие H на N определяется следующими матрицами:

$$a \sim \begin{pmatrix} 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & 1 \end{pmatrix}, \; b \sim \begin{pmatrix} \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot \end{pmatrix}, \; c \sim \begin{pmatrix} \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & & \cdot & 1 & \cdot & \cdot & \cdot \end{pmatrix}.$$

Работа выполнена при финансовой поддержке РФФИ (проекты № 13-01-00505 и № 14-01-90013).

Список литературы

[1] *Мазуров В. Д., Ши В. Дж.* Признак нераспознаваемости конечной группы по спектру // Алгебра и логика, 51, №2 (2012), 239–243.

[2] *Lytkin Y. V.* On groups critical with respect to a set of natural numbers // SEMR, 10 (2013), 666–675; http://semr.math.nsc.ru/.

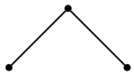
[3] *Лыткин Ю. В.* Группы, критические относительно спектров знакопеременных и спорадических групп // Сибирский математический журнал, 56, №1 (2015), 122–128.

Новосибирский государственный университет, Новосибирск
E-mail: jurasicus@gmail.com

О слабой нетеровости систем уравнений в нижних полурешетках

М. В. Малов

Понятие нетеровости по уравнениям является одним из основных в универсальной алгебраической геометрии. Одно из обобщений этого свойства – слабая нетеровость – изучалось в статьях А.Н. Шевлякова [**1**], Ю.С. Дворжецкого [**2**]. В данной работе изучается слабая нетеровость систем уравнений в классе нижних полурешеток, не содержащих следующей подполурешетки:



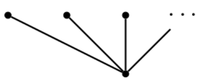
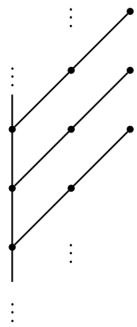
Найдены необходимые и достаточные условия слабой нетеровости систем от одной переменной над полурешетками из данного класса. Основные определения приведены в серии статей Э.Ю. Данияровой, А.Г. Мясникова, В.Н. Ремесленникова по универсальной алгебраической геометрии [**3, 4, 5**].

Сформулируем основное определение работы.

Определение. Система уравнений $\mathcal{S}$ называется *слабо нетеровой* над полурешеткой $\mathbf{M}$, если существует эквивалентная конечная система $\mathcal{S}^{'}$, множество решений которой совпадает с множеством решений системы $\mathcal{S}$.

В рассматриваемом классе полурешеток справедлива следующая теорема.

Теорема. *Пусть любые два элемента полурешетки* $x,\ y \in \mathbf{M}$ *соединены конечной цепью. Любая система от одной переменной над полурешеткой* $\mathbf{M}$ *будет слабо нетеровой тогда и только тогда, когда она не содержит подполурешеток, которые могут быть графически представлены в следующих видах:*

(a)  (b) 

Список литературы

[1] *Шевляков А. Н.* Алгебраическая геометрия над коммутативными полугруппами, автореферат канд. диссертации.

[2] *Дворжецкий Ю. С.* Системы уравнений над алгебраическими системами с порядком, автореферат канд. диссертации.

[3] *Даниярова Э. Ю., Мясников А. Г., Ремесленников В. Н.* Алгебраическая геометрия над алгебраическими системами. II. Основания // Фундамент. и прикл. мат. – 2011/2012. – Т. 17, вып. 1. – С. 65–106.

[4] *Daniyarova E., Miasnikov A., Remeslennikov V.* Algebraic geometry over algebraic structures. III. Equationally Noetherian property and compactness // Southeast Asian Bull. Math. – 2011. – Vol. 35. – P. 35–68.

[5] *Daniyarova E., Miasnikov A., Remeslennikov V.* Unification theorems in algebraic geometry // Algebra Discrete Math. – 2008. – Vol. 1. – P. 80–112.

ОФ ИМ СО РАН, г. Омск
E-mail: m.malov.v@gmail.com

Блочные графы расширений симметричных 2-схем

А. А. Махнев

Система инцидентности $(X, \mathbf{B})$ с множеством точек X и множеством блоков $\mathbf{B}$ называется t-(V, K, Λ) *схемой*, если $|X| = V$, каждый блок содержит ровно K точнек и любые t точек лежат ровно в Λ блоках. Любая 2-схема является (V, B, R, K, Λ) схемой, где B — число блоков, каждая точка инцидентна R блокам, и имеют место равенства $VR = BK$, $(V-1)\Lambda = R(K-1)$. Схема называется симметричной, если $B = V$. Схема называется квазисимметричной, если для любых двух блоков $B, C \in \mathbf{B}$ имеем $|B \cap C| \in \{x, y\}$. Числа x, y называются числами пересечений квазисимметричной схемы, и предполагается, что $x < y$.

Блочный граф квазисимметричной схемы $(X, \mathbf{B})$ в качестве вершин имеет блоки схемы и два блока $B, C \in \mathbf{B}$ смежны, если $|B \cap C| = y$.

Производной схемой для t-(V, K, Λ) схемы $\mathbf{D} = (X, \mathbf{B})$ в точке $x \in X$ называется схема $\mathbf{D}_x$ с множеством точек $X_x = X - \{x\}$ и множеством блоков $\mathbf{B}_x = \{B - \{x\} \mid x \in B \in \mathbf{B}\}$. Схема $\mathbf{E}$ называется расширением схемы $\mathbf{D}$ если производная схемы $\mathbf{E}$ в каждой точке изоморфна $\mathbf{D}$. Хорошо известно, что проективная плоскость расширяема, только если ее порядок равен 2 или 4. Трехкратное расширение проективной плоскости порядка 4 дает 5-(24,8,1) схему Витта.

Пусть 3-(V, K, Λ) схема $\mathbf{E} = (X, \mathbf{B})$ является расширением симметричной 2-схемы. По теореме Камерона (теорема 1.35 из [**1**]) либо $\mathbf{E}$ является адамаровой 3-$(4\Lambda+4, 2\Lambda+2, \Lambda)$ схемой, либо $V = (\Lambda+1)(\Lambda^2+5\Lambda+5)$ и $K = (\Lambda+1)(\Lambda+2)$, либо $V = 496$, $K = 40$ и $\Lambda = 3$. Существование 3-(496,40,3) схемы неизвестно. Дополнительный граф к блочному графу 3-(496,40,3) схемы сильно регулярен с параметрами (1197,156,15,21). Такой граф назовем монстром Камерона.

Теорема. *Для монстра Камерона Γ выполняются следующие утверждения:*

(1) *окрестность любой вершины в графе Γ — сильно регулярный граф с параметрами $(1197, 156, 15, 21)$ и спектром $156^1, 9^{741}, -15^{455}$, причем порядок коклики в этом графе не больше 105;*

(2) *множество блоков C_x, содержащих точку x схемы $\mathbf{E}$, является 495-кокликой графа Γ, для которой достигается равенство в границах Хофмана и Цветковича;*

(3) *подграф $\Gamma - C_x$ сильно регулярен с параметрами $(5643, 1092, 141, 228)$ и спектром $1092^1, 9^{5148}, -96^{494}$;*

(4) *для различных точек x, y схемы $\mathbf{E}$ имеем $|C_x \cap C_y| = 39$, причем для коклики $C_x - C_y$ графа $\Gamma - C_y$ достигается равенство в границе Хофмана.*

Список литературы

[1] *Cameron P., Van Lint J.* Designs, Graphs, Codes and their Links. London Math. Soc. Student Texts, N 22, Cambridge: Cambr. Univ. Press, 1981, 240 p.

Институт математики и механики им. Н. Н. Красовского УрО РАН, Уральский федеральный университет, Екатеринбург
E-mail: makhnev@imm.uran.ru

Кофакторы субнормальных подгрупп и инварианты конечной разрешимой группы

В. С. Монахов, И. Л. Сохор

Рассматриваются только конечные группы. Запись $H \lhd \lhd G$ означает, что H — субнормальная подгруппа группы G, $|G : H|$ — индекс подгруппы H в группе G, $|G|$ — порядок группы G, $\pi(G)$ — множество всех простых делителей $|G|$. Кроме того, $\Phi(G)$ — подгруппа Фраттини, $r_p(G)$ — p-ранг, $r(G)$ — ранг, $l_p(G)$ — p-длина, $n(G)$ — нильпотентная длина, $d(G)$ — производная длина разрешимой группы G, а $\rho(n)$ — максимум производных длин вполне приводимых разрешимых подгрупп полной линейной группы $\mathrm{GL}(n,p)$.

С каждой подгруппой H группы G связаны две нормальные в G подгруппы — нормальная оболочка H^G и ядро H_G. Нормальная оболочка H^G является наименьшей нормальной в G подгруппой, содержащей H, а ядро H_G — наибольшей нормальной в G подгруппой, содержащейся в H. Фактор-группа H/H_G называется кофактором подгруппы H.

В работе [**1**] исследовались инварианты (нильпотентная и производная длина, p-длина и ранг) разрешимой группы G в зависимости от значений числовой функции $t(G)$, которая определялась следующим образом:

$$t_p(G) = \max_{H \lhd \lhd G} \{j \mid p^j \top |H^G : H|\}, \ t(G) = max_{p\in\pi(G)} t_p(G).$$

Запись $p^m \top |H^G : H|$ означает, что p^m делит $|H^G : H|$, а p^{m+1} не делит $|H^G : H|$.

Естественно возникает задача изучения инвариантов конечных разрешимых групп в зависимости от канонических разложений $|H : H_G|$.

Введем следующие функции на множестве всех разрешимых групп:

$$u_p(G) = \max_{H \lhd \lhd G} \{j \mid p^j \top |H : H_G|\}, \ u(G) = \max_{p\in\pi(G)} u_p(G).$$

Доказана следующая теорема.

Теорема. *Пусть G — разрешимая группа. Тогда справедливы следующие утверждения:*

1) $r_p(G) \le 1 + u_p(G)$ *и* $r(G) \le 1 + u(G)$;
2) $l_p(G) \le 1 + u_p(G)$;
3) $n(G) \le d(G/\Phi(G)) \le 1 + \rho(1 + u(G)) \le 4 + u(G)$.

Список литературы

[1] *Guo W., Hu B., Monakhov V. S.* On indices of subnormal subgroups // Comm. Algebra. 2004. Vol. 33. P. 855–863.

Гомельский государственный университет им. Ф. Скорины, Гомель, Беларусь
E-mail: victor.monakhov@gmail.com, irina.sokhor@gmail.com

Взаимно перестановочные произведения расширенно c-сверхразрешимых конечных групп

Е. Н. Мысловец

Рассматриваются только конечные группы. В 1988 году В.А. Ведерниковым [**1**] было введено понятие c-сверхразрешимой группы. Группа называется c-сверхразрешимой, если она обладает главным рядом, факторы которого изоморфны простым группам. В работе [**2**] было предложено еще одно обобщение сверхразрешимости групп. Группа G называется расширенно сверхразрешимой [**2**], если любая силовская подгруппа группы G является $\mathbb{P}$-субнормальной в G.

В [**3**] введено понятие расширенно c-сверхразрешимой группы, обобщающее одновременно понятия c-сверхразрешимой и расширенно сверхразрешимой групп.

Определение Будем говорить, что группа G является расширенно c-сверхразрешимой группой, если ее каждый неабелевый главный фактор изоморфен простой группе, а для каждого абелевого главного фактора H/K группа $H/K \rtimes G/C_G(H/K)$ является расширенно сверхразрешимой.

Согласно [**4**], группа $G = HK$ называется произведением взаимно перестановочных подгрупп H и K, если H перестановочна с любой подгруппой из K, а K перестановочна с любой подгруппой из H. Через $\mathcal{K}_G$ ($\mathcal{K}_G^a$) обозначим [**4**] множество всех (абелевых) композиционных факторов группы G с точностью до изоморфизма.

Теорема. *Справедливы следующие утверждения:*

1) пусть группа $G = HK$, где H и K — взаимно перестановочные расширенно c-сверхразрешимые подгруппы, причем $\mathcal{K}_G^a \backslash \mathcal{K}_H^a \cap \mathcal{K}_G^a \backslash \mathcal{K}_K^a = \emptyset$. Тогда G — расширенно c-сверхразрешимая группа.

2) пусть группа $G = HK$, где H и K — взаимно перестановочные подгруппы, причем H — квазинильпотентная, а K — расширенно c-сверхразрешимая подгруппы группы G. Тогда G — расширенно c-сверхразрешимая группа.

Следствие. *Пусть $G = HK$, где H и K — взаимно перестановочные расширенно c-сверхразрешимые подгруппы, причем $(|G : H|, |G : K|) = 1$. Тогда G — расширенно c-сверхразрешимая группа.*

Список литературы

[1] *Ведерников В. А.* О некоторых классах конечных групп // Докл. АН БССР. 1988. Т. 2, N10. С. 872–875.

[2] *Васильев А. Ф., Васильева Т. И., Тютянов В. Н.* О конечных группах сверхразрешимого типа // Сибирский математический журнал. 2010. Т. 51, N6. С. 1270–1281.

[3] *Васильев А. Ф., Мысловец Е. Н.* Конечные cw-сверхразрешимые группы и произведения обобщенно нормальных подгрупп // Препринт N2. ГГУ им. Ф. Скорины. Гомель. 2014. 18 с.

[4] *Ballester-Bolinches A., Esteban-Romero R., Asaad M.* Products of Finite Groups. Berlin/New York: Walter de Gruyter, 2010. — 334 p.

Гомельский государсвтенный университет им. Ф. Скорины, Гомель
E-mail: myslovets@gmail.com

Контрпримеры к некоторым гипотезам о пронормальности холловых подгрупп

М. Н. Нестеров

Всюду через π обозначается некоторое фиксированное множество простых чисел. Подгруппа H конечной группы G называется *π-холловой*, если она является π-группой (т.е. все простые делители ее порядка лежат в π), а ее индекс не делится на числа из π. Подгруппа H называется *холловой* подгруппой, если она является π-холловой для некоторого множества π (эквивалентно, если $|H|$ и $|G : H|$ взаимно просты).

Говорят, что подгруппа H группы G *пронормальна*, если для любого элемента $g \in G$ подгруппы H и H^g сопряжены в подгруппе $\langle H, H^g \rangle$.

В «Коуровской тетради» записана следующая проблема [**1**, 18.32]: всегда ли холлова подгруппа конечной группы пронормальна в своём нормальном замыкании? Отрицательное решение проблемы даёт следующая

Теорема. *Пусть множество простых чисел π таково, что*

(1) *существует простая группа X, содержащая более одного класса сопряжённых π-холловых подгрупп;*

(2) *существует простая группа Y, содержащая π-холлову подгруппу, отличную от своего нормализатора в Y.*

Тогда в регулярном сплетении $G = X \wr Y$ существует непронормальная π-холлова подгруппа, нормальное замыкание которой совпадает с G.

Условиям теоремы удовлетворяет, например, множество $\{2, 3\}$: группа $X = L_3(2)$ содержит два класса сопряжённых $\{2, 3\}$-холловых подгрупп и группа $Y = L_2(16)$ содержит $\{2, 3\}$-холлову подгруппу, отличную от своего нормализатора в Y.

Подгруппу H группы G называют *сильно пронормальной*, если для любой подгруппы $K \leq H$ и любого элемента $g \in G$ подгруппа K^g сопряжена с некоторой подгруппой из H (но необязательно с K) с помощью элемента из $\langle H, K^g \rangle$.

Получено также отрицательное решение проблемы [**1**, 17.45(б)]: верно ли, что холловы подгруппы простых групп сильно пронормальны? А именно, показано, что $S_{10}(7)$ содержит $\{2, 3\}$-холлову подгруппу, не являющуюся сильно пронормальной. Отметим, что ранее не было известно примеров пронормальных, но не сильно пронормальных холловых подгрупп.

Работа выполнена при поддержке РНФ (проект 14-21-00065).

Список литературы

[1] Коуровская тетрадь: нерешённые вопросы теории групп. Изд. 18. Новосибирск, 2014.

Новосибирский государственный университет, Новосибирск
E-mail: mauk00@mail.ru

Разложение Леви для ковровых подгрупп группы Шевалле над полем

Я. Н. Нужин

Пусть Φ — приведенная неразложимая система корней, $E(\Phi, K)$ — группа Шевалле типа Φ над коммутативным кольцом K с единицей, порожденная корневыми подгруппами $x_r(K) = \{x_r(t) \mid t \in K\}$, $r \in \Phi$. *Ковром типа* Φ *над* K называется набор аддитивных подгрупп $\mathfrak{A} = \{\mathfrak{A}_r \mid r \in \Phi\}$ кольца K с условием

$$C_{ij,rs}\mathfrak{A}_r^i\mathfrak{A}_s^j \subseteq \mathfrak{A}_{ir+js}, \quad r, s, ir + js \in \Phi, \ i, j > 0, \tag{1}$$

где $\mathfrak{A}_r^i = \{a^i \mid a \in \mathfrak{A}_r\}$, а константы $C_{ij,rs}$ равны ± 1, ± 2 или ± 3. Включения (1) происходят из коммутаторной формулы для корневых элементов. Всякий ковер $\mathfrak{A}$ определяет *ковровую подгруппу* $E(\mathfrak{A})$, порожденную подгруппами $x_r(\mathfrak{A}_r)$, $r \in \Phi$. Ковер $\mathfrak{A}$ назовем: *неприводимым*, если все его аддитивные подгруппы ненулевые; *унипотентным*, если нулевые все его аддитивные подгруппы, индексированные отрицательными корнями относительно некоторой фундаментальной системы корней.

Теорема 1. *Ковровая подгруппа $E(\mathfrak{A})$ группы Шевалле типа Φ над полем K является полупрямым произведением подгрупп*

$$E(\mathfrak{A}^+) = \left\langle x_r(\mathfrak{A}_r) \mid r \in \Phi, \ \mathfrak{A}_r \neq 0, \ \mathfrak{A}_{-r} = 0 \right\rangle$$

и

$$E(\mathfrak{A}^\pm) = \left\langle x_r(\mathfrak{A}_r) \mid r \in \Phi, \ \mathfrak{A}_r\mathfrak{A}_{-r} \neq 0 \right\rangle$$

с ядром $E(\mathfrak{A}^+)$, причем подгруппа $E(\mathfrak{A}^+)$ определяется унипотентным ковром типа Φ, а подгруппа $E(\mathfrak{A}^\pm)$ является центральным произведением ковровых подгрупп, каждая из которых определяется неприводимым подковром типа Φ_i для некоторой неразложимой подсистемы корней Φ_i системы Φ.

Доказательство этой теоремы опирается на лемму 2 из [**1**], которая утверждает, что любой ковер типа Φ над полем является объединением унипотентного ковра и определенного числа неприводимых подковров, соответствующих неразложимым подсистемам корней системы Φ. Теорему 1 можно рассматривать как аналог разложения Леви для параболических подгрупп групп Шевалле над полем (см. [**2**, теорема 8.5.2]).

Список литературы

[1] *Левчук В. М.* О порождающих множествах корневых элементов групп Шевалле над полем // Алгебра и логика.—1983.—Т. 22, N5.—С. 504–517.

[2] *Carter R. W.* Simple groups of Lie type. — London-New York-Sydney-Toronto: John Wiley and Sons, 1972.—331 p.

Сибирский федеральный университет, Красноярск
E-mail: nuzhin2008@rambler.ru

К теории центральной сравнимости элементов группы

Л. И. Теняева, И. И. Павлюк, Ин. И. Павлюк

Для построения пары Фробениуса (G, M) (в терминологии В.П. Шункова) введено понятие центральной сравнимости элементов группы и получен ряд результатов, связанных с центральной эквивалентностью и понятием модулятора $M = M(a) = \{x/x\ _1 \equiv : a\}$ [1].

Теорема 1. *Пусть G - группа. Тогда* $(\forall a, g \in G)\,((M(a))^g = M(a^g))$.

Теорема 2. *В группе G без центра $(Z(G) = e)$ истина формула*
$(\forall g, x \in G)\,(\forall a \in G)\,((M(a))^g \neq (M(a))^x) \Leftrightarrow ((M(a))^x \cap (M(a))^g = \{e\})$.

Список литературы

[1] *Павлюк Ин. И.* Группы с отношениями сравнимости для подгрупп и элементов: монография. Павлодар: Кереку, 2013. - 121 с.

Павлодарский государственный университет, Павлодар, Казахстан
E-mail: Inessa7772@mail.ru

Убывающие инвариантные ряды подгрупп в проконечных группах

К. Н. Пономарёв

Убывающим инвариантным рядом подгрупп топологической группы G называется строго убывающая вполне упорядоченная по убыванию система замкнутых нормальных подгрупп группы G, исходящая из всей группы G, и доходящая до единичной подгруппы. Строится теория убывающих инвариантных рядов бесконечных проконечных групп. В качестве приложения установлено, что мощность бесконечной проконечной группы G выражается экспонентой ее веса: $|G| = 2^{w(G)}$.

Убывающий инвариантный ряд подгрупп бесконечной группы G называется *калиброванным рядом*, если на каждом шаге происходит сужение группы ряда до ее нормальной подгруппы конечного индекса.

Теорема 1. *Рассмотрим бесконечную проконечную группу G веса $w(G)$.*

Утверждается, что в группе G имеются калиброванные убывающие инвариантные ряды подгрупп $\mathfrak{C}$. При этом мощность любого такого ряда совпадает с весом группы,

$$p(\mathfrak{C}) = w(G).$$

Теорема 2. *Любой убывающий инвариантный ряд подгрупп бесконечной проконечной группы G уплотняется до некоторого калиброванного ряда.*

В частности, мощность любого убывающего инвариантного ряда подгрупп группы G не превосходит веса группы:

$$p(\mathfrak{R}) \leqslant w(G).$$

Теорема 3. *Мощность бесконечной проконечной группы G выражается экспонентой ее веса:*

$$|G| = 2^{w(G)}.$$

Отметим, что хотя это утверждение мало известно, оно не является новым, поскольку вытекает из общей теоремы Архангельского о мощности однородных компактных хаусдорфовых топологических пространств.

Работа выполнена при финансовой поддержке Министерства образования и науки РФ, по государственному заданию N.2014/138, проект 1052.

НГТУ, Новосибирск
E-mail: ponomaryov@ngs.ru

Об абелевых 3-группах Шура

Г. К. Рябов

Пусть G — конечная группа с единицей e, $\mathbb{Z}G$ — целочисленное групповое кольцо, $\underline{X} = \sum_{x \in X} x$. Кольцо $\mathcal{A} \subset \mathbb{Z}G$ называется S-кольцом над группой G, если существует разбиение $\mathcal{S} = \mathcal{S}(\mathcal{A})$ группы G такое, что (1) $\{e\} \in \mathcal{S}$; (2) если $X \in \mathcal{S}$, то $X^{-1} = \left\{x^{-1} | x \in G\right\} \in \mathcal{S}$; (3) $\mathcal{A} = Span_{\mathbb{Z}} \{\underline{X} : X \in \mathcal{S}\}$. Пусть Γ — группа подстановок элементов группы G, причем $G_{right} \leq \Gamma \leq Sym(G)$, где $G_{right} = \{x \mapsto xg, \ x \in G : g \in G\}$. Положим $\mathcal{A} = \mathcal{A}(\Gamma, \ G) = Span_{\mathbb{Z}} \{\underline{X} : \ X \in Orb(\Gamma_e, \ G)\}$, где Γ_e — стабилизатор точки e в группе Γ. Тогда $\mathbb{Z}$-модуль $\mathcal{A}$ является S-кольцом над группой G. S-кольцо $\mathcal{A}$ над группой G называется *шуровым*, если $\mathcal{A} = \mathcal{A}(\Gamma, \ G)$ для некоторой группы подстановок Γ. Конечная группа G называется *шуровой*, если каждое S-кольцо над ней шурово.

Недавно в [1] были получены сильные необходмые условия шуровости абелевых групп. Из них следует, что только группы $\mathbb{Z}_3 \times \mathbb{Z}_{3^n}$ при $n \geq 1$ могут быть нециклическими абелевыми шуровыми 3-группами, отличными от группы $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$. В работе доказана следующая

Теорема 1. *Группы $\mathbb{Z}_3 \times \mathbb{Z}_{3^n}$ при $n \geq 1$ шуровы.*

Этот результат завершает классификацию шуровых p-групп, где p нечетное простое. Из теоремы 1 и ранее известных результатов следует:

Теорема 2. *Пусть p — нечетное простое число. Тогда p-группа G шурова, если и только если G циклическая или $p = 3$ и G изоморфна одной из следующих групп: $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$, $\mathbb{Z}_3 \times \mathbb{Z}_{3^n}$, $n \geq 1$.*

Список литературы

[1] *Evdokimov S., Kovács I., Ponomarenko I.* On schurity of finite abelian groups, subm. to Comm. Algebra, http://arxiv.org/abs/1309.0989 [math.GR], 2013.

Новосибирский государственный университет, Новосибирск

О пересечении $\mathfrak{f}$-абнормальных максимальных подгрупп в разрешимых группах

М. В. Селькин, Р. В. Бородич

В теории конечных групп хорошо известна классическая работа Г.Фраттини [1], получившая свое развитие в различных направлениях. В работе [2] В.Гашюцем исследовались пересечения абнормальных максимальных подгрупп. В.Дескинсом [3] исследовались пересечения максимальных подгрупп с ограничениями на индексы. Развитие в 60-х годах теории формаций, позволило систематизировать накопившийся богатый фактический материал о максимальных подгруппах. Этому способствовало введённое в работах Р.Картера, Т.Хоукса [4] и Л.А.Шеметкова [5] понятие $\mathfrak{F}$-абнормальной максимальной подгруппы.

Теорема. *Пусть $\mathfrak{F}$ — локальная формация Фиттинга, содержащая все нильпотентные группы. Если в разрешимой группе G существуют $\mathfrak{F}$-абнормальные максимальные подгруппы, не принадлежащие формации $\mathfrak{F}$ и не содержащие $\mathfrak{F}$-радикал, то пересечение всех таких подгрупп принадлежит $\mathfrak{F}$.*

Если $\mathfrak{F}$ — формация всех нильпотентных групп, то из теоремы получаем

Следствие. *Пусть G — разрешимая группа. Если в группе G существуют ненильпотентные абнормальные максимальные подгруппы, не содержащие $F(G)$, то пересечение всех таких подгрупп нильпотентно.*

Список литературы

[1] *Frattini G.* Intorno alla generasione dei gruppi di operazioni // Atti Acad. Dei Lincei 1885. Vol.1. P.281-285.

[2] *Gaschütz W.* Über die Φ-Untergruppen endlicher Gruppen // Math. Z. — 1953. — Bd. 58. — S. 160–170.

[3] *Deskins W.E.* A condition for the solvability of a finite group // III.J.Math. — 1961. — Vol. 5. — № 2, P. 306–313.

[4] *Carter R., Hawkes T.* The $\mathfrak{F}$-normalizers of a finite soluble group // J.Algebra. — 1967. — V. 5, № 2 — P. 175–202.

[5] *Шеметков Л.А.* Ступенчатые формации групп // Матем. сб. — 1974. — Т.94, № 4. — С. 628–648.

Учреждение образования "Гомельский государственный университет имени Ф.Скорины", Гомель
E-mail: Borodich@gsu.by

О точно трижды транзитивных группах и полях Керби-Титса

А. И. Созутов

Группа G перестановок множества F ($|F| \geq k$) называется *точно k-транзити-в-ной* на F, если для любых двух упорядоченных множеств $(\alpha_1, ..., \alpha_k)$ и $(\beta_1, ..., \beta_k)$ элементов из F таких, что $\alpha_i \neq \alpha_j$ и $\beta_i \neq \beta_j$ для $i \neq j$, существует точно один элемент группы G переводящий α_i в β_i ($i = 1, ..., k$). Согласно известным результатам К. Жордана, Ж. Титса и М. Холла (см., например, [**1**][стр. 215]) при $k \geq 4$ точно k-транзитивны только симметрические группы S_k, S_{k+1} и знакопеременная группа A_{k+2}, а также группы Матье M_{11} ($k = 4$) и M_{12} ($k = 5$). Конечные точно 3-транзитивные группы классифицировал Г. Цассенхауз [**2**], а локально конечные — О. Кегель [**3**]. В [**4**][теорема 2] доказано, что точно трижды транзитивная группа перестановок с периодическим стабилизатором двух точек локально конечна. Стабилизатор G_α точки α в точно $(k+1)$-транзитивной группе G перестановок множества X действует на множестве $F = X \setminus \{\alpha\}$ точно k-транзитивно. Это намечает индуктивный переход, но действующий скорее в обратном направлении, поскольку условие k-транзитивности существенно слабее условия $(k+1)$-транзитивности. Не каждая точно 2-транзитивная группа T вложима в 3-транзитивную группу G в качестве стабилизатора точки. Но если такое вложение есть, то для изучения T появляется дополнительный ресурс в виде внешнего инволютивного автоморфизма.

В нашем докладе речь пойдет о точно 3-транзитивных группах и связанных с ними KT-полях [**1**, гл. V] при дополнительных условиях существования в исследуемой группе G конечной, совершенной или почти совершенной инволюции.

Инволюция j бесконечной группы G называется *конечной в* G, если $|jj^g| < \infty$ для каждого элемента $g \in G$; *совершенной в* G, если любые две неперестановочных инволюции из j^G сопряжены при помощи инволюции из этого же класса; и *почти совершенной в* G, если любые две инволюции из j^G, порядок произведения которых бесконечен, сопряжены при помощи инволюции из j^G [**5**][стр. 15].

Работа поддержана РФФИ (грант 15-01-04897 А).

Список литературы

[1] *Wähling H.* Theorie der Fastkörper.– Essen: Thalen Ferlag.– 1987.

[2] *Zassenhaus H.* Uber endliche Fastkorper // Hamb. Abh.– 1936.– B. 11.– S. 187-220.

[3] *Kegel O. H.* Zur Structur lokal endlicher Zassenhausgruppen.– Arch. Math.– 18 (1967).– S. 337-348.

[4] *Созутов А. И., Дураков Е. Б.* О локальной конечности периодических точно трижды транзитивных групп // Алгебра и логика (в печати).

[5] *Созутов А. И., Сучков Н. М., Сучкова Н. Г.* Бесконечные группы с инволюциями.– Красноярск, Сибирский федеральный университет, 2011. 149 с.

Сибирский федеральный университет, Красноярск
E-mail: sozutov_ai@mail.ru

О группах с фробениусовыми элементами

А. И. Созутов, А. М. Попов

Элемент a группы G называется *H-фробениусовым*, если H — собственная подгруппа в G и все подгруппы вида $L_g = \langle a, a^g \rangle$, где $g \in G \setminus H$, являются группами Фробениуса с дополнениями, содержащими элемент a. При этом группа L называется *группой Фробениуса с дополнением* T *и ядром* F, если F и T — собственные подгруппы в L, $T \cap T^x = 1$ для $x \in L \setminus T$, $L = F \leftthreetimes T$ и каждый элемент из L содержится либо в F, либо в некоторой подгруппе T^x (см. вопрос 6.53 из [**1**]). Неединичный элемент b группы G называется *конечным в* G, если для любого $g \in G$ подгруппа $\langle b, b^g \rangle$ конечна.

Допустим в G есть H-фробениусовый элемент a порядка > 2. Будет ли в этом случае объединение всех ядер фробениусовых подгрупп группы G с дополнением $\langle a \rangle$ подгруппой? Особенно интересен случай, когда элемент a с любым своим сопряженным порождают конечную подгруппу (вопрос 10.61 из Коуровской тетради [**1**]).

Положительный ответ на вторую часть данного вопроса при $|a| \notin \{3, 5\}$ был получен в [**2**]. Для случая $|a| = 2n > 2$ вопрос 10.61 решен полностью в [**3**]. В [**4**] исследован случай $|a| = 3n > 3$. При этом в [**2**] существенно использовалась конечность подгрупп L_g, в [**3**] — абелевость групп с расщепляющим автоморфизмом порядка 2, а в [**4**] — нильпотентность ядер фробениусовых подгрупп L_g.

Теорема. *Пусть a — H-фробениусовый элемент группы G и ядра всех фробениусовых подгрупп $L_g = \langle a, a^g \rangle$ при $g \in G \setminus H$ нильпотентны. Если $|a| > 5$ и подгруппа $\langle a \rangle$ содержит конечный в H элемент b, то объединение F всех ядер фробениусовых подгрупп группы G с дополнением $\langle a \rangle$ является периодической нормальной подгруппой группы G и $G = FH$.*

Работа поддержана РФФИ (грант 15-01-04897 А).

Список литературы

[1] Коуровская тетрадь: Нерешенные вопросы теории групп – 13-е изд.– Новосибирск, 1995 г.

[2] *Попов А. М.* О строении группы с конечным H-фробениусовым элементом.– Алгебра и логика.– Т. 43 (2004), N2.– С. 220-228.

[3] *Попов А. М., Созутов А. И.* О группе с H-фробениусовым элементом четного порядка.– Алгебра и логика.– Т. 44 (2005) N1.– С. 70–80.

[4] *Попов А. М., Созутов А. И.* О группах с фробениусовыми элементами // Сибирский математический журнал (в печати).

СФУ, Красноярск, СибГАУ, Красноярск
E-mail: sozutov_ai@mail.ru, vm_popov@sibsau.ru

К вопросу об аппроксимируемости корневыми классами HNN-расширений с центральными связанными подгруппами

Е. В. Соколов

Согласно [**1**] содержащий хотя бы одну неединичную группу класс групп $\mathcal{C}$ называется корневым, если он замкнут относительно взятия подгрупп и прямых произведений конечного числа сомножителей, а также удовлетворяет следующему условию: если X — некоторая группа и $1 \leqslant Z \leqslant Y \leqslant X$ — субнормальный ряд группы X такой, что X/Y, $Y/Z \in \mathcal{C}$, то в группе X существует нормальная подгруппа T такая, что $T \subseteq Z$ и $X/T \in \mathcal{C}$. Можно показать, что корневыми являются те и только те наследственные классы групп, которые замкнуты относительно декартовых сплетений [**2**].

Д. В. Гольцовым [**3**] установлено, что если $\mathcal{C}$ — замкнутый относительно факторизации корневой класс групп и $B \in \mathcal{C}$, то произвольное HNN-расширение группы B с тривиально пересекающимися центральными связанными подгруппами аппроксимируется классом $\mathcal{C}$. Частичным обобщением этого результата является приводимое далее утверждение, в котором отсутствует требование тривиальности пересечения связанных подгрупп.

Теорема. *Пусть $\mathcal{C}$ — замкнутый относительно факторизации корневой класс групп, содержащий хотя бы одну непериодическую группу. Пусть также G — HNN-расширение некоторой группы B со связанными подгруппами H и K, лежащими в центре B. Тогда следующие утверждения равносильны и при выполнении любого из них группа G аппроксимируется классом $\mathcal{C}$.*

1. *Существует гомоморфизм группы B на группу из класса $\mathcal{C}$, инъективный на подгруппах H и K.*
2. *Существует гомоморфизм группы G на группу из класса $\mathcal{C}$, инъективный на подгруппах H и K.*

В частности, если $B \in \mathcal{C}$, то группа G $\mathcal{C}$-аппроксимируема.

Список литературы

[1] *Gruenberg K. W.* Residual properties of infinite soluble groups // Proc. Lond. Math. Soc. 1957. V. 7. P. 29–62.

[2] *Sokolov E. V.* A characterization of root classes of groups // Comm. Algebra. 2015. V. 43, № 2. P. 856–860.

[3] *Гольцов Д. В.* Аппроксимируемость HNN-расширения с центральными связанными подгруппами корневым классом групп // Матем. заметки. 2015. Т. 97, вып. 5. С. 665–669.

Ивановский государственный университет, г. Иваново
E-mail: ev-sokolov@yandex.ru

О рангах планарности многообразий коммутативных полугрупп

Д. В. Соломатин

Настоящая работа посвящена изучению свойства планарности графов Кэли полугрупп для многообразий коммутативных полугрупп. А именно, исследуется предложенное Л. М. Мартыновым понятие ранга планарности многообразия полугрупп. Напомним соответствующее определение. Пусть $\boldsymbol{V}$— произвольное многообразие полугрупп. Если существует такое натуральное число r, что все $\boldsymbol{V}$-свободные полугруппы ранга $\leq r$ допускают планарный граф Кэли, а $\boldsymbol{V}$-свободная полугруппа ранга $r+1$ уже не допускает планарный граф Кэли, то *рангом планарности* $\boldsymbol{V}$ называется это число r. Если для многообразия $\boldsymbol{V}$ такого натурального числа не существует, то говорят, что многообразие $\boldsymbol{V}$ имеет бесконечный ранг планарности. Ранее автором в [**1**] найдены ранги многообразий коммутативных моноидов и дана классификация этих многообразий по рангам планарности.

Здесь мы приводим достижимую оценку рангов планарности многообразий коммутативных комбинаторных полугрупп, т. е. многообразий, не содержащих неединичных групп. Доказана следующая

Теорема. *Нетривиальное многообразие комбинаторных коммутативных полугрупп либо имеет бесконечный ранг планарности и при этом совпадает с многообразием полугрупп с нулевым умножением, либо имеет ранг планарности* ≤ 3.

Доказательство этого утверждения опирается на следующее, представляющее самостоятельный интерес и довольно общее утверждение.

Предложение. *Если многообразие коммутативных полугрупп определяется системой тождеств, все слова входящие в запись которых имеют длину более 2, то ранг планарности этого многообразия не превышает 3.*

Список литературы

[1] *Соломатин Д. В.* Ранги планарности многообразий коммутативных моноидов // Вестник Омского университета. Изд-во: Омский государственный университет им. Ф.М. Достоевского (Омск). — 2012. — Т.4 (66). — С. 41–45.

Омский государственный педагогический университет, Омск
E-mail: denis_2001j@bk.ru

Большие абелевы подалгебры алгебр Шевалле и большие абелевы подгруппы конечных групп лиева типа

Г. С. Сулейманова

Алгебру Шевалле $L_\Phi(K)$ над полем K, ассоциированную с системой корней Φ, характеризуют базой Шевалле, состоящей из элементов e_r $(r \in \Phi)$ вместе с подходящей базой подалгебры Картана [**1**, § 4.4]. Элементы e_r $(r \in \Phi^+)$ образуют базу максимальной нильпотентной подалгебры $N\Phi(K)$. В [**2**] записана следующая задача, исследованная при $K = C$ в [**3**]: *Описать абелевы подалгебры наивысшей размерности в алгебре $N\Phi(K)$ над произвольным полем K.*

В конечной группе подгруппу наибольшего порядка со свойством $\mathbb{P}$ называют *большой $\mathbb{P}$-подгруппой.* Проблема описания больших абелевых подгрупп унипотентного радикала U подгруппы Бореля конечной группы G лиева типа (см. обзор [**4**, Проблема (1.6)]) завершена в 2013 году [**5**]; из найденного решения вытекает теорема 1 ниже. Подалгебру наивысшей размерности со свойством $\mathbb{P}$ в произвольной алгебре далее называем также *большой $\mathbb{P}$-подалгеброй.* Большие нормальные абелевы подгруппы в U описаны в [**6**].

Теорема 1. *Каждая большая абелева подгруппа в U либо переводится автоморфизмом группы G в большую нормальную абелеву подгруппу в U, либо G типа G_2 и $charK \neq 3$, или типа F_4 и $2K = 0$, или типов ${}^3D_4$, ${}^2F_4$ или ${}^2E_6$.*

Автором и В.М. Левчуком, наряду с описанием максимальных абелевых идеалов алгебры $N\Phi(K)$, получено описание больших абелевых идеалов алгебры $N\Phi(K)$ и доказана

Теорема 2. *В алгебре Шевалле $L_\Phi(K)$ классического типа над полем каждая большая абелева подалгебра подалгебры $N\Phi(K)$ переводится автоморфизмом алгебры $L_\Phi(K)$ в идеал подалгебры $N\Phi(K)$.*

Список литературы

[1] *Carter R.* Simple groups of Lie type, Wiley and Sons, New York, 1972.

[2] *Levchuk V. M., Suleimanova G. S.* The generalized Mal'cev problem on abelian subalgebras of the Chevalley algebras // Lobachevskii Journal of Mathematics, №4(2015).

[3] *Мальцев А. И.* Коммутативные подалгебры полупростых алгебр Ли // Известия АН СССР, сер. матем., т. 9 (1945), № 4, с. 291-300.

[4] *Кондратьев А. С.* Подгруппы конечных групп Шевалле // Успехи математических наук, т. 41 (1986), № 1 (247), с. 57-96.

[5] *Сулейманова Г. С.* Большие элементарные абелевы унипотентные подгруппы групп лиева типа // Известия Иркутского государственного университета. Серия "Математика", т. 6 (2013), № 2, с. 69-76.

[6] *Levchuk V. M., Suleimanova G. S.* Extremal and maximal normal abelian subgroups of a maximal unipotent subgroup in groups of Lie type // J. Algebra, vol. 349 (2012), iss. 1, no.1, p. 98-116.

Хакасский технический институт – филиал СФУ, Абакан
E-mail: suleymanova@list.ru

О нормальных подгруппах групп ограниченных подстановок

Н. М. Сучков, Н. Г. Сучкова

Пусть N, Z — множества всех натуральных и целых чисел соответственно; M — любое из этих множеств; $S(M)$ — группа всех подстановок множества M. Подстановка $g \in S(M)$ называется ограниченной, если

$$w(g) = \max_{\alpha \in M} |\alpha - \alpha^g| < \infty.$$

Очевидно, что множество

$$\mathrm{Lim}(M) = \{x | x \in S(M), w(x) < \infty\}$$

является группой. В работе [**1**] был построен пример смешанной группы $H = AB$, где A, B — локально конечные подгруппы. Затем в [**2**] установлено, что $H = \langle g | g \in \mathrm{Lim}(Z), |g| < \infty \rangle$. При этом $\mathrm{Lim}(Z) = H \leftthreetimes \langle d \rangle$, где $\alpha^d = \alpha + 1$ при всех $\alpha \in Z$. Факторизация смешанной группы $\mathrm{Lim}(N)$ двумя локально конечными подгруппами доказана в [**3**]. Там же доказано, что $\mathrm{Lim}(M) = \langle x | x \in S(M), w(x) = 1 \rangle$.

Продолжено изучение групп ограниченных подстановок.

Теорема 1. *Коммутантом группы* $\mathrm{Lim}(Z)$ *является группа* H. *Группа* $\mathrm{Lim}(N)$ *совпадает со своим коммутантом.*

Найден метод построения локально конечных нормальных подгрупп группы $\mathrm{Lim}(N)$. Пусть

$$L = \{\mu_1, \mu_2, \dots, \mu_n, \dots\} \text{ —}$$

бесконечное подмножество множества N, где $\mu_1 < \mu_2 < \dots < \mu_n < \dots$; $m \in N$. Элементы μ_i и μ_j будем называть m-эквивалентными, если либо $i = j$, либо $i < j$ ($j < i$) и $\mu_{k+1} - \mu_k \le m$; $i \le k \le j - 1$ ($j \le k \le i - 1$). Обозначим через $B_m(L)$ множество всех классов m-эквивалентности элементов L.

Определение. *Множество L назовем m-рассеянным, если все классы множества $B_m(L)$ конечны и вполне m-рассеянным, если порядки этих классов не превосходят некоторого числа $c(m)$. Множество L будем называть (вполне) рассеянным, если оно (вполне) m-рассеянное при каждом натуральном m.*

Пусть для элементов множества L выполняются неравенства $\mu_n + 1 < \mu_{n+1}$ ($n = 1, 2, \dots$) и

$$a = (\mu_1\ \mu_1 + 1)(\mu_2\ \mu_2 + 1) \dots (\mu_n\ \mu_n + 1) \dots .$$

Теорема 2. *Нормальное замыкание инволюции a в группе* $\mathrm{Lim}(N)$ *тогда и только тогда локально конечно, когда L — вполне рассеянное множество.*

Список литературы

[1] *Сучков Н. М.* Пример смешанной группы, факторизуемой двумя периодическими подгруппами, Алгебра и логика, 23:5 (1984), 573–577.

[2] *Сучков Н. М.* О подгруппах произведения локально конечных групп, Алгебра и логика, 24:4 (1985), 408–413.

[3] *Сучков Н. М., Сучкова Н. Г.* О группах ограниченных подстановок, Журнал СФУ, Математика и физика, 3:2 (2010), 262–266.

СФУ, Красноярск
E-mail: ns7654321@mail.ru

О порожденных инволюциями бесконечных подгруппах похожих на группы Голода групп

А. В. Тимофеенко

Выяснено, что построенные в 1980-е годы, [**1, 2**], конечно порожденные бесконечные подгруппы бесконечного индекса некоторых 2-групп Голода с бесконечным центром могут порождаться инволюциями.

Теорема. *Для каждого $r \geq 2$ и каждого $d > r$ можно построить финитно аппроксимируемую r-порождённую 2-группу с бесконечным центром, у которой конечны все $(r-1)$-порожденные подгруппы, а некоторая бесконечная подгруппа порождена d инволюциями и содержится в нормальной подгруппе бесконечного индекса .*

Список литературы

[1] *Тимофеенко А. В.* Бесконечные подгруппы бесконечного индекса в 2-порождённых p-группах типа Голода, Сиб. матем. ж., 27:5 (1986), 194-195.

[2] *Тимофеенко А. В.* О существовании групп Голода с бесконечным центром, Матем. заметки, 39:5 (1986), 647-650.

Красноярский госпедуниверситет им. В. П. Астафьева, Красноярск
E-mail: A.V.Timofeenko62@mail.ru

Свободные полинильпотентные группы с неразрешимыми универсальными теориями

Е. И. Тимошенко

Доказано, что свободная группа ранга ≥ 2 любого полинильпотентного многообразия $\mathfrak{N}_{c_1}\mathfrak{N}_{c_2}\dots\mathfrak{N}_{c_s}$, $s \geq 2$, $c_i \geq 1$, $c_s \geq 2$ имеет неразрешимую универсальную теорию.

Работа выполнена при финансовой поддержке РФФИ, проект 15-01-01485 и при поддержке Министерства образования и науки Российской Федерации соглашение №14.B37.21.0359.

Новосибирский государственный технический университет, Новосибирск
E-mail: eitim45@gmail.com

Разрешимые группы с ограничениями на силовские подгруппы подгруппы Фиттинга

А. А. Трофимук

Все обозначения и используемые определения соответствуют [**1**].

В. С. Монахов [**2**] ввел понятие нормального ранга $r_n(P)$ как наименьшее натуральное число k такое, что любая нормальная подгруппа p-группы P порождается не более, чем k элементами. Кроме того в этой работе было доказано, что нильпотентная длина разрешимой группы с силовскими подгруппами P нормального ранга $r_n(P) \leq 2$ не превышает 4.

На строение разрешимой группы существенное влияние оказывает ее подгруппа Фиттинга. Так из результата Бэра [**1**, с. 720] следует сверхразрешимость разрешимой группы G, у которой существует цепочка подгрупп

$$\Phi(G) = G_0 \subset G_1 \subset \ldots \subset G_{m-1} \subset G_m = F(G)$$

такая, что G_i нормальна в G и $|G_{i+1}/G_i|$ является простым числом для всех i. В работе [**3**] замечено, что для оценки производной длины разрешимой группы достаточно рассматривать порядки силовских подгрупп только ее подгруппы Фиттинга.

Для формулировки основного результата введем следующее обозначение:

$$r_n(F) = \max_{p\in\pi(F)} r_n(F_p).$$

Здесь F — подгруппа Фиттинга группы G, F_p — силовская p-подгруппа группы F для $p \in \pi(F)$.

Теорема. *Пусть G — разрешимая группа и $r_n(F) \leq 2$. Тогда нильпотентная длина группы G не превышает 4, а производная длина группы G не превышает 6.*

Пример 1. Пусть S — экстраспециальная группа порядка 27. Вычисления в системе GAP показали, что ее группой автоморфизмов является группа $[E_{3^2}]GL(2,3)$. Полупрямое произведение $G = [S]GL(2,3)$ является группой порядка $1296 = 2^4 3^4$ с подгруппой Фиттинга $F = S$ порядка 27 и $r_n(F) = 2$. Производная длина G равна 6, а нильпотентная длина равна 4. Данный пример показывает, что оценки производной и нильпотентной длины, полученные в теореме, являются точными.

Список литературы

[1] *Huppert B.* Endliche Gruppen I / B. Huppert // Berlin, Heidelberg, New York. — 1967.

[2] *Монахов В. С.* О разрешимых конечных группах с силовскими подгруппами малого ранга / В.С.Монахов // Доклады Национальной академии наук Беларуси. — 2002. — Т. 46, № 2. — С. 25–28.

[3] *Трофимук А. А.* Производная длина конечных групп с ограничениями на силовские подгруппы / А. А. Трофимук // Математические заметки. — 2010. — Т. 87, № 2. — С. 287–293.

БрГУ им. А.С. Пушкина, Брест
E-mail: alexander.trofimuk@gmail.com

Об аппроксимируемости корневыми классами групп Баумслага-Солитера

Е. А. Туманова

Напомним, что группы с одним определяющим соотношением вида

$$BS(m,\ n) = \langle a,\ b;\ a^{-1}b^m a = b^n\rangle,$$

где без потери общности можно считать $|n| \geq m > 0$, называются группами Баумслага-Солитера. Напомним также, что содержащий хотя бы одну неединичную группу класс групп $\mathcal{K}$ называется корневым, если он замкнут относительно взятия подгрупп и прямых произведений конечного числа сомножителей, а также удовлетворяет условию Грюнберга: если X — некоторая группа и $1 \leqslant Z \leqslant Y \leqslant X$ — субнормальный ряд группы X такой, что $X/Y,\ Y/Z \in \mathcal{K}$, то в группе X существует нормальная подгруппа T такая, что $T \subseteq Z$ и $X/T \in \mathcal{K}$.

В данной работе полностью решен вопрос об аппроксимируемости групп Баумслага-Солитера замкнутыми относительно факторизации корневыми классами.

Теорема. *Пусть $\mathcal{K}$ — замкнутый относительно факторизации корневой класс групп, $\pi(\mathcal{K})$ — множество всех простых делителей конечных порядков элементов групп из класса $\mathcal{K}$.*

1. *Если класс $\mathcal{K}$ содержит хотя бы одну непериодическую группу, то группа $BS(m,\ n)$ $\mathcal{K}$-аппроксимируема.*
2. *Пусть класс $\mathcal{K}$ состоит только из периодических групп. Тогда имеют место следующие утверждения.*
   а) *Если $1 < m < |n|$, то группа $BS(m,\ n)$ не является $\mathcal{K}$-аппроксимируемой.*
   б) *Группа $BS(m,\ m)$ $\mathcal{K}$-аппроксимируема тогда и только тогда, когда m является $\pi(\mathcal{K})$-числом.*
   в) *Группа $BS(m,\ -m)$ $\mathcal{K}$-аппроксимируема тогда и только тогда, когда m является $\pi(\mathcal{K})$-числом и $2 \in \pi(\mathcal{K})$.*
   г) *Группа $BS(1,\ n)$, где $|n| \neq 1$, $\mathcal{K}$-аппроксимируема тогда и только тогда, когда существует число $p \in \pi(\mathcal{K})$, не делящее n и такое, что порядок элемента $\overline{n}$ группы $\mathbb{Z}_p^*$ является $\pi(\mathcal{K})$-числом.*

Отметим, что приведенная теорема обобщает ряд результатов об аппроксимируемости групп Баумслага-Солитера конечными π-группами.

Ивановский государственный университет;
Ивановская пожарно-спасательная академия ГПС МЧС России, г. Иваново
E-mail: helenfog@bk.ru

Конечные группы с $\mathbb{P}$-субнормальными подгруппами

В. Н. Тютянов, Т. В. Тихоненко

В работе [**1**] Л.С. Казарин определил композиционные факторы конечной группы, которая имеет цепь подгрупп с простыми индексами, начинающуюся с единичной подгруппы. Данная работа послужила источником появления целой серии публикаций по данной тематике (А.Ф. Васильев, Т.И. Васильева, В.Н. Тютянов, В.С. Монахов, В.Н. Княгина и др.), в которых исследовалось строение конечной группы с заданными системами подгрупп, обладающих цепями с простыми индексами.

В работе [**2**] было введено важное определение, которое неоднократно обобщалось в различных направлениях.

Определение. Подгруппа H группы G называется $\mathbb{P}$-субнормальной в G, если либо $H = G$, либо существует цепь подгрупп $H = H_0 \subset H_1 \subset \cdots \subset H_{n-1} \subset H_n = G$ такая, что $|H_i : H_{i-1}|$-простое число для любого $i = 1, \ldots, n$. Обозначается через H $\mathbb{P}$-sn G.

Доказан следующий результат.

Теорема. *Пусть G — конечная группа, у которой единичная подгруппа не является $\mathbb{P}$-субнормальной в G, но $\mathbb{P}$-субнормальна во всякой собственной подгруппе группы G. Тогда $G/\Phi(G) \in \{A_6; J_1; Sz(2^r)$, где r — нечетное простое число; $PSL_2(r)$, где $3 < r$ — простое число; $PSL_2(11^r)$, $PSL_2(7^r)$, $PSL_2(5^r)$, $PSL_2(3^r)$, где r — простое число; $PSL_2(2^r)$, где $3 \le r$ — простое число; $PSL_2(2^{32})$; $PSU_3(3)$; $PSU_3(7)$; $PSU_3(q)$, где $q+1$ — простое число Ферма; $PSL_3(5)$; $PSL_3(7)$; $PSL_3(11)\}$.*

Список литературы

[1] *Казарин Л. С.* О группах с факторизацией // Докл. АН СССР. 1981. Т. 256. № 1. С. 26–29.

[2] *Васильев А. Ф., Васильева Т. И., Тютянов В. Н.* О конечных группах сверхразрешимого типа // Сиб. мат. журн. 2010. Т. 51. № 6. С. 1270–1281.

Международный университет «МИТСО», Гомельский филиал, Гомель, Гомельский государственный технический университет им. П.О. Сухого, Гомель
E-mail: tyutyanov@front.ru, tihonenkotanya@rambler.ru

Элементы алгебраической геометрии над некоторыми классами вполне простых полугрупп

П. А. Уляшев

Пусть S — произвольная полугруппа, I и Λ — непустые множества индексов и P — матрица элементов из S размера $|\Lambda| \times |I|$. Матричной полугруппой Риса $\mathcal{M}(S; I; \Lambda; P)$ называется множество $I \times S \times \Lambda$ с заданной на нем операцией умножения

$$(i, s, \lambda)(j, t, \mu) = (i, sp_{\lambda j}t, \mu).$$

Согласно классической теореме Риса (см. в [**1**]) любая вполне простая полугруппа изоморфна некоторой матричной полугруппе Риса над группой.

В работе рассматриваются классы вполне простых полугрупп с ограничениями на матрицу P. При помощи методов, описанных в [**2**], получены критерии, определяющие координатные полугруппы алгебраических множеств.

Список литературы

[1] *Howie J.* Fundamentals of semigroup theory / The Clarendon Press, Oxford University Press, London Mathematical Society Monographs. NewSeries, 12 (1995), 351p.

[2] *Даниярова Э. Ю., Мясников А. Г., Ремесленников В. Н.* Алгебраическая геометрия над алгебраическими системами. II. Основания / Фундаментальная и прикладная математика, 2011/2012, том 17, № 1, С. 65–106.

ОФ ИМ СО РАН, Омск
E-mail: p.ulyashev@gmail.com

Конечные факторизуемые группы с разрешимыми $\mathrm{K}\mathbb{P}^2$-субнормальными сомножителями

И. К. Чирик

В. С. Монахов [**1**, теорема 2] без использования классификации конечных простых групп доказал разрешимость конечной группы $G = AB$, при условии, что подгруппы A и B разрешимы и $|G : A| = p$ или p^2, $|G : B| = q$ или q^2, где p и q — простые числа. Эта теорема получила развитие в работах А. Ф. Васильева, Т. И. Васильевой, В. Н. Тютянова, В. Н. Княгиной и В. С. Монахова [**2**]–[**4**].

Пусть $\mathbb{N}$ и $\mathbb{P}$ — множества всех натуральных и простых чисел соответственно. Зафиксируем $t \in \mathbb{N}$ и обозначим

$$\mathbb{P}^t = \{p^k \mid p \in \mathbb{P},\ k \leq t,\ k \in \{0\} \cup \mathbb{N}\}.$$

Подгруппа H группы G называется $\mathrm{K}\mathbb{P}^t$-субнормальной подгруппой, если $H = G$ или существует цепочка подгрупп

$$H = H_0 \subseteq H_1 \subseteq \ldots \subseteq H_n = G$$

такая, что для каждого i подгруппа H_{i-1} нормальна в H_i или $|H_i : H_{i-1}| \in \mathbb{P}^t$. Если в этой цепочке $|H_i : H_{i-1}| \in \mathbb{P}^t$ для всех i, то подгруппа H называется $\mathbb{P}^t$-субнормальной в группе G. При $t = 1$ эти определения предложены в [**2**], [**4**].

Без использования классификации конечных простых групп доказана следующая теорема, поглощающая [**2**, теорема 4.2], [**3**, теорема 1 (1)], [**4**, теорема 5.2].

Теорема. *Пусть A и B — $\mathrm{K}\mathbb{P}^2$-субнормальные подгруппы группы G и $G = AB$. Если A и B разрешимы, то G разрешима.*

Пример. Простая неабелева группа $\mathrm{PSL}_2(7)$ является произведением $\mathrm{K}\mathbb{P}^3$-субнормальной разрешимой подгруппы индекса 2^3 и $\mathrm{K}\mathbb{P}$-субнормальной разрешимой подгруппы S_4 индекса 7. Поэтому условие $\mathrm{K}\mathbb{P}^2$-субнормальности нельзя заменить $\mathrm{K}\mathbb{P}^3$-субнормальностью.

Список литературы

[1] *Монахов В. С.* Факторизуемые группы с разрешимыми факторами нечетных индексов // В кн.: Исследование нормального и подгруппового строения конечных групп. Минск: Наука и техника. 1984. С. 105–111.

[2] *Васильев А. Ф., Васильева Т. И., Тютянов В. Н.* О произведениях $\mathbb{P}$-субнормальных подгрупп в конечных группах // Сибирский матем. журнал. 2012. Том 53, № 1. С. 59–67.

[3] *Княгина В. Н., Монахов В. С.* Конечные факторизуемые группы с разрешимыми $\mathbb{P}^2$-субнормальными подгруппами // Сибирский матем. журнал. 2013. Том 54, № 1. С. 77–85.

[4] *Васильев А. Ф., Васильева Т. И., Тютянов В. Н.* О $\mathrm{K}\mathbb{P}$-субнормальных подгруппах конечных группах // Матем. заметки. 2014. Том 95, № 4. С. 517–528.

Гомельский инженерный институт МЧС Республики Беларусь, Гомель
E-mail: chyrykira@mail.ru

К линейной независимости степеней линейных форм

В. А. Чуркин

Пространство H_n^k вещественных однородных многочленов степени k от n переменных имеет базис, составленный из *k-х степеней подходящих линейных форм* [1]. Для каких линейных форм это верно? Верно ли это, если система $N = \binom{n-1+k}{n-1} = \dim H_n^k$ линейных форм *в общем положении*, т. е. когда любая подсистема из n линейных форм линейно независима?

Напомним, что произведением Адамара матриц одинакового размера $A = (a_{ij})$ и $B = (b_{ij})$ называется матрица $A \circ B = (a_{ij}b_{ij})$. Аналогично определяется произведение Адамара для столбцов.

Теорема 1. *Пусть заданы N вещественных линейных форм $\varphi_i = \sum_{j=1}^n a_{ij}x_j$ со строкой коэффициентов a_i. Тогда формы $\varphi_1^k, \ldots, \varphi_N^k$ линейно независимы в том и только том случае, когда k-я степень Адамара матрицы Грама системы векторов $a_1, \ldots, a_N$ невырождена.*

Теорема 2. *Пусть заданы $N = \binom{n-1+k}{n-1}$ вещественных линейных форм $\varphi_i = \sum_{j=1}^n a_{ij}x_j$. Пусть $A = (a_{ij})$ — матрица размера $N \times n$ и пусть $c_1, \ldots, c_n$ — столбцы A. Тогда формы $\varphi_1^k, \ldots, \varphi_N^k$ образуют базис H_n^k в том и только том случае, когда система векторов относительно произведения Адамара $c_1^{k_1} \circ \ldots \circ c_n^{k_n}$, где $\sum k_j = k$, образует базис пространства $\mathbb{R}^N$.*

Теорема 3. *Если $n = 2$, то система k-х степеней любых $N = k + 1$ линейных форм в общем положении образует базис пространства H_2^k. При $n = 3$, $k = 2$ существуют 6 линейных форм в общем положении, квадраты которых не образуют базис пространства H_3^2 квадратичных форм.*

Список литературы

[1] *Sonnenschein H.* A representation for polynomials in several variables, Amer. Math. Monthly, 78 (1971), 45–47.

Институт математики им. С.Л. Соболева СО РАН, г. Новосибирск
E-mail: churkin@math.nsc.ru

О группах Шункова, насыщенных группами лиева типа ранга 1

А. А. Шлепкин

Под покрытием группы понимается любая система ее подгрупп, теоретико-множественное объединение которых совпадает с самой группой. Первые исследования групп с различными покрытиями появились в работах П.Г. Конторовича и А.И. Старостина [1-3]. В.В. Беляев, А.В. Боровик, С. Томас, Б. Хартли и Г. Шют независимо доказали следующий результат [4,5,8,9]:

Если локльно-конечная группа G локально покрывается множеством подгрупп лиевского типа, ранги которых ограничены в совокупности, то и сама G является группой лиевского типа конечного ранга.

Естественным обощением понятия покрытия является понятие насыщенности [6].

Определение. *Пусть X — некоторое множество групп. Группа G насыщена группами из множества X, если любая конечная подгруппа из G содержится в подгруппе группы G, изоморфной некоторой группе из X.*

Очевидно, что если G — локально-конечная группа, то понятия насыщенности и покрытия группы эквивалентны.

В связи с упомянутым выше результатом о локально-конечных группах, обладающих локальным покрытием из конечных простых групп лиева типа ограниченного ранга, А.К. Шлепкиным был поставлен вопрос 14.101 в Коуровской тетради [7]:

Верно ли, что периодическая группа, насыщенная конечными простыми группами лиева типа, ранги которых ограничины в совокупности, сама является простой группой лиева типа конечного ранга?

Конечными простыми группами лиева типа ранга 1 над полем K являются следующие группы:

$$A_1(K),\ B_2(K),\ G_2(K),\ A_2(K).$$

Получен следующий результат:

Теорема. *Периодическая группа Шункова, насыщенная группами из множества конечных простых групп лиева типа ранга 1, изоморфна простой группе лиева типа ранга 1 над подходящим локально-конечным полем.*

Список литературы

[1] *Конторович П. Г.* Инвариантно покрываемые группы, Матем. сб. , 8 (1940), 423–430.

[2] *Конторович П. Г.* Инвариантно покрываемые группы II, Матем. сб., (1951), 79–88.

[3] *Конторович П. Г., Пекелис А. С., Старостин А. И.* Структурные вопросы теории групп, Матем., зап., Уральского ун-та. 3, (1961), 3–50.

[4] *Беляев В. В.* Локально-конечные группы Шевалле, В кн.: Исследования по теории групп, Свердловск: УНЦ АН СССР., (1984), 39–50.

[5] *Боровик А. В.* Вложения конечных групп Шевалле и периодические линейные группы, Сиб. мат. ж., 24, (1983), 26–35.

[6] *Шлепкин А. К.* Сопряженно бипримитивно конечные группы, содержащие конечные неразрешимые подгруппы, Сб. тезисов 3-й междунар. конф. по алгебре, Красноярск, (1993), 363.

[7] Коуровская тетрадь, Нерешенные вопросы теории групп. 16 издание, — Новосибирск: изд-во ИМ СО РАН, 2006.

[8] *Thomas S.* The classification of the simple periodic linear groups, Arch. Math. — V. 41., (1983), 103–116.

[9] *Hartly B., Shute G.* Monomorphisms and direct limits of finite groups of Lie type, Quart J. Math. Oxford., — V. 35., (1984), 49–71.

Сибирский федеральный университет, Красноярск
E-mail: shlyopkin@mail.ru

C^*-simplicity of n-periodic products of groups

V. S. Atabekyan

A discrete group is said to be C^*-simple if the reduced C^*-algebra of the group is simple. The following question was posed in [**1**]: Does there exist a countable group which is C^*-simple and which does not contain non-abelian free subgroups? In [**2**] proved, that for every $m \geq 2$ and every sufficiently large odd n, the reduced C^*-algebra of free periodic group $B(m,n)$ is simple. We obtain the following result.

Theorem. *The n-periodic product of any two non-trivial groups with only countably many amenable subgroups is a C^*-simple group for any odd $n \geq 1003$.*

Corollary 1. *The free periodic group $B(m,n)$ is C^*-simple for any odd $n \geq 1003$ and $m \geq 2$.*

Corollary 2. *There exist $2^{\aleph_0}$ non-isomorphic finitely generated simple groups of a given odd period $n \geq 1003$ which are C^*-simple.*

References

[1] *de la Harp P.* On simplicity of reduced C*-algebras of groups, Bull. London Math. Soc. (2007) 39 (1), 1–26.

[2] *Olshanskii A. Yu.*, *Osin D. V.* C*-simple groups without free subgroups. (2014), arXiv:1401.7300.

Yerevan State University, Yerevan (Armenia)
E-mail: varujan@atabekyan.com

On semiproportional columns in the character tables of the groups $\mathrm{Sp}_4(q)$ and $\mathrm{PSp}_4(q)$

V. A. Belonogov

Considered theme is connected with notions of the interaction, D-block and Φ-block (see [**1**] and also [**2**]). Functions α and β from a set H to the field $\mathbb{C}$ are called *semiproportional* if they are not proportional and there exists a subset M of H such that the restrictions of α and β on M, as well as their restrictions on $G\backslash M$, are proportional. Previously the author stated the following two conjectures.

Conjecture 1 (on semiproportional characters). *If a finite group has two semiproportional irreducible characters φ and ψ then $\varphi(1) = \psi(1)$.*

Conjecture 2 (on semiproportional columns of the character table). *If the character table of a finite group has two semiproportional columns corresponding to two its classes of conjugate elements then the cardinality of one of this classes divides cardinality of other.*

Earlier the author proved Conjectures 1 and 2 for the sporadic simple groups in [**3**], groups $\mathrm{L}_2(q)$, $\mathrm{SL}_2(q)$, $\mathrm{PGL}_2(q)$, $\mathrm{GL}_2(q)$ in [**4**], $\mathrm{PGL}_3(q)$, $\mathrm{GL}_3(q)$, $\mathrm{PGU}_3(q)$, $\mathrm{GU}_3(q)$ in [**5**], $\mathrm{L}_3(q)$, $\mathrm{SL}_3(q)$, $\mathrm{U}_3(q)$, $\mathrm{SU}_3(q)$ in [**6**], and $\mathrm{Sp}_4(q)$ ($\cong\mathrm{PSp}_4(q)$) with even q in [**7**].

Conjecture 1 is proved also for groups $\mathrm{Sp}_4(q)$ and $\mathrm{PSp}_4(q)$ with odd q in [**8**].

Theorem. *The conjecture 2 is true for the symplectic groups $\mathrm{Sp}_4(q)$ and $\mathrm{PSp}_4(q)$ with odd q.*

This work was supported by RFBR (project no. 13-01-00469) and Complex program of fundamental scientific investigations of UB RAS (project no. 15-16-1-5).

References

[1] *Belonogov V. A.* *D*-blocks of characters of finite group. Amer. Math. Soc. Transl. (2), 143 (1989), 103-128.

[2] *Belonogov V. A.* Representations and characters in the theory of finite groups. Sverdlovsk, Ural Branch of AS USSR, 1990, 380 pp. (in Russian).

[3] *Belonogov V. A.* Interactions and D-blocks in finite groups. In "Subgroups Structure of Groups". Ural Branch of AS USSR, Sverdlovsk, 1988, 4–44 (in Russian).

[4] *Belonogov V. A.* On small interactions in finite groups. Trudy Inst. Mat. i Mekh. UrO RAN, 1992, vol. 2, 3–18.

[5] *Belonogov V. A.* Small interactions in groups $\mathrm{GL}_3(q)$, $\mathrm{GU}_3(q)$, $\mathrm{PGL}_3(q)$ и $\mathrm{PGU}_3(q)$. Trudy Inst. Mat. i Mekh. UrO RAN, 1996, vol. 4, 17–47 (in Russian).

[6] *Belonogov V. A.* Small interactions in groups $\mathrm{SL}_3(q)$, $\mathrm{SU}_3(q)$, $\mathrm{PSL}_3(q)$ и $\mathrm{PSU}_3(q)$. Trudy Inst. Mat. i Mekh. UrO RAN, 1998, vol. 5, 3–27 (in Russian).

[7] *Belonogov V. A.* Small interactions in groups $\mathrm{Sp}_4(q)$ for even q. Proc. Steklov Inst. Math., 2012, vol. 279, suppl. 1, S1–S20.

[8] *Belonogov V. A.* Semiproportional irreducible characters of groups $\mathrm{Sp}_4(q)$ and $\mathrm{PSp}_4(q)$ for odd q. Trudy Inst. Mat. i Mekh. UrO RAN, 2013, vol. 19, no. 1, 25–40 (in Russian).

Inst. Math. Mech., Ural Branch of RAS, Ekaterinburg (Russia)
E-mail: belonogov@imm.uran.ru

Shunkov groups with the maximal condition for uncomplemented abelian subgroups

N. S. Chernikov

The following author's new theorems hold.

Theorem 1. *The infinite periodic Shunkov group G satisfies the maximal condition for uncomplemented abelian subgroups iff $G = A \leftthreetimes (C \times D)$ where A is infinite and A is a direct product of normal in G subgroups of prime order, C is a direct product of groups of prime order or $C = 1$, D is cyclic, if $D \neq 1$, then for every $g \in D \setminus \{1\}$, the centralizer of g in A is finite, if C is infinite, then $D = 1$.*

Theorem 2. *The infinite periodic Shunkov group satisfies the maximal condition for uncomplemented subgroups iff it is completely factorizable.*

Institute of Mathematics of the National Academy of Sciences of Ukraine, Kyiv (Ukraine)
E-mail: chern@imath.kiev.ua

Recognition by spectrum for finite simple classical groups in characteristic 2

M. A. Grechkoseeva, A. V. Vasil'ev

We say that finite groups are isospectral if their sets of element orders coincide. The recognition by spectrum problem for a finite group G is to find the number $h(G)$ of pairwise non-isomorphic finite groups isospectral to G. If $h(G) = 1$ then G is referred to as recognizable by spectrum.

Recall that there are five series of finite simple classical groups over fields of characteristic 2, namely $L_n(q)$ with $n \geqslant 2$, $U_n(q)$ with $n \geqslant 3$, $S_{2n}(q) \simeq O_{2n+1}(q)$ with $n \geqslant 2$, and $O^{\pm}_{2n}(q)$ with $n \geqslant 4$. The recognition problem is solved for all n in linear and unitary cases (see [**1, 2**]), and for $n = 2, 3, 4$ and $n \geqslant 20$ in symplectic and orthogonal cases (see [**3, 4, 5**] for small dimensions and [**6**] for large). Our purpose is to complete the study of symplectic and orthogonal cases. The result is the following

Theorem. *Let q be even and let L be one of the simple groups $S_{2n}(q)$ with $n \geqslant 2$, or $O^{\pm}_{2n}(q)$ with $n \geqslant 4$. Then L is recognizable by spectrum or one of the following holds:*

(1) *L is $S_4(q)$ or $S_8(q)$, and $h(L) = \infty$;*

(2) *L is $S_6(2)$ or $O^{+}_8(2)$, and $h(L) = 2$.*

Acknowledgments. The work is supported by Russian Science Foundation (project 14-21-00065).

References

[1] *Grechkoseeva M. A.* Recognition by spectrum for finite linear groups over fields of characteristic 2, Algebra Logic, 47 (2008), no. 4, 229–241.

[2] sl Grechkoseeva M. A. and Shi W. J. On finite groups isospectral to finite simple unitary groups over fields of characteristic 2, Sib. Élektron. Mat. Izv., 10 (2013), 31–37.

[3] *Mazurov V. D., Xu M. C., and Cao H. P.* Recognition of the finite simple groups $L_3(2^m)$ and $U_3(2^m)$ by their element orders, Algebra Logic, 39 (2000), no. 5, 324–334.

[4] *Staroletov A. M.* On recognition by spectrum of the simple groups $B_3(q)$, $C_3(q)$ and $D_4(q)$, Siberian Math. J., 53 (2012), no. 3, 532–538.

[5] *Grechkoseeva M. A. and Staroletov A. M.* Unrecognizability by spectrum of finite simple orthogonal groups of dimension nine, Sib. Élektron. Mat. Izv., 11 (2014), 921–928.

[6] *Zvezdina M. A.* Spectra of automorphic extensions of finite simple symplectic and orthogonal groups over fields of characteristic 2, Sib. Élektron. Mat. Izv., 11 (2014), 823–832.

Sobolev Institute of Mathematics,
Novosibirsk State University, Novosibirsk (Russia)
E-mail: grechkoseeva@gmail.com, vasand@math.nsc.ru

Spectra of automorphic extensions of finite simple groups $F_4(q)$ and ${}^3D_4(q)$

M. A. Grechkoseeva, M. A. Zvezdina

The *spectrum* of a finite group G denoted by $\omega(G)$ is the set of its element orders. Groups are called *isospectral* if their spectra coincide. Let S be a finite non-abelian simple group and let G be a finite group such that $S < G \leq \mathrm{Aut}(S)$. Our work is concerned with the following problem (see [**1**, Question 17.36]): in which cases is G isospectral to S? We solve this problem for the simple exceptional groups $F_4(q)$, with q odd, and ${}^3D_4(q)$.

Theorem 1. *Let $S = F_4(q)$, where q is a power of an odd prime p, and let $S < G \leq \mathrm{Aut}(S)$. Then $\omega(G) = \omega(S)$ if and only if G/S is a 2-group and $p \notin \{3, 7, 11\}$.*

Theorem 2. *Let $S = {}^3D_4(q)$, where q is a power of a prime p, and let $S < G \leq \mathrm{Aut}(S)$. Then $\omega(G) = \omega(S)$ if and only if G/S is a 2-group and $p \geq 7$.*

Theorems 1 and 2 complete the study of finite groups isospectral to simple groups of types F_4 and ${}^3D_4$. Indeed, the groups $F_4(2^k)$ are recognizable by spectrum, that is $\omega(G) = \omega(F_4(2^k))$ implies $G \simeq F_4(2^k)$ [**2**]. The group ${}^3D_4(2)$ is irrecognizable by spectrum, that is there are infinitely many pairwise non-isomorphic finite groups isospectral to ${}^3D_4(2)$ [**3**]. Finally, if S is one of the groups $F_4(q)$, with q odd, or ${}^3D_4(q)$, with $q \neq 2$, and G is a finite group isospectral to S, then it follows from [**4, 5, 6**] that $S \leq G \leq \mathrm{Aut}(S)$, and so Theorem 1 and 2 can be applied.

Also Theorem 1 and 2 provide a positive answer to [**1**, Question 16.24].

Acknowledgments. The work is supported by Russian Science Foundation (project 14-21-00065).

References

[1] *Mazurov V. D. and Khukhro E. I.* (eds.), The Kourovka notebook. Unsolved problems in group theory, 18 ed., Institute of Mathematics, Russian Academy of Sciences, Siberian Div., Novosibirsk, 2014.

[2] *Cao H. P., Chen G. Y., Grechkoseeva M. A., Mazurov V. D., Shi W. J., Vasil'ev A. V.* Recognition of the finite simple groups $F_4(2^m)$ by the spectrum, Siberian Math. J., 2004, Volume 45, Issue 6, P. 1031–1035.

[3] *Mazurov V. D.* Unrecognizability by spectrum for a finite simple group ${}^3D_4(2)$, Algebra and Logic, 2013, Volume 52, Issue 5, P. 400–403.

[4] *Alekseeva O. A.* Kondratiev A. S., Quazirecognizability by the set of element orders for groups ${}^3D_4(q), F_4(q)$, for q odd, Algebra and Logic, 2005, Volume 44, Issue 5, P. 287–301.

[5] *Alekseeva O. A.* Quazirecognizability by the set of element orders for groups ${}^3D_4(q)$, for q even, Algebra and Logic, 2006, Volume 45, Issue 1, P. 1–11.

[6] *Grechkoseeva M. A.* Element orders in covers of finite simple groups, Algebra and Logic, 2013, Volume 52, Issue 5, P. 426–428.

Sobolev Institute of Mathematics, Novosibirsk State University, Novosibirsk (Russia)
E-mail: grechkoseeva@gmail.com, maria.a.zvezdina@gmail.com

On the automorphisms of Adyan's groups

A. E. Grigorian, Sh. A. Stepanyan

The additive group of rational numbers is torsion-free and every two its non-cyclic subgroups have nontrivial intersection. The question of the existence of non-abelian groups with such properties posed by Kontorovich had long remained open. The first examples of these groups were constructed by S.I.Adyan (see, for example, [**1**]). These groups are denoted by $A(m, n)$. They have the following presentations.

$$A(m,n) = \langle a_1, a_2, ...a_m, d \,|\, a_j d = d a_j \text{ ш } A^n = d \, \text{for all} \, A^n \in \bigcup_{i=1}^{\infty} \mathcal{E}_i \text{ ш } 1 \leq j \leq m \rangle,$$

where $n \geq 665$ is an arbitrary odd number. In [**2**] proved that the automorphism group $AutA(m, n)$ contains no involutions. We study the automorphism tower of $A(m, n)$. In particular, we obtain the following result.

Theorem. *The inner automorphisms group of $A(m, n)$ is characteristic subgroup in the group $Aut(A(m, n))$ of all automorphisms for all $m > 1$ and odd $n \geq 1003$.*

References

[1] *Adian S. I.* The Burnside problem and identities in groups. Ergebnisse der Mathematik und ihrer Grenzgebiete, 95. Springer-Verlag, Berlin-New York, 1979.

[2] *Sozutov A. I., Durakov E. B.* On groups with isolated involution, Sibirsk. Mat. Zh., 55:4 (2014), 863–874.

Yerevan State University, Yerevan (Armenia)
E-mail: shogh.stepanyan@gmail.com

Subgroup-closed lattice formations

S. F. Kamornikov, Xiaolan Yi

All groups considered in this paper are finite. The notation and terminology agree with the books [1,2].

One of the most striking results in the theory of subnormal subgroups is the celebrated "join" theorem, proved by H. Wielandt in 1939: the subgroup generated by two subnormal subgroups of a finite group is itself subnormal. As a result, the set of all subnormal subgroups of a group is a sublattice of the subgroup lattice.

Therefore the following question naturally arises:

Which are the formations $\mathfrak{F}$ for which the set $sn_{\mathfrak{F}}(G)$ of all $\mathfrak{F}$-subnormal subgroups of G is a sublattice of the subgroup lattice of G for every group G?

This question was first proposed by L.A. Shemetkov in his monograph [2, Problem 12] in 1978 and it appeared in the Kourovka Notebook [3, Problem 9.75] in 1984.

In 1992, A. Ballester-Bolinches, K. Doerk, and M.D. Perez-Ramos gave the answer to that question in the soluble universe for subgroup-closed saturated formations. In 1993, A.F. Vasil'ev, S.F. Kamornikov, and V.N. Semenchuk published the solution of the Shemetkov's problem in the general finite universe for subgroup-closed saturated formations.

This paper can be considered as a further great step of the programme aiming to the classification of all lattice formations. Here we solve the Shemetkov's problem for all subgroup-closed formations. The main purpose of our paper is to prove the following theorem.

Theorem. *Let $\mathfrak{F}$ be a subgroup-closed formation. Then $\mathfrak{F}$ is a lattice formation if and only if $\mathfrak{F} = \mathfrak{M} \times \mathfrak{K} \times \mathfrak{L}$ for some subgroup-closed formations $\mathfrak{F}$, $\mathfrak{M}$ and $\mathfrak{L}$ satisfying the following conditions:*

(1) $\pi(\mathfrak{M}) \cap \pi(\mathfrak{K}) = \emptyset$, $\pi(\mathfrak{K}) \cap \pi(\mathfrak{L}) = \emptyset$ *and* $\pi(\mathfrak{M}) \cap \pi(\mathfrak{L}) = \emptyset$.

(2) $\mathfrak{M} = \mathfrak{S}_{\pi(\mathfrak{M})}(\mathfrak{M})$ *is a saturated formation, and it is an $\mathfrak{M}^2$-normal Fitting class.*

(3) *Every non-cyclic $\mathfrak{M}$-critical group G with $\Phi(G) = 1$ is a primitive group of type 2 such that $G/Soc(G)$ is a cyclic group of prime power order.*

(4) *There exists a partition $\{\pi_j | j \in J\}$ of $\pi(\mathfrak{K})$ such that $\mathfrak{K} = \times_{j \in J} \mathfrak{S}_{\pi_j}$. Moreover, $|\pi_j| > 1$ for all $j \in J$.*

(5) $\mathfrak{L} \subseteq \mathfrak{N}_{\pi(\mathfrak{L})}$.

References

[1] *Kamornikov S. F., Sel'kin M. V.* Subgroup functors and classes of finite group. Minsk: Belaruskaya Nauka, 2003.

[2] *Shemetkov L. A.* Formations of finite groups. Moscow: Nauka, 1978.

[3] *Mazurov V. D., Khukhro E. I.* (Eds.). Unsolved problems in group theory: The Kourovka Notebook. Novosibirsk: Russian Academy of Sciences, Siberian Branch, Institute of Mathematics, 2010.

Gomel Branch of International University MITSO, Belarus; Zhejiang Sci-Tech University, China
E-mail: sfkamornikov@mail.ru; yixiaolan2005@126.com

On the pronormality of subgroups of odd indices in finite simple groups

A. S. Kondrat'ev, N. V. Maslova, D. O. Revin

A subgroup H of a group G is *pronormal* in G if H and H^g are conjugate in $\langle H, H^g\rangle$ for every $g \in G$.

In [**1**] the following conjecture was formulated.

Conjecture. *Subgroups of odd indices are pronormal in finite simple groups.*

We prove the following theorem.

Theorem. *All subgroups of odd indices are pronormal in the following finite simple groups*:

(1) A_n, *where* $n \geq 5$;
(2) *sporadic groups*;
(3) *groups of Lie type over fields of characteristic* 2;
(4) $L_{2^n}(q)$;
(5) $U_{2^n}(q)$;
(6) $S_{2n}(q)$, *where* $q \not\equiv \pm 3 \pmod 8$;
(7) $O_n(q)$;
(8) *exeptional groups of Lie type not isomorphic to* $E_6(q)$ *or* ${}^2E_6(q)$.

The work is supported by Russian Science Foundation (project 14-21-00065). The second author is a winner of the competition of the Dmitry Zimin Foundation "Dynasty" for support of young mathematicians in 2013 year.

References

[1] *Vdovin E. P., Revin D. O.* Pronormality of Hall subgroups in finite simple groups // Sib. Math. J. 2012. Vol. 53, no. 3. P. 419–430.

IMM UB RAS, Ekaterinburg (Russia), IMM UB RAS, Ekaterinburg (Russia), IM SB RAS, Novosibirsk (Russia)
E-mail: a.s.kondratiev@imm.uran.ru, butterson@mail.ru, danila.revin@gmail.com

On the minimal volume of subspace trades

D. S. Krotov

Let F^v be a v-dimensional space over a finite field F of order q, and let $\left[{F^v \atop i}\right]$ denote the set of i-demensional subspaces of F^v. By $\mathrm{Gr}(F^v, i)$, we denote the Graßmann graph on the vertex set $\left[{F^v \atop i}\right]$, where two subsets are adjacent iff they intersect in a $(i-1)$-dimensional subspace. A pair (T_0, T_1) of disjoint nonempty subsets of $\left[{F^v \atop k}\right]$ is called a subspace bitrade of type $\mathrm{T}(t, k, v)$ iff every subspace from $\left[{F^v \atop t}\right]$ is covered by the same number of subspaces from T_0 and T_1.

Theorem 1. *Let the integers t, k, and v satisfy $0 \le t < k < v - t$. The minimal possible cardinality $|T_0 \cup T_1|$ of a subspace bitrade (T_0, T_1) of type $T(t, k, v)$ equals*

$$\prod_{i=0}^{t}(1+q^i) = \sum_{j=0}^{t+1} q^{\frac{j(j-1)}{2}} \left[{t+1 \atop j}\right]_q$$

where $\left[{i \atop j}\right]_q = \frac{[i]_q[i-1]_q \ldots [i-j+1]_q}{[1]_q[2]_q \ldots [j]_q}$, $[r]_q = 1 + q + \ldots + q^{r-1}$.

The analog of this theorem for the classical design trades (where the role of F^v is played by a set of v elements, the role of the i-dimensional subspaces is played by the subsets of cardinality i, and the formulas hold with $q = 1$) was proven in [**2**].

An example of the set $|T_0 \cup T_1|$ that can be split into a minimal bitrade (T_0, T_1) consists of all k-dimensional subspaces of F^v whose all vectors satisfy $x_1x_2 + \ldots + x_{2t+1}x_{2t+2} = 0$, $x_{k+t+2} = 0, \ldots, x_v = 0$, written as v-tuples $(x_1, \ldots, x_v)$ in some fixed basis.

In the case $k = t + 1$, the statement of Theorem 1 was proven in [**1**]; the proof of the general case uses that result. The proof of the minimality is based on Corollary 1.

Lemma 1. *Let a real-valued function ϕ on $\left[{F^v \atop k}\right]$ be a sum of eigenfunctions ϕ_0, ϕ_1, $\ldots$, ϕ_{k-t-1} of the graph $\mathrm{Gr}(F^v, k)$, where the corresponding eigenvalues are the $k - t$ minimal eigenvalues of $\mathrm{Gr}(F^v, k)$. And let for some fixed $(t + 1)$-dimensional subspace U, the set U_k consist of all k-dimensional subspaces that include U. Then the distribution $\left(\sum_{Z \in \left[{F^v \atop k}\right], d(Z,U_k)=j} \phi(Z)\right)_{j=0}^{t+1}$ of ϕ with respect to U_k is proportional to $\left((-1)^j q^{\frac{j(j-1)}{2}} \left[{t+1 \atop j}\right]_q\right)_{j=0}^{t+1}$.*

Corollary 1. *A non-constant function ϕ satisfying the hypothesis of Lemma 1 (in particular, the characteristic function $\chi_{T_0} - \chi_{T_1}$ of any subspace bitrade (T_0, T_1) of type $T(t, k, v)$) has at least $\sum_{j=0}^{t+1} q^{\frac{j(j-1)}{2}} \left[{t+1 \atop j}\right]_q$ nonzeros.*

The work was funded by the Russian Science Foundation (Grant 14-11-00555).

References

[1] *Krotov D. S., Mogilnykh I. Yu., Potapov V. N.* To the theory of q-ary Steiner and other-type trades. Electronic preprint http://arxiv.org/abs/1412.3792

[2] *Hwang H. L.* On the structure of (v, k, t) trades // Journal of Statistical Planning and Inference. 1986. Vol. 13. P. 179–191. http://dx.doi.org/10.1016/0378-3758(86)90131-X

Sobolev Institute of Mathematics, Novosibirsk (Russia)
E-mail: krotov@math.nsc.ru

On the finite prime spectrum minimal groups

N. V. Maslova

Let G be a finite group. The *prime spectrum* $\pi(G)$ is the set of all prime divisors of $|G|$. G is *prime spectrum minimal* if $\pi(G) \neq \pi(H)$ for every proper subgroup H of G. We continue the study of the normal structure of finite prime spectrum minimal groups, started in [**1**]. The following results are obtained.

Theorem. *Let G be a finite group containing a nonabelian composition factor S with $|\pi(S)| = 3$. Then one of the following statements holds*:

(1) *$S \in \{A_6, PSU_3(3), PSU_4(2)\}$ and G is not prime spectrum minimal*;

(2) *$S \in \{A_5, PSL_2(7), PSL_3(3)\}$ and G is prime spectrum minimal if and only if there exists a normal series*

$$G = G_0 > G_1 > \ldots > G_n = 1$$

such that

(i) *for $i \geq 1$, the factor G_i/G_{i+1} is an elementary abelian p-group isomorphic to a Sylow subgroup of G for some prime divisor p of $|G|$ and G/G_i acts irreducibly on G_i/G_{i+1}*;

(ii) *for the factor $\bar{G} = G_0/G_1$, one of the following statements holds*:

(a) *$\bar{G}$ is isomorphic to either A_5 or $PSL_3(3)$*;

(b) *$O_3(\bar{G}) = \Phi(\bar{G})$ and $\bar{G}/\Phi(\bar{G}) \cong PSL_2(7)$*;

(3) *$S \cong PSL_2(8)$ and if G is prime spectrum minimal then nonabelian composition factors of G are exhausted by groups from the set $\{S\} \cup \{Sz(2^w) \mid w \equiv \pm 1 \pmod 3\}$*;

(4) *$S \cong PSL_2(17)$ and if G is prime spectrum minimal then nonabelian composition factors of G are exhausted by groups from the set $\{S\} \cup \{Sz(2^w)\}$.*

Moreover, in the cases (3) *and* (4) *the following statements hold*:

(i) *for every group S_1 from the set $\{Sz(2^w) \mid w \equiv \pm 1 \pmod 3\}$ or $\{Sz(2^w)\}$, respectively, there exists a finite prime spectrum minimal group G containing composition factors isomorphic to S and S_1*;

(ii) *for every positive integer m there exist $S_1, \ldots S_m$ from the set $\{Sz(2^w) \mid w \equiv \pm 1 \pmod 3\}$ or $\{Sz(2^w)\}$, respectively, and finite prime spectrum minimal group G containing composition factors isomorphic to $S, S_1, \ldots, S_m$.*

The work is supported by Russian Science Foundation (project 14-11-00061). The author is a winner of the competition of the Dmitry Zimin Foundation "Dynasty" for support of young mathematicians in 2013 year.

References

[1] *Maslova N. V., Revin D. O.* On the nonabelian composition factors of a finite prime spectrum minimal group // Proc. Steklov Inst. Math. 2014. Vol. 287, Suppl 1. P. 116–127.

IMM UB RAS, Ekaterinburg (Russia)
E-mail: butterson@mail.ru

On verbal embeddings of residually finite groups

Vahagn H. Mikaelian

The well-known theorem on embeddings of countable groups into 2-generator groups [**1**] was a stimulus for wide research on embeddings with additional properties. One of the main directions of research was on embeddings of countable group H into 2-generator group G, where G has a given property $\mathcal{P}$, as soon as H possesses $\mathcal{P}$. Here $\mathcal{P}$ may be the property of being a soluble group, finitely generated nilpotent group, linearly ordered group, one of the types of generalized nilpotent groups or generalized soluble group, etc.. Some of our results on embeddings of countable generalized soluble groups can be found in [**3**]–[**6**].

Another direction of research was on embeddings, where the image of H "occupies a small part" inside the 2-generator group G, for example, if the embedding is V-verbal in the sense, that the image of H is inside the verbal subgroup $V(G)$ for the given non-trivial words set $V \subseteq F_\infty$ (this is a generalization of results of P. Hall, B.H. Neumann and others, who proved the same for cases when V is the commutator, second commutator, etc.). We covered some cases on verbal embeddings in [**2**], [**3**].

In the current talk we would like to continue the mentioned research and focus on verbal embeddings of countable, residually finite groups, started by of J.S. Wilson in [**9**]. We prove:

Theorem. *Let H be an arbitrary countable, residually finite group and $V \subseteq F_\infty$ be any non-trivial word set. Then there exists a 2-generator residually finite group G with a subgroup $\tilde{H}$ such that H is isomorphic to $\tilde{H}$, and $\tilde{H}$ lies in the verbal subgroup $V(G)$.*

The proof is based on technics with generalizations of the operation of wreath products, we used in [**3**]–[**6**], and on some ideas on residually finite groups from [**9**].

References

[1] Higman G., Neumann B., Neumann Hanna, Embedding theorems for groups, J. London Math. Soc. 3 24, (1949), 247–254.

[2] *Mikaelian V. H.* Subnormal embedding theorems for groups, J. London Math. Soc., 62 (2000), 398–406.

[3] *Mikaelian V. H.* On embeddings of countable generalized soluble groups in two-generated groups, J. Algebra, 250 (2002), 1–17.

[4] *Mikaelian V. H.* An embedding construction for ordered groups, J. Austral Math. Soc. (A), 74 (2003), 379–392.

[5] *Mikaelian V. H.* Infinitely many not locally soluble SI*-groups, Ricerche di Matematica, Univ. Studi Napoli, Naples, 52 (2003), 1–19.

[6] *Mikaelian V. H.* On embedding properties of SD-groups, International Journal of Mathematics and Mathematical Sciences, 2004:2 (2004) 65–76.

[7] *Ol'shanskii A. Yu.* Embedding of countable periodic groups in simple 2-generator periodic groups, Ukrain. Mat. Zh. 43 (1991), no. 7-8, 980–986 (Russian); translation in Ukrainian Math. J. 43 (1991), no. 7-8, 914–919 (1992).

[8] *Roman'kov V. A.* Embedding theorems for nilpotent groups. (Russian) Sibirsk. Mat. Zhurnal. 13 (1972), 859–867

[9] *Wilson J. S.* Embedding theorems for residually finite groups, Math. Z. 174 (1980), no. 2, 149–157.

Informatics and Applied Mathematics Department, Yerevan State University, Yerevan 0025, Armenia.
E-mail: v.mikaelian@gmail.com

Isotopically transitive pairs of MOLS

V. N. Potapov

Let F_q be the Galois field of order q. A subset M of F_q^n is called an *MDS code* (with code distance $k+1$) if $|M \cap \Gamma| = 1$ for each k-dimensional face Γ. For $k = n-1$, an MDS code is equivalent to a set of $(n-2)$ *mutually orthogonal latin squares* (MOLS).

Proposition 1. *Let $M \subset F_q^m$ be an MDS code and let for each $x \in M$ a set $L(x) \subset F_{q'}^m$ be an MDS code. Then the set $C = \{(x,y) \mid x \in M, y \in L(x)\} \subset F_q^m \times F_{q'}^m$ is an MDS code.*

If the code $L(x)$ doesn't depend on x then the MDS code C is *obtained as Cartesian product*. A subset T of MDS code C is called a *subcode* if T is a MDS code in $A_1 \times \cdots \times A_n$ and $T = C \cap (A_1 \times \cdots \times A_n)$ where $A_i \subset F_q$, $i \in \{1,\ldots,n\}$. An *isotopism* is a transform $\overline{\tau} : \overline{x} \mapsto \overline{\tau x}$ where $\overline{x} = (x_1,\ldots,x_n) \in F_q^n$, $\overline{\tau x} = (\tau_1 x_1,\ldots,\tau_n x_n)$, $\tau_i \in S_q$. Define the *group of autotopisms* $\mathrm{Ist}(A) = \{\overline{\tau} \mid \overline{\tau} A = A\}$, which map $A \subseteq F_q^n$ to itself. A set $A \subseteq F_q^n$ is called *isotopically transitive* if for every two vertices $\overline{x}, \overline{y}$ from A there exists an isotopism $\overline{\tau}$ such that $\overline{\tau}(\overline{x}) = \overline{y}$ and $\overline{\tau}(A) = A$; i.e., the group $\mathrm{Ist}(A)$ acts transitively on A. It is clear that two isotopic codes are isotopically transitive or not simultaneously. A code is called *linear* if it is a linear subspace. Obviously, a linear code is isotopically transitive.

Proposition 2. *If a code C is obtained as the Cartesian product of two isotopically transitive codes, then C is isotopically transitive.*

Proposition 3. *a) Any vertex of an MDS code obtained as the Cartesian product lies in two proper subcodes (at least). b) A linear MDS code over $GF(q^2)$ (q is prime) either hasn't subcodes or any vertex of the code lies in two proper subcodes.*

Consider the code $C_0 \subset (F_q \times F_q)^4$, $(x_i, y_i) \in F_q \times F_q$, determined by the equations

$$\begin{cases} x_3 = l_{11}x_1 + l_{12}x_2; x_4 = l_{21}x_1 + l_{22}x_2; \\ y_3 = m_{11}y_1 + m_{12}y_2 + \xi_1(x_1,x_2); y_4 = m_{21}y_1 + m_{22}y_2 + \xi_2(x_1,x_2), \end{cases}$$

where ξ_1 and ξ_2 are quadratic functions and the pairs of vectors (l_{11}, l_{12}), (l_{21}, l_{22}) and (m_{11}, m_{12}), (m_{21}, m_{22}) are not collinear. This code corresponds to 2-MOLS in $F_q \times F_q \cong F_{q^2}$. The following theorem can be verified by direct calculation.

Theorem 1. *If the pairs of vectors (l_{11}, l_{12}), (m_{11}, m_{12}) and (l_{21}, l_{22}), (m_{21}, m_{22}) are not collinear, then C_0 is an isotopically transitive MDS code.*

The proof of Theorem 2 is based on Proposition 3.

Theorem 2. *If $\xi_2(x_1,x_2) = x_1x_2$ and $\xi_1(x_1,x_2) \equiv 0$ then C_0 isn't isotopic to a linear code or to a code obtained as the Cartesian product.*

The idea to use quadratic functions for constructing transitive codes was proposed in [**1**].

References

[1] *Krotov D. S., Potapov V. N.* Propelinear 1-perfect codes from quadratic functions // IEEE Trans. Inform. Theory. 2014. V. 60, N 4. P. 2065–2068.

Sobolev Institute of Mathematics, Novosibirsk, Russia
E-mail: vpotapov@math.nsc.ru

Distance regular colorings of the n-dimensional rectangular grid with the large number of colors

A. Yu. Vasil'eva

A vertex partition $(V_1, \ldots, V_k)$ of a graph G is called a perfect k-coloring (or equitable partition, or regular partition, or partition design) if for every $i, j \in \{1, \ldots, k\}$ there is the number a_{ij} such that every vertex of V_i has exactly a_{ij} neighbors in V_j. The matrix $A = (a_{ij})$ is called the parameter matrix of the coloring. A perfect coloring $(V_1, \ldots, V_k)$ is distance regular if its parameter matrix is three-diagonal (i.e. $(V_1, \ldots, V_k)$ is the distance coloring with respect to V_1). In this case the set V_1 is called a distance regular code and we will write the matrix $(a_{ij})_{ij=1}^k$ as the sequence of its nonzero elements: $[a_{11}a_{12}|a_{21}a_{22}a_{23}|a_{32}a_{33}a_{34}| \ldots, |a_{kk-1}a_{kk}]$. A k-coloring of graph vertices can be presented as a function φ over graph vertices with values in the set $\{1, 2, \ldots, k\}$.

We study the distance regular colorings of the infinite $2n$-regular graph of the n-dimensional rectangular grid $\mathbf{Z}^n$. The coloring $\varphi = \varphi(x_1, \ldots, x_n)$ of $\mathbf{Z}^n$ is called reducible if it can be reduced to the coloring of $\mathbf{Z}^1$, i.e. for any $(x_1, x_2, \ldots, x_n) \in \mathbf{Z}^n$

$$\varphi(x_1, x_2, \ldots, x_n) = \varphi_1 (\delta_1 x_1 + \delta_2 x_2 + \ldots + \delta_n x_n),$$

where φ_1 is a k-coloring of $\mathbf{Z}^1$ and $\delta_1, \ldots, \delta_k \in \{0, 1, -1\}$. Earlier it was shown [**2**] that any irreducible distance regular coloring of $\mathbf{Z}^n$ has at most $2n+1$ colors but it wasn't known if the k-coloring exists for an arbitrary fixed $k \leq 2n+1$ or not.

Theorem. *For every $n \in \mathbb{N}$ and every $k \geq [n/2] + 1$ there exists irreducible distance regular k-coloring of $\mathbf{Z}^n$, moreover, all theirs variables are essential.*

Finally, we give the examples of the irreducible distance regular colorings of $\mathbf{Z}^n$ for an arbitrary n. Let $r \geq n$.

1) The matrix $[2n-r, r|1, 2n-r, r-1|2, 2n-r, r-2| \ldots |r-1, 2n-r, 1|r, 2n-r]$ is the parameter matrix of the $(r+1)$-coloring, $n+1 \leq r+1 \leq 2n+1$.

2) In the case $r = 2q+1$
$[2n-r, 2q+1|1, 2n-r, 2q|2, 2n-r, 2q-1| \ldots |q-1, 2n-r, q+2|q, k+q+1]$
is the parameter matrix of the $(q+1)$-coloring, $[n/2]+1 \leq q+1 \leq n+1$.

3) In the case $r = 2q$
$[2n-r, 2q|1, 2n-r, 2q-1|2, 2n-r, 2q-2| \ldots |q-1, 2n-r, q+1|2q, 2n-r]$
is the parameter matrix of the $(q+1)$-coloring, $[n/2]+1 \leq q+1 \leq n+1$.

References

[1] *Avgustinovich S. V., Vasil'eva A. Yu., Sergeeva I. V.* Distance regular colorings of the infinite rectangular grid // Diskretn. Anal. Issled. Oper. 2011. Vol. 18. N3. P. 3–10.

[2] *Avgustinovich S., Vasil'eva A.* Distance Regular Colorings of n-Dimensional Rectangular Grid // http://arxiv.org/abs/1412.7665

Sobolev Institute of Mathematics, Novosibirsk
E-mail: vasilan@math.nsc.ru

On finite 2-groups generated by an element and involution or by three involutions

B. M. Veretennikov

Classifications of groups in title are old problems in the theory of finite 2-groups. Finite 2-groups, generated by an element and involution, are described in [**1**] under some rather strong conditions. Finite 2-groups of exponent 4, generated by three involutions, are classified in §61 [**2**], in particular the maximal order of such groups is 2^{10}.

We present following statements.

Theorem 1. *For any integer $n \geq 2$ there exists a finite 2-group G of derived length 3, generated by an element of order 2^n and involution, with G'' of rank $\binom{2^n-1}{2}$ and arbitrary exponent.*

Theorem 2. *There exists a finite 2-group G of derived length 4, generated by three involutions, with G''' of arbitrary large rank and exponent.*

For construction of such groups we use the group from [**3**]. This group is an Alperin group, i.e. group in which every two-generated subgroup has a cyclic commutator subgroup.

References

[1] *Ustyuzhaninov A. D.* Finite 2-groups generated by an element and involution, In: Subgroup Structure of Groups (in Russian), Sverdlovsk (1988), pp. 153-157.

[2] *Berkovich Y., Janko Z.* Groups of prime power order, Volume 2, Walter de Gruyter, Berlin, N.Y., 2008.

[3] *Veretennikov B. M.* On the second commutants of finite Alperin groups, Sib. Mat. Zh., **55**, N 1 (2014), 19–34.

Ural Federal University, Ekaterinburg (Russia)
E-mail: boris@veretennikov.ru

V. Секция «Теория колец»

filipp@ya.ru, fburtyka@sfedu.ru

Алгебраическая теория булевых матричных полиномов

Ф. Б. Буртыка

Впервые алгебраическая теория матричных полиномов появилась в статьях [**1, 2**] для матричных полиномов над комплексными числами, там же приведен алгоритм нахождения корней таких матричных полиномов. Похожий алгоритм был предложен и в статье [**3**], однако все эти работы оставили без рассмотрения многие алгебраические аспекты теории матричных полиномов.

В последнее же время в связи с приложениями в гомоморфной криптографии [**4, 5, 6**] возникла необходимость более глубокого изучения свойств матричных полиномов и, в первую очередь, такого важного их подкласса как булевы матричные полиномы.

В настоящем исследовании рассмотрены многие естественно возникающие принципиальные вопросы относительно колец матричных полиномов от одной переменной а также их факторколец. Освещен вопрос расширения упомянутых алгоритмов нахождения корней матричных полиномов на алгебраически не замкнутые поля, в частности поле Галуа из двух элементов. Основная часть работы посвящена комбинаторным вопросам, связанным с кольцами и факторкольцами булевых матричных полиномамов.

Работа выполнена при поддержке гранта РФФИ (проект №15-07-00597 А).

Список литер туры

[1] *Dennis J. E. Jr, Traub J. F., Weber R.* The algebraic theory of matrix polynomials. SIAM Journal on Numerical Analysis, 13(6):831–845, 1976.

[2] *Dennis J. E. Jr, Traub J. F., Weber R.* Algorithms for solvents of matrix polynomials. SIAM Journal on Numerical Analysis, 15(3):523–533, 1978.

[3] *Шаваровский Б. З.* Поиск полного набора решений или доказательство неразрешимости некоторых классов матричных многочленных уравнений с коммутирующими коэффициентами. Журнал вычислительной математики и математической физики, 47(12):1988–1997, 2007.

[4] *Буртыка Ф. Б.* Симметричное полностью гомоморфное шифрование с использованием неприводимых матричных полиномов. Известия Южного федерального университета. Технические науки, 157(8):107–122, 2014.

[5] *Burtyka P., Makarevich O.* Symmetric fully homomorphic encryption using decidable matrix equations. In Proceedings of the 7th International Conference on Security of Information and Networks, page 186. ACM, 2014.

[6] *Буртыка Ф. Б.* Пакетное симметричное полностью гомоморфное шифрование на основе матричных полиномов. Труды Института системного программирования РАН, 26(5):99–115, 2014.

Южный федеральный университет, Ростов-на-Дону

О P-адических характеристиках элементов P-локальных групп без кручения

С. В. Вершина

Абелева группа без кручения A называется p-локальной группой (p — простое число), если $qA = A$ для любого простого числа $q \neq p$. Обозначим через $\mathbb{Z}_p$ локализацию кольца целых чисел $\mathbb{Z}$ относительно простого числа p. Поле $K \subset \widehat{\mathbb{Q}}_p$ называется полем расщепления [**1**] группы A и кольцо $R = K \cap \widehat{\mathbb{Z}}_p$ называется кольцом расщепления группы A, если $R \otimes_{\mathbb{Z}_p} A \cong D \oplus F$, где D — делимый R-модуль, F — свободный R-модуль. Пусть элемент a группы A имеет нулевую p-высоту в группе A. Внутренней p-адической характеристикой [**2**] элемента a группы A называется множество $H_*(a) = \{\alpha \in \widehat{\mathbb{Z}}_p \mid \alpha a = \lim S_n(\alpha)a \in A\}$, где предел рассматривается в p-адической топологии. Внешней p-адической характеристикой [**3**] $H^*(a)$ элемента A группы A относительно p-базиса $X = \{x_1 = a, \ldots, x_n\}$ назовем внутреннюю p-адическую характеристику элемента $a + \bigoplus_{i=2}^{n} < x_i >$ в фактор-группе $A/\bigoplus_{i=2}^{n} < x_i >$.

Предложение 1. *Пусть A — редуцированная p-локальная группа без кручения, a — элемент нулевой p-высоты, $X = \{x_i\}_{i=1}^{n}$ — p-базис, $W = X \cup Y$ — максимальная линейно независимая система элементов группы A. Тогда:*

(1) *$H_*(a)$ — сервантная подгруппа аддитивной группы кольца $\widehat{\mathbb{Z}}_p$;*
(2) *$H_*(a)a = \{\alpha a \mid \alpha \in H_*(a)\}$ — сервантная подгруппа группы A;*
(3) *$H^*(a)$ — сервантная подгруппа аддитивной группы кольца $\widehat{\mathbb{Z}}_p$;*
(4) *$H_*(a) \subset H^*(a)$;*
(5) *Если $H_*(x_i) = H^*(x_i)$ для $i = 1, \ldots, n$ относительно W, то $A \cong \oplus_{i=1}^{n} A_i$, где $A_i \cong H_*(x_i)$;*
(6) *$\oplus_{i=1}^{n} H_*(x_i)x_i \subset A \subset \oplus_{i=1}^{n} H^*(x_i)x_i$;*
(7) *Если $H^*(x_1) = H^*(x_2) = \ldots = H^*(x_n) = \mathbb{Z}_p$ относительно W, то $A \cong \oplus_n \mathbb{Z}_p$.*

Теорема 1. *Если $H_*(a)$ изоморфна аддитивной группе кольца расщепления R^+, то $H_*(a)a$ является квазислагаемым группы A.*

Теорема 2. *Группа $H^*(a)$ является кольцом расщепления для группы A в том и только том случае, если $H^*(a)$ является подкольцом в $\widehat{\mathbb{Z}}_p$ и $r(H^*(a)) = dim_{\mathbb{Q}} K$.*

Список литер туры

[1] *Lady E. L.* Splitting fields for torsion-free modules over discrete valuation rings, I // Journal of Algebra. — 1977. — Vol. 49(1). — P. 261–275.

[2] *Иванов А. М.* Об одном свойстве p-сервантных подгрупп группы целых p-адических чисел // Математические заметки. — 1980. — Т. 27(6). — С. 859–867.

[3] *Вершина С. В.* Группы расщепления неразложимых p-локальных групп без кручения. // ¡¡Алгебра и логика: теория и приложения¿¿. Материалы международной конференции, посвященной 80-летию В. П. Шункова. — Красноярск, 2013. С. 25–26.

Московский педагогический государственный университет, Москва
E-mail: svetlanavershina@gmail.com

Инварианты действия полупростой алгебры Хопфа на PI-алгебре

М. С. Еряшкин

Пусть H — конечномерная алгебра Хопфа. В статье [**1**] было показано, что коммутативная H-модульная H-полупервичная A цела над своей подалгеброй инвариантов A^H. Это обобщает классический результат теории инвариантов, принадлежащей Э. Нётер, о том, что коммутативная алгебра A является целым расширением подалгебры инвариантов A^G, в случае действия конечной группы G автоморфизмами на алгебре A. Естественным продолжением этого направления исследований является рассмотрение аналогичного вопроса о целостности H-модульной алгебры над подалгеброй инвариантов для H-модульных алгебр, удовлетворяющих полиномиальному тождеству. В работах [**2**] и [**3**] было показано, что алгебра A цела над подалгеброй центральных инвариантов $Z(A)^H$ при выполнении некоторых дополнительных условий для алгебры A. В случае, когда алгебра Хопфа H является полупростой и кополупростой, удалось показать, что некоторые из этих предположений являются излишними.

Теорема. *Пусть H — конечномерная полупростая и кополупростая алгебра Хопфа, A — H-модульная PI-алгебра. Тогда алгебра A цела над подалгеброй инвариантов A^H.*

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований 14-01-31200 и за счет средств субсидии, выделенной Казанскому федеральному университету для выполнения государственного задания в сфере научной деятельности, проект №1.2045.2014.

Список литер туры

[1] *Skryabin S. M.* Invariants of finite Hopf algebras, Advances in Math. **183** (2), 209-239 (2004).
[2] *Еряшкин М. С.* Инварианты и кольца частных H-полупервичных H-модульных алгебр удовлетворяющих полиномиальному тождеству. Изв. вузов. Матем., принята к печати.
[3] *Etingof P.* Galois bimodules and integrality of PI comodule algebras over invariants, arXiv:1306.3821 [math.QA] (2013)

Казанский (Приволжский) федеральный университет, Казань
E-mail: mikhail.eryashkin@gmail.com

Йордановы супералгебры с ассоциативной четной частью.

В. Н. Желябин, А. С. Захаров

Пусть $J = A+M$ — йорданова супералгебра с четной частью A и нечетной частью M. Предположим, что A — ассоциативная алгебра, и M — ассоциативный A-модуль. Рассмотрим $\mathrm{Hom}_A(M, A)$ — A-модуль гомоморфизмов из M в A. Пусть отображение $\phi_{a,x} : M \to A$ задано правилом $\phi_{a,x}(y) = (a, y, x)$, где $(u, v, w) = (uv)w - u(vw)$ — ассоциатор элементов u, v, w. Тогда $\phi_{a,x} \in \mathrm{Hom}_A(M, A)$ и $\phi_{a,x}(y)z = \phi_{a,x}(z)y$ для любых $a \in A, x, y, z \in M$.

Пусть As — изоморфная копия A, и Φ — A-подмодуль в $\mathrm{Hom}_A(M, A)$, содержащий все отображения $\phi_{a,x}$ и удовлетворяющий условию $\phi(x)y = x\phi(y)$ для всех $\phi \in \Phi, x, y \in M$. Рассмотрим векторное пространство

$$J(A, M, \Phi) = (A \oplus As) \oplus (M \oplus \Phi).$$

Определим на $J(A, M, \Phi)$ операцию умножения, полагая

$$(a + bs) \cdot (c + ds) = ac + bd + (ad + bc)s,$$

$$a \cdot x = ax,\ a \cdot \phi = \phi \cdot a = a\phi,\ (as) \cdot \phi = 0,\ (as) \cdot x = \phi_{a,x},$$

$$x \cdot y = xy,\ \phi \cdot x = -x \cdot \phi = \phi(x)s,\ \phi \cdot \psi = 0,$$

где элементы $a, b, c, d \in A, x, y \in M, \phi, \psi \in \Phi$, в правых частях равенств стоит произведение элементов из J, $a\phi$ — A-модульное действие на Φ.

Теорема 1. *Алгебра $J(A, M, \Phi)$ — йорданова супералгебра с четной частью $A + As$ и нечетной $M + \Phi$.*

Если $J = A + M$ — йорданова супералгебра скобочного типа и $\Phi = \mathrm{Hom}_A(M, A)$, то супералгебра $J(A, M, \Phi)$ получается из J с помощью известной конструкции добавления одной нечетной переменной.

Теорема 2. *Пусть йорданова супералгебра $J = A + M$ проста. Тогда супералгебра $J(A, M, \Phi)$ также проста. Если J не является супералгеброй билинейной формы, то $\Phi = \mathrm{Hom}_A(M, A)$. Если J является супералгеброй невырожденной билинейной формы, то A - поле, $\Phi = 0$, $J(A, M, \Phi) = Ae_1 + Ae_2 + M$, где e_1, e_2 — ортогональные идемпотенты.*

Исследование выполнено за счет гранта Российского научного фонда (проект No14-21-00065).

НГУ, ИМ СОРАН, г. Новосибирск
E-mail: antzakh@gmail.com,vicnic@math.nsc.ru

О классификации некоторых классов конечных коммутативных локальных колец

Е. В. Журавлев

Пусть R – коммутативное локальное кольцо характеристики $p = 2$, $J = J(R)$ – радикал Джекобсона кольца R, $R/J(R) = GF(p^r) = F$ – конечное поле и

$$J^4 = 0,\ \dim_F J/J^2 = 2,\ \dim_F J^2/J^3 = 2,\ \dim_F J^3 = 1.$$

Тогда $R = F \oplus Fu_1 \oplus Fu_2 \oplus Fv_1 \oplus Fv_2 \oplus Fw$ и $J = Fu_1 \oplus Fu_2 \oplus Fv_1 \oplus Fv_2 \oplus Fw$, где $\{u_1, u_2, v_1, v_2, w\}$ – отмеченный базис идеала J над полем F (подробнее см. [**1**]), причем $u_1, u_2 \in J \setminus J^2$, $v_1, v_2 \in J^2 \setminus J^3$, $w \in J^3$. Так как $u_iu_j \in J^2$ и u_iv_j, $v_ju_i \in J^3$, то $u_iu_j = a^1_{ij}v_1 + a^2_{ij}v_2 + b_{ij}w$ и $u_iv_j = c_{ij}w$, $v_ju_i = d_{ij}w$ для некоторых a^1_{ij}, a^2_{ij}, b_{ij}, c_{ij}, $d_{ij} \in F$, $i, j = \overline{1,2}$.

Рассмотрим матрицы умножения: $A_1 = \left(a^1_{ij}\right)$, $A_2 = \left(a^2_{ij}\right)$, $B = \left(b_{ij}\right)$, $C = \left(c_{ij}\right)$ и $D = \left(d_{ij}\right)$, $i, j = \overline{1,2}$. Так как R – коммутативное кольцо, то $C = D$, а матрицы A_1, A_2, B являются симметрическими.

Пусть $\delta \in F$, $\forall x \in F\ \delta \neq x + x^2$, и $\mu = a^2c + ac^2 + c^3(1+\delta)$, $\eta = a^3 + ac^2\delta + c^3\delta$,

$$M = \{z \in F \mid \forall s \in \{0,1\}\ \forall a, c \in F,\ a \neq 0 \text{ или } c \neq 0,\ (\eta(1+s) + \mu\delta)z + \eta \neq 0\}.$$

Рассмотрим множество функций $\varphi_{s,a,c} : M \to F$, $\varphi_{s,a,c}(z) = \dfrac{(\eta + \mu s)z + \mu}{(\eta(1+s) + \mu\delta)z + \eta}$, где $s \in \{0,1\}$, $a, c \in F$, $a \neq 0$ или $c \neq 0$. Относительно бинарной операции $(\phi_1 \circ \phi_2)(z) = \phi_1(\phi_2(z))$ $(\phi_1, \phi_2 \in \mathcal{K})$ это множество образует группу, которая действует на множестве M. Пусть $\mathcal{K} \setminus M$ – множество представителей орбит. Пусть также z_0 – такой фиксированный элемент поля F, что $z_0 + 1 \notin F^{*3}$.

Все попарно неизоморфные кольца, описанные выше, определяются следующими пятерками матриц:

$$A_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, C = D = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix};$$

$$A_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, C = D = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix};$$

$$A_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, C = D = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix};$$

$$A_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, C = D = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix};$$

$$A_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & 0 \\ 0 & \delta \end{pmatrix}, B = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, C = D = \begin{pmatrix} 0 & 1 \\ \delta & 0 \end{pmatrix};$$

$$A_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & 0 \\ 0 & \delta \end{pmatrix}, B = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, C = D = \begin{pmatrix} 1 & z \\ 1 + \delta z & 1 \end{pmatrix},\ z \in \mathcal{K} \backslash M;$$

$A_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, $A_2 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, $C = D = \begin{pmatrix} 1 & z \\ 1 & 1 \end{pmatrix}$, где $z = 0$ или $z = 1$ или $z = z_0$.

Список литер туры

[1] *Журавлев Е.В.* Локальные кольца порядка p^6 с 4-нильпотентным радикалом Джекобсона. Сибирские электронные математические известия. [Электронный ресурс]. (2006), №3. Режим доступа: http://semr.math.nsc.ru.

[2] *Corbas B., Williams G.D.* Congruence of two-dimensional subspaces in $M_2(K)$ (characteristic 2). Pacific Journal of mathematics. (1999) v. 188, № 2, p. 237-249.

Алтайский государственный университет, Барнаул
E-mail: evzhuravlev@mail.ru

Тождества векторных пространств, вложенных в конечные ассоциативные алгебры

И. М. Исаев, А. В. Кислицин

Пусть E – векторное пространство над полем F, являющееся подпространством ассоциативной F-алгебры A, причем A порождается пространством E как алгебра (в этом случае будем говорить о векторном пространстве E, вложенном в ассоциативную алгебру A или просто об L-пространстве E). Тождеством L-пространства E назовем ассоциативный многочлен, который обращается в нуль в алгебре A на элементах пространства E.

Класс всех векторных пространств, вложенных в ассоциативные алгебры и удовлетворяющих всем тождествам L-пространства E, будем называть L-многообразием, порожденным L-пространством E и обозначать $\mathrm{Var}_L E$.

В настоящей работе рассматриваются векторные пространства, вложенные в конечные ассоциативные алгебры. Доказано следующее утверждение.

Теорема 1. *Пусть $M_2(F)$ – алгебра матриц второго порядка над конечным полем $F = GF(q)$. Тогда L-многообразие, порожденное $M_2(F)$ как L-пространством, имеет конечное число L-подмногообразий. В частности, любое L-подмногообразие $\mathrm{Var}_L M_2(F)$ имеет конечный базис тождеств по модулю тождеств алгебры $M_2(F)$.*

Отметим, что L-многообразие $\mathrm{Var}_L M_2(F)$ не имеет конечного базиса тождеств [**2**].

Ранее авторами настоящей работы доказано, что тождества L-пространства $E_0 = \langle e_{11} + e_{12}, e_{22}\rangle_F$, вложенного в алгебру $T_2(F)$ верхних треугольных матриц второго порядка, над полем F нулевой характеристики, не имеет конечного базиса тождеств [**1**]. Такие L-пространства мы будем называть НКБ-пространствами. В настоящей работе аналогичное утверждение доказано для случая конечного поля.

Теорема 2. *Векторное L-пространство $E_0 = \langle e_{11} + e_{12}, e_{22}\rangle_F$ над конечным полем $F = GF(q)$ является НКБ-пространством с базисом тождеств*

$$x^{q^2-q+1} - x, St_3(x,y,z), [x,y][u,v], (x-x^q)(y-y^q), [x,y](z-z^q),$$
$$(x-x^q)[y,z], [x,y]z_1z_2\dots z_k[u,v] | k = 1,2,\dots,$$

где $St_3(x,y,z)$ – стандартный многочлен третьей степени.

Следствие 1. *Конечная неассоциативная четырехмерная алгебра $\overline{V} = V \oplus E = \langle v_1, v_2, e_{11} + e_{12}, e_{22}\rangle_{GF(q)}$, ненулевые произведения базисных элементов которой определяются правилом $v_i \cdot e_{ij} = v_j$, не имеет конечного базиса тождеств.*

Ранее был известен пример конечной пятимерной алгебры, не имеющей конечного базиса тождеств [**2, 3**].

Утверждение следствия 1 верно, если алгебру $\overline{V}$ рассматривать как кольцо характеристики p. В частности, верно следующее утверждение:

Следствие 2. *Конечное неассоциативное кольцо характеристики p, порожденное элементами $\{v_1, v_2, e_{11}+e_{12}, e_{22}\}$, ненулевые произведения которых определяются правилом $v_i \cdot e_{ij} = v_j$, не имеет конечного базиса тождеств.*

В случае $p = 2$ получаем кольцо из шестнадцати элементов, не имеющее конечного базиса тождеств.

Список литер туры

[1] *Исаев И. М., Кислицин А. В.* О тождествах пространств линейных преобразований малых размерностей // Тезисы международной конференции по теории колец, посвященной 90-летию со дня рождения А. И. Ширшова (Новосибирск, 14–18 июля 2011 г.). Новосибирск: Институт математики СО РАН. 2011. С. 44–45.

[2] ***Исаев И. М.***, ***Кислицин А. В.*** Тождества векторных пространств и примеры конечномерных линейных алгебр, не имеющих конечного базиса тождеств // Алгебра и логика. 2013. Т. 52. №4. С. 435–460.
[3] ***Исаев И. М.*** Существенно бесконечно базируемые многообразия алгебр // Сибирский математический журнал. 1989. Т. 30. №6. С. 75–77.

Алтайский государственный педагогический университет, Барнаул
E-mail: isaev@uni-altai.ru, kislitsin@uni-altai.ru

Обращение дифференцируемой перестановки над группой

А. В. Карпов

Пусть заданы группа $\mathbb{G}$, записанная аддитивно, с нормальным рядом $\mathbb{G} = H_0 \trianglerighteq H_1 \trianglerighteq \ldots \trianglerighteq H_n = e$ и подмножество $\Psi \subseteq End(\mathbb{G})$ эндоморфизмов группы $\mathbb{G}$, переводящих подгруппы из нормального ряда $\{H_k\}$ в себя.

Определение. Функция $f : \mathbb{G} \to \mathbb{G}$ называется *дифференцируемой* в точке $a \in \mathbb{G}$ относительно нормального ряда $\mathbb{G} = H_0 \trianglerighteq H_1 \trianglerighteq \ldots \trianglerighteq H_n = e$, если существует эндоморфизм $\psi_{f(a)} \in \Psi$, такой что для любого члена нормального ряда H_k и любого элемента $h \in H_k$ выполняется равенство

$$f(a+h) \equiv f(a) + \psi_{f(a)}(h) \pmod{H_{k+1}}.$$

Функция называется дифференцируемой, если она дифференцируема в каждой точке группы $\mathbb{G}$. Эндоморфизм $\psi_{f(a)}$ называется производной функции f в точке a.

Дифференцируемые функции над группой являются обобщением полиномиальных функций над примарным кольцом вычетов $\mathbb{Z}_{p^m}$, где в роли производной выступает умножение на значение формальной производной полинома.

Естественно называть дифференцируемую биективную функцию *дифференцируемой перестановкой.* Будем говорить, что g — *обратная (по модулю H_k)* к f дифференцируемая перестановка, если для всех $x \in \mathbb{G}$ выполняется

$$g(f(x)) = x \quad (g(f(x)) \equiv x \pmod{H_k}).$$

В докладе решается задача нахождение обратной дифференцируемой перестановки к заданной. Это удается сделать, если группа $\mathbb{G}$ — разрешима, и известно промежуточное решение по модулю некоторой подгруппы из нормального ряда. Обратная перестановка строится рекурсивно по следующей теореме.

Теорема. *Пусть f — перестановка элементов разрешимой группы $\mathbb{G}$, дифференцируемая относительно нормального ряда $\mathbb{G} = H_0 \trianglerighteq H_1 \trianglerighteq \ldots \trianglerighteq H_n = e$, g_k — обратная перестановка к f по модулю H_k. Тогда обратной к f по модулю H_{k+1} является перестановка*

$$g_{k+1}(x) = 2g_k(x) - g_k(f(g_k(x))) - [-g_k(x) + g_k(f(g_k(x))), g_k(x)].$$

Следствие. *Если в условиях теоремы группа $\mathbb{G}$ абелева или нильпотентна, то*

$$g_{k+1}(x) = 2g_k(x) - g_k(f(g_k(x))).$$

Томский государственный университет, Томск
E-mail: karpov@isc.tsu.ru

Абсолютные идеалы почти вполне разложимых абелевых групп

Е. И. Компанцева

Кольцом на абелевой группе G называется любое кольцо, аддитивная группа которого совпадает с G. Подгруппы группы G, являющиеся идеалами в любом кольце на G, называют абсолютными идеалами группы G. Изучению абсолютных идеалов абелевых групп посвящены работы Е.Фрида, Л. Фукса, К. Маклина, А. Чехлова, Т. Фам. Главным абсолютным идеалом, порожденным элементом $g \in G$, называется наименьший абсолютный идеал $< g >_{AI}$, содержащий g.

Очевидно, любая вполне характеристическая подгруппа абелевой группы G является ее абсолютным идеалом. В [1] сформулирована проблема изучения абелевых групп, для которых верно обратное утверждение, то есть любой абсолютный идеал является вполне характеристической подгруппой. Такие группы называют afi-группами. В настоящей работе изучаются afi-группы в классе почти вполне разложимых абелевых групп (ПВР-групп). ПВР-группы изучались многими алгебраистами (см., например, [2,3]).

Мы будем рассматривать жесткие ПВР-группы кольцевого типа с циклическим регуляторным фактором (ЦРФ-группы) [3]. Для таких групп определены числа $m_i \in N\,(i = \overline{1,k})$, являющиеся инвариантами почти изоморфизма группы G, при этом при подходящем выборе элементов $e_i\,(i = \overline{1,k})$, принадлежащих регулятору A, любой элемент $g \in G$ однозначно представим в виде $g = \sum_{i=\overline{1,k}} \frac{r_i}{m_i} e_i$, где $r_i \in Q$.

Теорема 1. *Пусть G – жесткая почти вполне разложимая группа кольцевого типа с циклическим регуляторным фактором, $g = \sum_{i=\overline{1,k}} \frac{r_i}{m_i} e_i \in G$. Тогда* $< g >_{AI} = < g > + \bigoplus_{i=\overline{1,k}} r_i A_i$.

Отметим, что строение главного идеала $< g >_{AI}$ в теореме 1 не зависит от выбора элементов e_i, а, следовательно, и от выбора чисел $r_i\,(i = \overline{1,k})$.

Описание главных абсолютных идеалов позволяет доказать, что любая жесткая ЦРФ-группа кольцевого типа является afi-группой.

Теорема 2. *В жесткой ЦРФ-группе кольцевого типа любой абсолютный идеал является вполне характеристической подгруппой.*

Список литературы

[1] *Fried E.* On the subgroups of abelian groups that are ideals in every ring, Proc. Colloq. Abelian Groups, Budapest, 1964, p.51-55.

[2] *Mader A., Schultg P.* Endomorphism rings and automorphism groups of almost completely decomposable groups, Comm. in Algebra, 28, 2000, p.51-68.

[3] *Благовещенская Е. А.* Почти вполне разложимые абелевы группы и их кольца эндоморфизмов, СПб, Изд-во Политехн. ун-та, 2009.

Финансовый университет при Правительстве РФ, Москва;
МПГУ, Москва
E-mail: kompantseva@yandex.ru

Решеточные изоморфизмы конечных однопорожденных колец

С. С. Коробков

Пусть R и R^φ — ассоциативные кольца с изоморфными решётками подколец $L(R)$ и $L(R^\varphi)$ соответственно. Изоморфизм φ решётки $L(R)$ на решётку $L(R^\varphi)$ называется решёточным изоморфизмом (проектированием) кольца R на кольцо R^φ. Кольцо R^φ называется проективным образом кольца R. Свойство алгебры быть однопорождённой (иначе — моногенной) относится к числу основных свойств, рассматриваемых при изучении решёточных изоморфизмов различных алгебр (полугрупп, групп, колец, алгебр над полем). В работе [**1**] доказано, что проективные образы колец Галуа являются однопорождёнными кольцами. О решёточных изоморфизмах однопорождённых конечных колец с единицей сообщалось в [**2**]. Данное сообщение посвящено решёточным изоморфизмам конечных однопорождённых колец, не содержащих единичного элемента. Ниже под p-кольцом (p — простое число) понимается кольцо, аддитивная группа которого является p-группой. Доказаны следующие утверждения:

Теорема 1. *Пусть R — конечное коммутативное ненильпотентное p-кольцо, не содержащее единицы. Кольцо R тогда и только тогда однопорождено, когда R представимо в виде: $R = T \dotplus \langle r\rangle$, где T — ненулевое однопорождённое кольцо, разложимое в конечную прямую сумму колец $T_i = S_i + (r_i)$, при этом $S_i \cong GR(p^{n_i}, m_i)$, r_i — нильпотентный элемент, единичный элемент подкольца S_i является единицей в T_i, r — ненулевой нильпотентный элемент.*

Теорема 2. *Пусть конечное однопорождённое p-кольцо R представимо в виде $R = T_1 \dotplus \cdots \dotplus T_k \dotplus \langle r\rangle$, где $T_i = S_i + (r_i)$, $S_i \cong GR(p^{n_i}, m_i)$, $n_i > 1$, $m_i > 1$, r_i — нильпотентный элемент, единичный элемент подкольца S_i является единицей в T_i $(i = \overline{1,k})$, r — ненулевой нильпотентный элемент. Пусть φ — решёточный изоморфизм кольца R на кольцо R^φ. Тогда справедливы следующие утверждения:*

1) $T_i^\varphi = S_i^\varphi + (r_i')$, $S_i^\varphi \cong S_i$, r_i' — нильпотентный элемент, единичный элемент подкольца S_i^φ является единицей в T_i^φ, $(i = \overline{1,k})$;

2) $(T_i \dotplus \langle r\rangle)^\varphi = T_i^\varphi \oplus \langle r\rangle^\varphi$ $(i = \overline{1,k})$. Кольцо $T_i^\varphi \oplus \langle r\rangle^\varphi$ коммутативно и подкольцо T_i^φ является идеалом в нём;

3) $R^\varphi = (T_1^\varphi \dotplus \cdots \dotplus T_k^\varphi) \oplus \langle r\rangle^\varphi$;

4) $(Rad\, R)^\varphi = Rad\, R^\varphi$;

5) R^φ — однопорождённое p-кольцо.

Список литер туры

[1] *Коробков С.С.* Проектирования колец Галуа // Алгебра и логика. (В печати).

[2] *Коробков С. С.* Проектирования конечных моногенных колец. Международная конференция "Мальцевские чтения-14" 10 - 13 ноября 2014 г., Тезисы докладов. Институт математики им. С.Л. Соболева СО РАН, Новосибирск, с. 107.

Уральский государственный педагогический университет, Екатеринбург
E-mail: ser1948@gmail.com

Об автоморфизме порядка 2 конечного полуполя

О. В. Кравцова

Полуполем называется множество S, на котором определены две бинарные алгебраические операции $+$ и $*$, при выполнении условий:

1) $\langle S,+\rangle$ – абелева группа;

2) $\langle S^*,*\rangle$ – лупа;

3) нейтральный по сложению элемент удовлетворяет условию $0*x=0$ для любого $x\in S$;

4) выполняются дистрибутивные законы $a*(b+c)=a*b+a*c$, $(b+c)*a=b*a+c*a$ для любых $a,b,c\in S$.

Пусть W – линейное пространство размерности n над полем $GF(p)$ (p – простое число). Рассмотрим биективное отображение $\theta : W\to GL_n(p)\cup\{0\}$, удовлетворяющее условиям:

1) $\theta(0,0,\ldots 0)=0$, $\theta(1,0,\ldots,0)$ – единичная матрица;

2) $\theta(y+z)=\theta(y)+\theta(z)$ для любых $y,z\in W$.

Множество $R=\{\theta(y)|y\in W\}$ называют *регулярным множеством.* Введем умножение на множестве W правилом

$$x*y=x\cdot\theta(y),\quad x,y\in W.$$

Тогда $\langle W,+,*\rangle$ – полуполе с нулем $(0,0,\ldots,0)$ и единицей $(1,0,\ldots,0)$. Обратно, любое конечное полуполе может быть представлено линейным пространством при подходящем выборе регулярного множества.

Пусть W – полуполе порядка p^{2n}, представленное линейным пространством над $GF(p)$ с использованием регулярного множества $R\subset GL_{2n}(p)\cup\{0\}$. Обозначим $\pi(W)$ проективную плоскость порядка p^{2n}, координатизируемую полуполем W (*полуполевую плоскость*). Автоморфизм проективной плоскости порядка p^{2n}, поточечно фиксирующий подплоскость порядка p^n, называется *бэровской коллинеацией.*

Теорема 1. *Пусть $\varphi : x\to xA$ – автоморфизм порядка 2 полуполя W, $A\in GL_{2n}(p)$. Тогда матрица $\begin{pmatrix}A & 0\\ 0 & A\end{pmatrix}$ задает бэровскую инволюцию полуполевой плоскости $\pi(W)$.*

Теорема 2. *Пусть π – полуполевая плоскость порядка p^{2n}, допускающая бэровскую инволюцию в трансляционном дополнении. Тогда, с точностью до изотопизма, можно считать, что ее координатизирующее полуполе допускает автоморфизм порядка 2.*

Теорема 3. *Если полуполе порядка p^{2n} допускает автоморфизм порядка 2, то некоторое изотопное ему полуполе содержит подполуполе порядка p^n.*

Работа поддержана РФФИ (грант 15-01-04897 А).

Сибирский федеральный университет, Красноярск
E-mail: ol71@bk.ru

Градуированные алгебры Ли характеристики три с матрицей Картана второго порядка

М. И. Кузнецов, Н. А. Хорева

Важную роль в классификации простых алгебр Ли над алгебраически замкнутым полем F характеристики $p > 0$ играет теорема распознавания В.Г. Каца ([**2**]), доказанная в [**4**] для $p > 3$. Эта теорема дает описание конечномерных транзитивных неприводимых градуированных алгебр Ли L с редуктивной компонентой L_0. Для $p = 3$ список всех градуированных алгебр Ли, удовлетворяющих условиям теоремы распознавания, не известен.

Исследование градуированных алгебр Ли L в [**1**], [**2**], [**4**] в значительной степени основано на локальном анализе, который состоит в рассмотрении подалгебр в L, порожденных элементами $e_i,\ f_i,\ h_i, i = 1, 2$, такими что

$$[e_i,\ f_j] = \delta_{ij}h_i,\ h_i \in H,\ [h_i,\ e_j] = a_{ij}e_j,\ [h_i,\ f_j] = -a_{ij}f_j,\ a_{ij} \in F. \tag{1}$$

Следуя [**3**], обозначим через $\tilde{\mathfrak{g}}(A)$ - алгебру Ли, заданную образующими $e_i,\ f_i,\ h_i$, $i = 1, 2$, и соотношениями (1). Так же, как в [**3**], определяется алгебра Ли $\mathfrak{g}(A)$.

При замене образующих $e_i,\ f_i,\ h_i$ на пропорциональные и при перестановке номеров образующих матрица Картана меняется. Такие матрицы Картана назовем эквивалентными. В данной работе найдены все конечномерные алгебры Ли $\mathfrak{g}(A)$ над алгебраически замкнутым полем F характеристики $p = 3$ и все матрицы Картана, соответствующие бесконечномерным алгебрам Ли.

Предложение. *Пусть A—2×2-матрица. Алгебр Ли $\mathfrak{g}(A)$ над полем характеристки 3 бесконечномерна тогда и только тогда, когда матрица A эквивалентна одной из следующих матриц:*

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ \begin{pmatrix} 2 & a \\ 2 & a \end{pmatrix},\ \begin{pmatrix} 2 & 0 \\ 2 & a \end{pmatrix},\ \begin{pmatrix} 2 & 1 \\ 2 & a \end{pmatrix},\ \begin{pmatrix} 2 & a \\ 2 & 0 \end{pmatrix},\ \begin{pmatrix} 2 & \xi \\ 2 & \eta \end{pmatrix},$$

где $\xi,\ \eta \notin \mathbb{F}_3,\ \xi \neq \eta,\ a \neq 2.$

Работа выполнена в рамках проекта № 1410, фнансируемого Минобрнауки России по госзаданию.

Список литер туры

[1] *Кац В.Г.* Простые неприводимые градуированные алгебры Ли конечного роста // Изв.АН СССР , сер. матем. – 1968.– т. 32. – С. 1323-1367.

[2] *Кац В.Г.* Классификация простых алгебр Ли над полем ненулевой характеристики // Изв. АН СССР , сер. матем. – 1970. – Т. 34. –С. 385-408.

[3] *Кац В.* Бесконечномерные алгебры Ли. М.: Мир. – 1993. – 425 с.

[4] *Benkart G., Gregory T., Premet A.* The Recognition theorem for graded Lie algebras in prime characteristic // Memoirs Amer. Math. Soc. – 2009. – V. 127, N. 920. - 145 p.

Нижегородский госуниверситет им. Н. И. Лобачевского, Нижний Новгород
E-mail: kuznets-1349@yandex.ru

Обобщенный граф делителей нуля ассоциативного кольца

А. С. Кузьмина

Пусть R – ассоциативное кольцо, $D(R)^*$ – множество ненулевых делителей нуля кольца R, $J(R)$ – радикал Джекобсона кольца R, $l(a) = \{x \in R;\ xa = 0\}$, $r(a) = \{x \in R;\ ax = 0\}$ для любого элемента $a \in R$.

Графом делителей нуля $\Gamma(R)$ *кольца* R называется граф, вершинами которого являются все ненулевые делители нуля кольца (односторонние и двусторонние), причем две различные вершины x, y соединяются ребром тогда и только тогда, когда $xy = 0$ или $yx = 0$.

Рассмотрим на множестве $D(R)^*$ следующее отношение эквивалентности σ:

$$a\sigma b \Leftrightarrow r(a) \cup l(a) = r(b) \cup l(b) \text{ для любых элементов } a, b \in D(R)^*.$$

Класс эквивалентности, содержащий элемент a, будем обозначать через $[a]$.

Теорема 1. *Пусть R – ассоциативное конечное кольцо и $a \in D(R)^*$. Если $a^2 = 0$, то $xy = 0$ или $yx = 0$ для любых $x, y \in [a]$. Если $a^2 \neq 0$, то $xy \neq 0$ и $yx \neq 0$ для любых $x, y \in [a]$.*

Рассмотрим *обобщенный граф делителей нуля кольца* R. Вершинами такого графа будем считать все классы эквивалентности $[a]$, где $a \in D(R)^*$, причем две вершины $[a]$ и $[b]$ смежны между собой тогда и только тогда, когда $ab = 0$ или $ba = 0$. Если известно количество элементов в каждом классе эквивалентности, то мы легко можем от обобщенного графа делителей нуля перейти к обычному графу делителей нуля. Таким образом, понятие графа делителей нуля позволяет более просто и компактно строить графы делителей нуля колец больших порядков. Ранее понятие обобщенного графа делителей нуля для коммутативных колец рассматривалось в работах [**1, 2, 3**] и др.

Кроме того, нами доказана

Теорема 2. *Пусть обобщенный граф делителей нуля конечного ассоциативного кольца R состоит из двух вершин. Тогда либо граф $\Gamma(R)$ является полным двудольным, либо кольцо R удовлетворяет одному из следующих условий:*

(1) $R/J(R)$ – поле, кольцо R не содержит единицу и $J(R)^2 = (0)$;

(2) R – локальное кольцо (с единицей), причем $J(R)$ удовлетворяет условию (3) настоящей теоремы;

(3) R – нильпотентное кольцо, $R = A \oplus B$, $B^2 = (0)$, $A^3 = (0)$, A – прямо неразложимое кольцо, не удовлетворяющее тождеству $x^2 = 0$.

Также доказаны некоторые свойства конечных ассоциативных колец, граф делителей нуля которых состоит из трех вершин.

Работа проведена в рамках задания № 2014/418 на выполнение государственных работ в сфере научной деятельности в рамках базовой части государственного задания Минобрнауки России

Список литер туры

[1] *Bloomfield N.* The zero-divisor graphs of commutative local rings of order p^4 and p^5 // Comm. Algebra. – 2013. – 41. – pp. 765–775.

[2] *Levy R., Shapiro J.* The zero-divisor graph of von Neumann regular rings // Comm. Algebra. – 2002. – 30. – pp. 745–750.

[3] *Mulay S. B.* Cycles and symmetries of zero-divisors // Comm. Algebra. – 2002. – 30. – pp. 3533–3558.

Алтайский государственный педагогический университет, Барнаул
E-mail: akuzmina1@yandex.ru

Изоморфизмы колец бесконечных нильтреугольных матриц и присоединенных групп

В. М. Левчук, В. В. Цыганков

Пусть K - ассоциативное кольцо с единицей. Для любой цепи Γ с отношением порядка $<$ кольцо $NT(\Gamma, K)$ всех финитарных Γ-матриц $\parallel a_{ij} \parallel_{i,j\in\Gamma}$ над K с условием нильтреугольности $a_{ij} = 0$ $(i \leq j)$ локально нильпотентно и, следовательно, радикально. Финитарность равносильна тому, что матричные единицы e_{ij} $(i, j \in \Gamma,\ i > j)$ дают базу в алгебре $NT(\Gamma, K)$. Автоморфизмы и изоморфизмы колец $R = NT(\Gamma, K)$, ассоциированных колец Ли $\Lambda(R)$ и присоединенных групп изучены в [**1**] и [**2**], когда $|\ \Gamma\ | < \infty$ или K есть кольцо без делителей нуля.

Оказывается, если Γ есть цепь $Z^{(+)}$ положительных (или $Z^{(-)}$ отрицательных) целых чисел, то все нильтреугольные Γ-матрицы над K дают также радикальное кольцо. Мы переносим методы [**1**] и [**2**] для описания автоморфизмов и изоморфизмов указанных радикальных колец, их ассоциированных колец Ли и присоединенных групп. Далее полагаем $\Gamma = Z^{\{+\}}$ и $R = GNT(\Gamma, K)$. При $i, j \in Z^{\{+\}}$ матрицы из R, у которых в столбцах с номерами $> j$ и в строках с номерами $< i$ стоят нули, образуют идеал в R, обозначаемый через GN_{ij}. Доказаны

Теорема 1. Пусть K - кольцо без делителей нуля. Тогда группы автоморфизмов кольца R, ассоциированного кольца Ли $\Lambda(R)$ и присоединенной группы совпадают. Их порождают автоморфизмы, индуцированные автоморфизмом основного кольца K, внутренние и диагональные автоморфизмы.

Лемма 1. Идеалы $GN_{i+1,i},\ i = 1, 2, 3, \cdots$ исчерпывают все максимальные абелевы идеалы в кольцах R и $\Lambda(R)$, а также максимальные абелевы нормальные подгруппы присоединенной группы.

См. [**4**]. Случай присоединенной группы, когда К - поле порядка ¿ 2, см. [**3**].

Список литер туры

[1] *Левчук В.М.* Некоторые локально нильпотентные кольца и их присоединенные группы. - Математические заметки. 1987. Т.42. No. 5. С. 631-641.

[2] *Kuzucuoglu F., Levchuk V.M.* Isomorphisms of Certain Locally Nilpotent Finitary Groups and Associated Rings. - Acta Applicandae Mathematicae. 82 (2004), 169-181.

[3] *Slowik R.* Bijective maps of infinite triangular and unitriangular matrices preserving commutators. - Linear and Multilinear Algebra. 2013. Vol. 61. No. 8. P. 1028-1040.

[4] *Цыганков В. В.* Максимальные абелевы идеалы кольца обобщенных нильтреугольных матриц. - Материалы междун. конф. студ., аспир. и молодых ученых. СФУ. 2015.

Автоморфизмы нильпотентной подалгебры $N\Phi(K)$ алгебры Шевалле

А. В. Литаврин

В алгебре Шевалле L_K с базисом $\{e_r\ (r \in \Phi),\ \cdots\}$ над полем или кольцом K, ассоциированной с системой корней Φ [**1**, § 4.4], выделяют нильпотентную подалгебру $N\Phi(K)$ с базисом $\{e_r | r \in \Phi^+\}$. Автор изучает автоморфизмы кольца Ли $N\Phi(K)$ классического типа над произвольным ассоциативно-коммутативным кольцом K с единицей, в частности, K-алгебры Ли $N\Phi(K)$.

Алгебра Ли $N\Phi(K)$ типа A_{n-1} изоморфна алгебре Ли, ассоциированной с алгеброй $NT(n, K)$ нижних нильтреугольных $n \times n$ матриц над K. Группы автоморфизмов кольца $NT(n, K)$, его ассоциированного кольца Ли и присоединенной группы (она изоморфна унитреугольной группе $UT(n, K)$) изучены ранее [**2**].

К основным элементарным автоморфизмам кольца Ли $N\Phi(K)$ относим: автоморфизмы индуцированные автоморфизмами основного кольца, диагональные, внутренние, графовые и центральные автоморфизмы. Порождаемые ими автоморфизмы называют стандартными.

В решении проблемы описания группы $Aut\ U$ унипотентных подгрупп U групп лиева типа существенным оказывается следующее обобщение в [**3**] центральных автоморфизмов: *Автоморфизм ϕ группы или кольца Ли, тождественный по модулю m-го гиперцентра и внешний по модулю $(m-1)$-го гиперцентра, называют гиперцентральным автоморфизмом высоты m.*

Для кольца Ли $N\Phi(K)$ типа C_n $(n > 4)$ получено описание группы $Aut\ (N\Phi(K))$.

Теорема 1. *Пусть K – ассоциативно коммутативное кольцо с единицей. Всякий автоморфизм кольца Ли $N\Phi(K)$ симплектического типа C_n $(n > 4)$ есть произведение стандартного и гиперцентрального высоты ≤ 5 автоморфизмов.*

Когда $2K = K$ и аннулятор элемента 3 в кольце K нулевой, автоморфизмы алгебры Ли $NC_n(K)$ $(n \geq 2)$ были описаны ранее [**4**]; наибольшая высота гиперцентральных автоморфизмов в этих случаях ≤ 3. Отметим, что в теореме 1 оценка высоты гиперцентральных автоморфизмов не улучшаемая.

Список литер туры

[1] *Carter R.* Simple groups of Lie type. – New York: Wiley and Sons, 1972.

[2] *Левчук В. М.* Связи унитреугольной группы с некоторыми кольцами. Ч. 2. Группы автоморфизмов / В.М.Левчук // Сибирский математический журнал – 1983 – Т. 24, №4, С. 543-557.

[3] *Левчук В. М.* Автоморфизмы унипотентных подгрупп групп Шевалле / В.М.Левчук // Алгебра и логика – 1990 – Т. 29, №3, С. 316-338.

[4] *Cao Y., Jiang D., Wang D.* Automorphisms of certain nilpotent algebras over commutative rings / Y. Cao, D. Jiang, J. Wang // J. Algebra – 2007 – Vol. 17, no. 3, P. 527-555.

Сибирский федеральный университет, г. Красноярск
E-mail: anm11@rambler.ru

О минимально полных ассоциативных кольцах

Л. М. Мартынов, Т. В. Павлова

Изучается введенное в [**1**] для произвольных (универсальных) алгебр понятие полноты для ассоциативных колец. Приведем необходимые определения применительно к ассоциативным кольцам. Напомним, что атомы решетки L подмногообразий многообразия всех ассоциативных колец исчерпываются многообразиями $\mathcal{F}_p = var\{px = 0, x^p = x\}$ и $\mathcal{Z}_p = var\{px = 0, xy = 0\}$ по всем простым p. Условимся в дальнейшем под *кольцом* понимать *ассоциативное кольцо*. Кольцо называется *полным*, если оно не имеет гомоморфизмов на ненулевые кольца из атомов решетки L. Если кольцо не имеет ненулевых полных подколец, то оно называется *редуцированным*. Ненулевое полное кольцо называется *минимально полным*, если любое его собственное подкольцо является редуцированным. Кольцо, полученное из аддитивной абелевой группы A введением нулевого умножения или заменой умножения кольца A на нулевое умножение, обозначается через A^0.

Предложение. *1) Простое кольцо с единицей является минимально полным тогда и только тогда, когда оно изоморфно либо конечному полю $GF(p^q)$ для некоторых простых чисел p и q, либо кольцу $M_2(GF(p))$ квадратных матриц порядка 2 над простым полем $GF(p)$ для некоторого простого числа p, либо полю $\mathbf{Q}$ рациональных чисел.*

2) Минимально полные нильпотентные кольца исчерпываются кольцом $\mathbf{Q}^0$ и кольцами $\mathbf{C}^0_{p^\infty}$ по всем простым p, где $\mathbf{Q}$ — поле рациональных чисел, а $\mathbf{C}_{p^\infty}$ — аддитивная квазициклическая группа типа p^∞.

Используя эти утверждения и результаты второго автора о полных и редуцированных артиновых (слева) кольцах, доказана

Теорема. *Минимально полные артиновы кольца исчерпываются следующими кольцами:*

1) кольцами с нулевым умножением $\mathbf{C}^0_{p^\infty}$ по всем простым p;

2) полем рациональных чисел $\mathbf{Q}$;

3) конечными кольцами R со свойством $R^2 = R$ с примарной аддитивной группой, для которых радикал Джекобсона $J(R) = pR$ и либо $R/pR \cong GF(p^q)$, либо $R/pR \cong M_2(GF(p))$, где числа p, q — простые.

Исследование выполнено при поддержке Министерства образования и науки Российской Федерации, задание № 2014/336.

Список литературы

[1] *Мартынов Л. М.* О понятиях полноты, редуцированности, примарности и чистоты для произвольных алгебр // Универс. алгебра и ее приложения: Труды межд. семинара. Волгоград: Перемена, 2000. — С. 179–190.

Омский государственный педагогический университет, г. Омск;
Филиал Тюменского государственного университета, г. Ишим
E-mail: l.m.martynov@yandex.ru; pavlova_tanya@bk.ru

Почти конечномерные альтернативные алгебры

А. С. Панасенко

Определение. Алгебра A называется почти конечномерной, если $dim(A) = \infty$ и $dim(A/I) < \infty$ для любого ненулевого $I \trianglelefteq A$.

Пример. Пусть $\mathcal{C}$ — алгебра Кэли-Диксона над полем F, т.е. центр $Z(\mathcal{C}) = F$, $F[x]$ — кольцо многочленов от переменной x. Тогда тензорное произведение $\mathcal{C} \otimes_F F[x]$ — почти конечномерная алгебра.

Доказаны следующие теоремы

Теорема 1. *Всякая почти конечномерная альтернативная алгебра первична.*

Теорема 2. *Пусть A — кольцо Кэли-Диксона с единицей. Предположим, что A — почти конечномерная алгебра. Тогда ее центр $Z(A)$ — почти конечномерная алгебра, A является локально конечной над своим центром $Z(A)$. Алгебра A содержит подалгебру B, которая является конечно порожденным $Z(A)$-модулем, $Z(B) = Z(A)$ и $(Z^*)^{-1}A = (Z^*)^{-1}B$. Более того, алгебра B — почти конечномерна.*

Теорема 3. *Пусть A — исключительная почти конечномерная алгебра. Тогда A является локально конечномерной. Если $\mathcal{L}(A) \neq A$, то A — алгебра с единицей, ее центр $Z(A)$ — конечномерное над F поле и A — локальная алгебра с наибольшим идеалом $\mathcal{L}(A)$.*

Теорема 4. *Конечно-порожденная альтернативная неассоциативная почти конечномерная алгебра A над полем F является кольцом Кэли-Диксона. Если, к тому же, F — несчетно, то A — подпрямое произведение алгебр Кэли-Диксона.*

Работа выполнена при поддержке фонда РФФИ, проект 14-01-00014.

Новосибирский государственный университет, Новосибирск
E-mail: tom-anjelo@mail.ru

Коммутаторная ширина элементов однородных метабелевых алгебр Ли

Е. Н. Порошенко

Пусть $\mathbb{F}$ — алгебраически замкнутое поле характеристики нуль, обладающее следующим свойством:

(∗) существует алгоритм, позволяющий для любой конечной системе над $\mathbb{F}$ установить, совместна ли эта система.

Обозначим через $M(A)$ свободную метабелеву алгебру с множеством порождающих $A = \{a_1, a_2, \ldots, a_n\}$ над алгебраически замкнутым полем $\mathbb{F}$ характеристики 0, обладающим свойством (∗). Через $M(A; S)$ будем обозначать метабелеву алгебру Ли с множеством порождающих A и множеством определяющих отношений S. Производные алгебр $M(A)$ и $M(A; S)$ будем обозначать $M'(A)$ и $M'(A; S)$ соответственно.

Определение 1. *Пусть $\alpha[u]$ — неассоциативный моном от элементов множества A ($\alpha \in \mathbb{F}$).* Мультистепень *монома $\alpha[u]$ — это вектор $\overline{\delta} = (\delta_1, \delta_2, \ldots, \delta_n)$, где δ_i — это число вхождений a_i в $[u]$.*

Определение 2. *Неассоциативный многочлен f называется* однородным, *если мультистепени всех его мономов равны.*

Определение 3. *Алгебра $M(A; S)$ называется* однородной, *если S состоит из однородных многочленов.*

Определение 4. *Пусть L — произвольная алгебра Ли.* Коммутаторной шириной *элемента $g \in L'$ называется наименьшее число k, такое что для некоторых $h_1, \ldots, h_k, h'_1, \ldots, h'_k \in L$ выполняется равенство $g = \sum_{s=1}^{k} [h_s, h'_s]$.*

В алгебры Ли понятие коммутаторной ширины пришло из групп, где, в свою очередь, произошло из понятия ширины, введенного Мерзляковым в [**1**]. В [**2**] было доказано, что для любого элемента $g \in M'(A)$ задача нахождения коммутаторной ширины этого элемента является алгоритмически разрешимой.

Основным результатом данной работы является следующая теорема.

Теорема. *Пусть $\mathbb{F}$ — алгебраически замкнутое поле характеристики нуль, удовлетворяющее свойству (∗) и пусть $M(A; S)$ — свободная метабелева алгебра Ли над полем $\mathbb{F}$. Задача нахождения коммутаторной ширины любого элемента $g \in M'(A; S)$ является алгоритмически разрешимой.*

Работа выполнена при финансовой поддержке РФФИ (грант 15–01–01485), а также Министерства образования и науки РФ (гос. задание № 214/138, проект 1052).

Список литературы

[1] *Мерзляков Ю. И.* Рациональные группы, изд. 2-е, М: Наука, 1987.

[2] *Порошенко Е. Н.* Коммутаторная ширина элементов свободной метабелевой алгебры Ли, Алгебра и логика, **53**, 5 (2014), 587–613.

Новосибирский государственный технический университет, Новосибирск
E-mail: auto_stoper@ngs.ru

Инкапсулированные кольца и их приложения в криптографии

А. В. Трепачева

Инкапсулированные (black-box) представления алгебраических структур помогают оценить сложность алгоритмов вне зависимости от их конкретного представления [**1, 2, 3**]. Для анализа криптостойкости полностью гомоморфного шифрования, основанного на факторизации чисел, хорошо подходит следующая структура.

Определение 1. *Инкапсулированное кольцо – это шестерка (n, k, h, F, G, T) в которой $n \in \mathbb{N}$ – определяет количество элементов в кольце, $k \in \mathbb{N}$ – определяет длину битового представления кодировки. Функции h, F, G, T определены следующим образом.*

(1) *Функция $h : \{0,1\}^k \to \mathbb{Z}_n$ сопоставляет элемент из кольца каждой k-битной двоичной строке. Функция h сюръективна, т. е. каждый элемент кольца представлен по меньшей мере одной битовой строкой.*

(2) *Функции $F, G : \{0,1\}^k \times \{0,1\}^k \to \{0,1\}^k$ выполняют сложение и умножение. Они удовлетворяют следующим соотношениям $h(F(x,y)) = h(x) + h(y)$ и $h(G(x,y)) = h(x)h(y)$.*

(3) *Функция $T : \{0,1\}^k \times \{0,1\}^k \to \{\mathtt{true}, \mathtt{false}\}$ проверяет равенство двух инкапсулированных элементов: $T(x,y) = \mathtt{true}$ тогда и только тогда, когда $h(x) = h(y)$.*

Определение 2. *Пусть(n, k, h, F, G, T) – инкапсулированное кольцо. Обозначим отображение, сопоставляющее элементу x некоторое представление $[x]$ как $[]$.* ***Проблема инкапсулированного кольца*** *состоит в следующем: найти алгоритм $\mathcal{A}$ который по данному n и оракулам $F, G, T, []$ и представлению $\alpha \in \mathbb{Z}_n$ находит α в явном виде.*

В работе изучается сложность алгоритмов решения проблемы инкапсулированного кольца при различных ограничениях на кольцо, а также показывается ее влияние на криптостойкость соответствующих алгебраически гомоморфных шифров.

Работа выполнена при поддержке гранта РФФИ №15-07-00597 А.

Список литер туры

[1] *Arvind V., Das B., Mukhopadhyay P.* The complexity of black-box ring problems. In *Computing and Combinatorics*, pages 126–135. Springer, 2006.

[2] *Boneh D., Lipton R. J.* Algorithms for black-box fields and their application to cryptography. In *Advances in Cryptology-CRYPTO'96*, pages 283–297. Springer, 1996.

[3] *Zumbragel J., Maze G., Rosenthal J.* Efficient recovering of operation tables of black box groups and rings. In *Information Theory, 2008. ISIT 2008. IEEE International Symposium on*, pages 639–643. IEEE, 2008.

Южный федеральный университет, Ростов-на-Дону
E-mail: alina1989malina@ya.ru, atrepacheva@sfedu.ru

О кольцах расщепления P-локальных абелевых групп без кручения

В. Х. Фарукшин

Пусть подполе K поля p-адических чисел $\widehat{\mathbb{Q}}_p$ является конечным алгебраическим расширением поля рациональных чисел $\mathbb{Q}$ и полем расщепления редуцированной p-локальной абелевой группы без кручения A конечного ранга.

Теорема. *Если $\{a_0 = 1, a_1, \dots, a_k\}$ — фундаментальный базис кольца целых чисел $\mathcal{O}_K$ поля расщепления K группы A, то сервантная оболочка $\langle a_0 = 1, a_2, \dots, a_k\rangle$ в аддитивной группе кольца целых p-адических чисел $\widehat{\mathbb{Z}}_p$ является кольцом расщепления группы A.*

Московский педагогический государственный университет, Москва
E-mail: fvkh@mail.ru

Свойства многообразия, порожденного матричной супералгеброй $M_{1,1}(G)$

О. Б. Финогенова

Пусть F — конечное или бесконечное поле характеристики, не равной 2. Всюду далее рассматриваются ассоциативные алгебры над полем F. Для алгебры A будем обозначать через A^1 алгебру с присоединенной единицей, через $T(A)$ — идеал тождеств A, а через $\mathsf{var}A$ — многообразие, порожденное A. Алгеброй Грассмана G счетного ранга называется алгебра $\langle e_1, e_2, \dots \mid e_i^2 = 0, e_ie_j = -e_je_i\rangle$. Легко видеть, что $G = G_0 \oplus G_1$, где G_0 и G_1 — подпространства, порожденные всеми словами четной или соответственно нечетной длины. Обозначим через $M_{1,1}(G)$ алгебру матриц вида $\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, d \in G_0,\ b, c \in G_1\right\}$. Аналогично можно определить $M_{1,1}(G^1)$, считая, что $a, d \in G_0 + F \cdot 1$.

Теорема 1. $T(M_{1,1}(G)) = T(G \otimes G)$.

В случае поля нулевой характеристики этот факт следует из равенства $T(M_{1,1}(G^1)) = T(G^1 \otimes G^1)$ ([**1**]). Отметим, что в случае поля положительной характеристики $T(M_{1,1}(G^1)) \neq T(G^1 \otimes G^1)$ (см. [**2**]).

Теорема 2. *Пусть $\mathcal{V}$ — собственное подмногообразие многообразия $\mathsf{var}M_{1,1}(G)$.*

(1) *$\mathcal{V}$ удовлетворяет тождеству вида $[x_1, y_1, z_1][x_2, y_2, z_2] \cdots [x_n, y_n, z_n] = 0$ при некотором n.*

(2) *$\mathcal{V}$ удовлетворяет тождеству вида $[x_1, y_1][x_2, y_2] \cdots [x_m, y_m] = 0$ для некоторого m, тогда и только тогда, когда не содержит алгебру G.*

В случае поля нулевой характеристики Теорема 2 доказана А. Кемером ([**3**]). Л. Самойловым в [**4**] установлено (1), если F — бесконечное поле положительной характеристики, и $T(\mathcal{V}) \setminus T(M_{1,1}(G))$ содержит полилинейное тождество.

Работа выполнена в рамках реализации базовой части госзадания на выполнение НИР (проект №2248 Министерства образования и науки РФ), поддержана грантом Президента РФ для поддержки ведущих научных школ Российской Федерации (проект НШ-5161.2014.1) и грантом РФФИ №14-01-00524.

Список литературы

[1] *Кемер А. Р.* Многообразия и $\mathbb{Z}_2$-градуированные алгебры, Изв. АН СССР. Сер. матем., **48(5)** (1984), 1042-1059.

[2] *Azevedo S. S., Fidelis M., Koshlukov P.* Tensor product theorems in positive characteristic, J. Alg. **276(2)** (2004), 836-845.

[3] *Кемер А. Р.* Нематричные многообразия, Алгебра и логика, **19** (1980), 255–283.

[4] *Самойлов Л. М.* О полилинейных компонентах первичных подмногообразий многообразия $\mathsf{var}(M_{1,1})$, Матем. заметки, **87(6)** (2010), 919-933.

Уральский федеральный университет, Екатеринбург
E-mail: ob.finogenova@urfu.ru

Weak σ-rigid rings and their extensions over Noetherian rings

V. K. Bhat

Let R be an associative ring with identity $1 \neq 0$, and σ an endomorphism of R. We recall $\sigma(*)$ property on R (i.e. $a\sigma(a) \in P(R)$ implies $a \in P(R)$ for $a \in R$, where $P(R)$ is the prime radical of R). Also recall that a ring R is said to be 2-primal if $P(R) = N(R)$, where $N(R)$ is the set of nilpotent elements of R, i.e. if the prime radical is a completely semiprime ideal. It can be seen that a $\sigma(*)$ ring is a 2-primal ring.

We recall that a ring R with an endomorphism σ is said to be a weak σ-rigid ring if $a\sigma(a) \in N(R)$ if and only if $a \in N(R)$ for $a \in R$.

In this paper we give a relation between a $\sigma(*)$-ring and a weak σ-rigid ring. We also give a necessary and sufficient condition for a Noetherian ring to be a weak σ-rigid ring.

Let now R be a ring and σ an automorphism of R. Then we know that σ can be extended to an automorphism (say $\overline{\sigma}$) of the skew polynomial ring $R[x;\sigma]$. In this paper we show that if R is a Noetherian ring and σ is an automorphism of R such that R is a weak σ-rigid ring, then $R[x;\sigma]$ is also a weak $\overline{\sigma}$-rigid ring.

School of Mathematics, SMVD University, Katra (India)
E-mail: vijaykumarbhat2000@yahoo.com

Coverings and fundamental groups of noncommutative spaces

Clarisson Rizzie Canlubo

The notion of the fundamental group is a very important and powerful invariant in topology. The topological formulation of the fundamental heavily depends on the fine structure of the topological space. This does not generalize well in algebraic geometry since algebraic curves are very rigid objects, even worse is in noncommutative geometry where there are no spaces to work with, in particular, there are no curves. The algebraic geometric formulation of the fundamental group due to Grothendieck on the other hand makes use of Galois theory for coverings. This is a more useful formulation and this is the path that we are going to explore to define covering spaces and fundamental groups of noncommutative spaces. In the spirit of noncommutative geometry, groups turn into quantum groups and spaces are replaced by algebras. With this, the fundamental group of a noncommutative space A is a quantum group satisfying a universal property while the corresponding covering space is a Hopf-Galois extension of A. In this talk, we will present some results that generalize those from classical geometry and some that do not. We will also look at some very interesting examples.

University of Copenhagen, Denmark
E-mail: clarisson@math.ku.dk

An algorithm for determining the irreducible polynomials over finite fields

Samuel H. Dalalyan

We propose an algorithm for determining the irreducible polynomials over finite fields, based on the use of the multiplicative order (abbreviate as m.o.) of the companion matrix of polynomials and the generalized Jordan normal form of square matrices.

Theorem. *Let $\mathbf{F} = \mathbf{F}_q$ be a finite field, where $q = p^n$, p is a prime, n is a positive integer. Let $f(t)$ be a unitary polynomial over $\mathbf{F}$ with a non-zero free term, $[f]$ be its companion matrix and $d = deg\, f(t)$, $m = ord\, f(t) = m.o.[f]$. Then the following assertions are true:*

1) $m \leq q^d - 1$ and $m = q^d - 1$ if and only if $f(t)$ is a primitive irreducible polynomial;

2) more generally, $f(t)$ is an irreducible polynomial if and only if p is not a divisor of m, $d = m.o.q(mod.m)$ and $rk([f]^l - E) = d$ for all positive integers $l < m$, diviving m, where E is a unit matrix.

Algorithm for finding the irreducible polynomials over a finite field.

Suppose that $f(t)$ is a unitary polynomial of a degree d over a finite field $\mathbf{F} = \mathbf{F}_q$ with a nonzero free term.

1. Construct the companion matrix $[f]$ of $f(t)$.
2. Compute $[f]^l$, $l = 2, 3, ...$ and find $m = m.o.[f]$. Then $m \leq q^d - 1$ and $m = q^d - 1$ if and only if $f(t)$ is a primitive irreducible polynomial.
3. Suppose that $m < q^d - 1$ and m is not a multiple of p. Then compute $q^l(mod.m)$, $l = 2, 3, ...$ and find $e = m.o.q(mod.m)$. The polynomial $f(t)$ is reducible if if $e \neq d$.
4. Calculate $r = rk([f]^l - E)$ for divisors $l_1 < l_2 < ...$ of m. If for a divisor $l < m$ of m the rank $r < d$, then the polynomial $f(t)$ is reducible. Otherwise, $f(t)$ is an irreducible polynomial.

Yerevan State University (Armenia)
E-mail: dalalyan@ysu.am

On projectively Krylov transitive Abelian p-groups

P. V. Danchev, A. R. Chekhlov

Recall that an abelian p-group G is called (fully) transitive if for all $x, y \in G$ with $U_G(x) = U_G(y)$ ($U_G(x) \leqslant U_G(y)$), where $U_G(g)$ denotes the Ulm sequence of the element $g \in G$, there exists an automorphism (endomorphism) of G which maps x onto y.

Definition 1. A group G is said to be *projectively Krylov transitive* if, given $x, y \in G$ with $U_G(x) = U_G(y)$, there exists $f \in Proj(G)$ with $f(x) = y$, where $Proj(G)$ is the subring of the endomorphism ring $E(G)$ of the group G generated by the idempotents of $E(G)$.

Definition 2. A group G is called *projectively transitive* if, given $x, y \in G$ with $U_G(x) = U_G(y)$, there exists $f \in Aut(G) \cap Proj(G)$ with $f(x) = y$, where $Aut(G)$ is the automorphism group of the group G.

Proposition 1. *If G is a p-group with $p \neq 2$, then G is projectively Krylov transitive if, and only if, G is projectively fully transitive.*

Proposition 2. *Any projectively Krylov transitive group G for which $p^\omega G$ is a direct sum of two cyclic groups, is fully transitive.*

Theorem 1. *There exists a projectively Krylov transitive 2-group G which is not projectively fully transitive and such that $2^\omega G$ is a direct sum of three cyclic groups.*

Theorem 2. *There exists a Krylov transitive group which is not projectively Krylov transitive.*

Plovdiv State University, Plovdiv, Bulgaria;
Tomsk State University, Tomsk, Russia.
E-mail: pvdanchev@yahoo.com; cheklov@math.tsu.ru

Free associative averaging algebra and homomorhic averaging operators

V. Yu. Gubarev

A linear operator T defined on an algebra A is named averaging operator if the following equalities are hold

$$T(x)T(y) = T(xT(y)) = T(T(x)y), \quad x, y \in A. \tag{1}$$

In [1] free associative averaging algebra was constructed. The construction uses direct limits and *averaging words* which one can consider as elements of free associative algebra generated on set X with linear operator T. By definition, an averaging word doesn't contain subwords of kind $T(u)T(v)$, $T(T(u)v)$ and $T(uT^2(v))$.

Let us introduce good words in free associative algebra with linear operator T generated by X $F_T^{\mathrm{Ass}}\langle X\rangle$ by induction (for monomials u, u_1, u_2 on X):
— u and $T(u)$ are good words;
— if v is good word of the form $T(w)$ or u_1wu_2, then $T(v)$ is good word; if v_1, v_2 are good words, then v_1v_2 is good word if there isn't a subword of kind $T(w_1)T^2(w_2)$ in the joint of words v_1 and v_2;
— there are no another good words.

Given monomial v from $F_T^{\mathrm{Ass}}\langle X\rangle$ let denote by $\overline{v}$ such monomial that $\overline{v}$ doesn't contain subword of kind $T(u)T^2(w)$; $v = \overline{v}$ in $F_T^{\mathrm{Ass}}\langle X \mid T(x)T^2(y) = T^2(x)T(y)\rangle$.

The set of good words on X generates a space B in $F_T^{\mathrm{Ass}}\langle X\rangle$. Let us define multiplication on B as $v_1 \cdot v_2 = \overline{v_1v_2}$ and action of linear operator S on B as

$$S\colon u \to T(u), \quad u_1vu_2 \to T(u_1vu_2), \quad v_1T(v_2), T(v_1)v_2 \to \overline{T(v_1)T(v_2)}.$$

Theorem 1. Algebra B with multiplication $\cdot$ and linear operator S is free associative averaging algebra on X.

Averaging operator T on A is called homomorphic [2] if it satisfies additionally to (1) an equality

$$T(x)T(y) = T(xy), \quad x, y \in A. \tag{2}$$

Theorem 2. *a) Let A be a simple algebra, then any homomorphic averaging operator on A is either zero or identity map.*

b) Let A be a semiprime algebra, then any homomorphic averaging operator on A is zero on an ideal $I = \ker T \lhd A$ and identity map on A/I.

The work is supported by Russian Science Foundation (project 14-21-00065).

References

[1] *Guo L., Pei J.* Averaging algebras, Schröder numbers, rooted trees and operads, J. Algebr. Comb., DOI: 10.1007/s10801-014-0574-x.

[2] *Gubarev V. Yu., Kolesnikov P. S.* Operads of decorated trees and their duals, Comment. Math. Univ. Carolin., **55**:4, 2014, 421–445.

Sobolev Institute of Mathematics of SB RAS, NSU, Novosibirsk
E-mail: wsewolod89@gmail.com

Simple finite-dimensional noncommutative Jordan superalgebras

A. P. Pozhidaev, I. P. Shestakov

Let $U = U_{\bar{0}} \oplus U_{\bar{1}}$ be a superalgebra, $U_{\bar{i}}U_{\bar{j}} \subseteq U_{\overline{i+j}}$, $i, j \in \mathbb{Z}_2$, $(-1)^{xy} := (-1)^{p(x)p(y)}$, where $p(x)$ is the parity of x ($p(x) = i$, if $x \in U_{\bar{i}}$); $L_x(y) := xy$, $R_x(y) := (-1)^{xy}yx$, $x \circ y := xy + (-1)^{xy}yx$.

A superalgebra U is called a *noncommutative Jordan superalgebra* provided that the operator identities

$$[R_{x\circ y}, L_z] + (-1)^{x(y+z)}[R_{y\circ z}, L_x] + (-1)^{z(x+y)}[R_{z\circ x}, L_y] = 0,$$
$$[R_x, L_y] = [L_x, R_y]$$

hold for all $x, y, z \in U$.

The class of noncommutative Jordan superalgebras is extremely extensive: it includes the alternative superalgebras, the Jordan superalgebras, the quasi-associative superalgebras, the quadratic flexible superalgebras and the superanticommutative superalgebras.

We classify the simple central finite-dimensional noncommutative Jordan superalgebras.

Theorem. *Let U be a finite-dimensional central simple noncommutative Jordan superalgebra over a field F, which is neither quasi-associative nor supercommutative. Then either*

(i) $U \cong K_3(\alpha, \beta, \gamma)$,

(ii) $U \cong M_{1,1}(F)(\alpha, \beta)$, $osp(1,2)^q$, $J(\Gamma_n, A)$, $\Gamma_n(D)$, $(B(m,n) + B(m,n)x, \{,\})$, $(V_{1/2}(Z,d), \{,\})$, $B(m,n)(D)$,

or there exists an extension P of F of degree 1 or 2 such that $U \otimes_F P$ is isomorphic as a superalgebra over P to one of the following:

(iii) $D_t(\alpha)$,

(iv) $U(V, f, \star)$.

The authors were supported by FAPESP 2014/ 13271-5 and the first author was partially supported by RFBR (grant 14-01-00014).

VI. Секция «Теория моделей и универсальная алгебра»

О распределении числа счетных моделей теорий ациклических графов

К. А. Байкалова

Определение [**1**]. Модель M теории T называется *предельной*, если M не является простой моделью ни над каким кортежем и $M = \bigcup\limits_{n\in\omega} M_n$ для некоторой элементарной цепи $(M_n)_{n\in\omega}$ простых моделей теории T над некоторыми кортежами.

Для счетной полной теории T мощности множеств типов изоморфизма простых над кортежами, предельных и остальных счетных моделей этой теории обозначим через $P(T)$, $L(T)$ и $\mathrm{NPL}(T)$ соответственно.

Определение [**1, 2**]. Набор $(P(T), L(T), \mathrm{NPL}(T))$ называется *тройкой распределения счетных моделей теории* T и обозначается через $cm_3(T)$.

На основе результатов из [**3**] была получена следующая теорема.

Теорема. *Пусть T — полная теория ациклического графа, не имеющая конечных моделей. Тогда $cm_3(T)$ принимает одно из следующих значений:*

(1) $(1, 0, 0)$,
(2) $(\omega, 1, 0)$,
(3) $(\omega, \omega, 0)$,
(4) $(\omega, 2^\omega, 0)$,
(5) $(2^\omega, 2^\omega, 0)$.

Данные исследования поддержаны грантом КН МОН РК № 0830/ГФ4.

Список литературы

[1] *Судоплатов С. В.* Классификация счетных моделей полных теорий. Ч.2. — Новосибирск: Изд-во НГТУ, 2014. — 448 с.

[2] *Popkov R. A., Sudoplatov S. V.* Distributions of countable models of complete theories with continuum many types // arXiv:1210.4043v1 [math.LO]. — 2012. — 30 p.

[3] *Байкалова К. А.* Предельные модели теории унаров // Вестник Омского университета. Омск: Издательство ОмГУ им. Ф.М. Достоевского 2014. № 2. С. 10-14.

Новосибирский государственный технический университет, Новосибирск
E-mail: bkristina@bk.ru

Некоторые классы теорий с позиции B-подобия моделей

М. И. Бекенов

Рассматривается фактор-класс относительно отношения B-подобия класса бесконечных моделей счетного языка первого порядка L. Отношение элементарной вложимости моделей индуцирует отношение порядка на этой фактор-алгебраической системе $[{K_L}^B, \leq_B]$, являющейся объединением всевозможных непересекающихся B-деревьев [**1**]. B-деревья соответствуют полным теориям. Каждый элемент дерева является его порождающим. При классификации теорий можно акцент делать на ω-подсистемы или μ-подсистемы, т.е. у подсистемы делать срез на модели мощности ω или μ [**1**].

Например, наряду с классом конечно порожденных теорий [**1**], выделяется класс теорий T, у которых $B_T(\omega) < \omega$. Если принимать во внимание операцию прямого произведения моделей теорий, то очерчивается подкласс теорий, у которых соответствующие этим теориям ω-подсистемы одноэлементные, или например класс теорий, у которых соответствующие этим теориям ω-подсистемы конечны. Наряду с объединением и пересечением теорий рассматривается прямое произведение теорий с позиций подсистем.

Список литературы

[1] *Бекенов М. И.* B-алгебраические системы теорий, Мальцевские чтения, Новосибирск, 2014

Евразийский Национальный Университет им. Л.Н.Гумилева, Астана
E-mail: bekenov50@mail.ru

О богатых семействах типов в многосортных системах и кластеризации типов в логических исчислениях

А. А. Викентьев

Доклад посвящен *обобщению и уточнению результатов и теорем о богатых семействах типов,* доказанных ранее в стабильном случае или с условиями стабильности[1] *на случай богатых семейств типов с параметрами для многосортных теорий с $\varkappa$–компактными (насыщенными, однородными) измеримыми моделями и свойством $\varkappa$–отделимости новых элементов, реализующих типы (над малыми подмножествами) из этих семейств, от элементов меньшей модели и наличия реализаций в большей (с богатым семейством) модели вполне определимых (стабильных) типов или неразличимых элементов. Стабильность теорий не предполагается, а известные теоремы получаются как следствия.*

Основными инструментами доказательств являются теоремы типа компактности, развитая техника современной теории моделей, в частности, для логических исчислений, локальной стабильности (Шелах, Лахлан, Балдвин, Пуаза, Пиллай, Хрушовский, Невельский, Бен Яков, Зильбер, Палютин, Судоплатов, Перетятькин, Морозов, Еримбетов, Кудайбергенов, Байжанов и многих др.) и наличия (даже локально) подходящих компактных измеримых (нужных мощностей $\varkappa$) моделей теории со свойствами $\varkappa$–отделимости над реализациями семейств стабильных (определимых) типов. Продолжено изучение предельных и двукардинальных моделей в классе теорий с покрытиями. Рассмотрены вопросы определимости систем с метрикой в наследственно конечных надстройках, и о мощностях типово определимых подмножеств и их двукардинальности. Интерес к этим вопросам и моделям имеет и прикладной характер в поиске наиболее информативных (нетривиальных) типов, логических закономерностей для кластеризации и упорядочения таких знаний с помощью привлечения метрических или измеримых систем. Все это служит для введения новых метрик на классах эквивалентных типов на измеримых подклассах измеримых (метрических) моделей, необходимых для разработки алгоритмов распознавания образов, поиска закономерностей, обнаружения аномальных событий и кластеризации многозначных формул–знаний. Найдены различные новые метрики и методы кластеризации для множеств формул в различных логиках и их индексы качества для сравнений. Проведены модельные эксперименты. Работа выполнена при финансовой поддержке РФФИ, проекты № 14–07–00851а, 14–7–00249а, кафедры ДМИ ММФ НГУ.

Институт математики СО РАН, Новосибирск
E-mail: vikent@math.nsc.ru

[1] Некоторые из них вошли в диссертацию автора “Теории с покрытием и формульные подмножества”, ИМ СО РАН, Новосибирск, 1992 г., 134 с. для семейств формул, а также опубликованы в сборнике, посвященному 90–летию академика А.Д. Тайманова — “Two cardinal theorems for sets of types in stable theory”, Казахстан, Алма–Ата, 2007, с. 67–69, были доложены Алма–Ате и Новосибирске — на ежегодных Мальцевских чтениях с 2006 г., в том числе к 100–летию акад. А.И. Мальцева и др.

Кластеризация многозначных логических высказываний с учетом новых расстояний и мер нетривиальностей

А. А. Викентьев, Р. А. Викентьев

В работе рассматривается одна из актуальных задач — анализ логических высказываний из базы знаний или полученных от экспертов. При анализе требуется найти близкие высказывания, выявить достоверные, найти нетривиальные и т.д. Для кластеризации знаний, построения решающих функций на основе формул-высказываний, надо ввести расстояние между формулами. В работе высказывания записаны в виде формул n–значной логики. С привлечением теории моделей определяются новые расстояния между формулами, обобщая множество возможных коэффициентов

$$\rho(\varphi,\psi)=\frac{1}{n^{|S(\Sigma)|}}\sum_{k=0}^{n-1}\sum_{l=0}^{n-1}\frac{|k-l|}{n-1}\,M\left(\frac{k}{n-1},\frac{l}{n-1}\right), \tag{1}$$

где $n^{|S(\Sigma)|}$ - количество всех моделей, $M\left(\frac{k}{n-1},\frac{l}{n-1}\right)$ - тех моделей, на которых формула φ принимает значение $\frac{k}{n-1}$, а ψ — $\frac{l}{n-1}$; и также новые меры нетривиальности обобщающие

$$I(\varphi)=\rho(\varphi,1)=\frac{1}{n^{|S(\Sigma)|}}\sum_{k=0}^{n-2}\frac{n-1-k}{n-1}\,M\left(\frac{k}{n-1}\right), \tag{2}$$

где $M\left(\frac{k}{n-1}\right)$ - количество моделей, на которых формула φ принимает значение $\frac{k}{n-1}$. Доказаны необходимые свойства введенных семейств мер. Отдельно рассматриваем и меру пересечения моделей для рассматриваемых пар формул. В работе исследованы и доказаны свойства метрики для введенных расстояний и мер нетривиальности; они учитывают многозначность, схожи со свойствами величин в случае 2– и 3–значных логик Лукасевича, и известных расстояний в общем случае, отвечают на вопросы Г.С. Лбова и применяются для алгоритмов кластеризации формул. Рассмотрены различные методы кластеризации знаний на основе новых расстояний и мер нетривиальности, а также методы сравнения результатов на основе введенных индексов качества кластеризации. Мера значений истинности формулы на модели первого порядка может служить степенью нетривиальности (недостоверности) формулы. Результаты распространяются на многозначные формулы первого порядка со свободными переменными. Все результаты переносятся на формулы первого порядка. Работа выполнена при поддержке грантов РФФИ, проекты 14–07–00851а, 14-07–00249а, кафедры ДМИ ММФ НГУ.

Список литературы

[1] *Лбов Г. С., Старцева Н. Г.* Логические решающие функции и вопросы статистической устойчивости решений. Новосибирск: Изд–во ИМ СО РАН, 1999.

[2] *Кейслер Г., Чен Ч. Ч.* Теория моделей. М.: Мир, 1977.

[3] *Викентьев А. А, Лбов Г. С.* О метризации булевой алгебры предложений и информативности высказ. экспертов // Доклады РАН 1998. Т.361, №2, С. 174–176.

[4] *Викентьев А. А, Лбов Г. С.* Setting the metric and informativeness on statements of experts // Pattern Recognition and Image Analysis, 1997, V.7, №2, P. 175–183.

[5] *Ершов Ю. Л., Палютин Е. А.* Математическая логика– М.: Физматлит, 2011.

[6] *Викентьев А. А., Коренева Л. Н.* К вопросу о расстояниях между формулами, описывающими структурированные объекты // Математические методы распознавания образов (ММРО-99), РАН ВЦ, Москва, 1999. С.151–154.

ИМ СО РАН и НГУ, Новосибирск
E-mail: vikent@math.nsc.ru

Об алгебрах распределений бинарных изолирующих формул теории одноместных предикатов с унарной функцией

Д. Ю. Емельянов

Исследуются алгебры распределений бинарных изолирующих формул [**1**] для теорий одноместных предикатов с унарной функцией. Для произвольного значения $\lambda \in (\omega \setminus \{0,1\}) \cup \{\infty\}$ обозначим через $\mathfrak{A}_{n,\lambda}$ алгебру $\langle A_{n,\lambda}; *\rangle$ с носителем $A_{n,\lambda} = \mathcal{P}(\{0,1,2\ldots,n-1,\neg\}) \setminus \{\emptyset\}$, задаваемую следующей таблицей:

$*$	$\mathbb{Z}_n$	$\neg$
$\mathbb{Z}_n$	$\langle \mathbb{Z}_n; +\rangle$	$\neg$
$\neg$	$\neg$	$\{0,1,2\ldots,n-1\}$ при $\lambda = 2$, $\{0,1,2\ldots,n-1,\neg\}$ при $\lambda \geq 3$

Для произвольного значения $\lambda \in (\omega \setminus \{0,1\}) \cup \{\infty\}$ обозначим через $\mathfrak{A}_{\mathrm{fr},\lambda}$ алгебру $\langle A_{\mathrm{fr},\lambda}; *\rangle$ с носителем $A_{\mathrm{fr},\lambda} = \mathcal{P}(\omega^2) \setminus \{\emptyset\}$, задаваемую следующей таблицей:

$*$	$(0,m')$	$(k',0)$	(k',m')
$(0,m)$	$(0,m+m')$	$(k'-m,0)$ при $k' \geq m$, $(0,m-k')$ при k'¡m	$(k'-m,m')$ при $k' \geq m$, $(0,m-k'+m')$ при k'¡m
$(k,0)$	$(k-i,m'-i)$, $0 \leq i \leq \min(k,m')$	$(k+k',0)$	$(k+k',m')$
(k,m)	$(k,m+m')$	$(k'-m+k,0)$ при $k' \geq m$, $(k,m-k')$ при k'¡m	при $\lambda = 2$: $(k,m-k'+m')$ при k'¡m, $(k+k'-m,m')$ при k'¿m; k'=m: $(k-m',0)$ при $k \geq m'$, $(0,m'-k)$ при k¡m'; при $\lambda \geq 3$: $(k-i,m'-i)$, $0 \leq i \leq \min(k,m')$

Теорема. *Пусть T — теория унара f с одноместными предикатами $\mathfrak{P}_{\nu(p)}$ — алгебра распределений бинарных изолирующих формул для типа $p \in S^1(\varnothing)$, имеющего реализации a и b с условием $b = f^s(a)$ для некоторого $s > 0$. Тогда алгебра $\mathfrak{P}_{\nu(p)}$ задается ровно одной из следующих алгебр: группой $\mathbb{Z}$, группой $\mathbb{Z}_n$, алгеброй $\mathfrak{A}_{n,\lambda}$, алгеброй $\mathfrak{A}_{\mathrm{fr},\lambda}$, алгеброй $\langle \omega^*; +\rangle$.*

Данная теорема обобщает результат, анонсированный в [**2**].

Список литературы

[1] *Судоплатов С. В.* Классификация счетных моделей полных теорий. — Новосибирск : Изд-во НГТУ, 2014.

[2] *Емельянов Д. Ю.* Алгебры распределений бинарных изолирующих формул теории одноместных предикатов с подстановкой // Материалы международной конференции “Мальцевские чтения”. — Новосибирск, 2014. — С. 126.

Новосибирский государственный университет, Новосибирск
E-mail: dima-pavlyk@mail.ru

Разрешимость универсальных теорий классов матроидов ограниченного ранга

А. В. Ильев

В настоящей работе рассмотрен вопрос разрешимости универсальных теорий матроидов, ранг которых не превосходит $k \in \mathbb{N}$.

Пусть $k \in \mathbb{N}$ — фиксированное число. Тогда *матроидом ранга, не превосходящего* k, называется пара $M = (U, \mathcal{I})$, где U — непустое (возможно бесконечное) множество, $\mathcal{I}$ — непустое семейство его *независимых* подмножеств, удовлетворяющее аксиомам:

(I1) $I \in \mathcal{I},\ J \subseteq I \Rightarrow J \in \mathcal{I}$ (аксиома наследственности);

(I2) для любых $I, J \in \mathcal{I}$ таких, что $|J| = |I| + 1$, существует элемент $j \in J \setminus I$, для которого $I \cup \{j\} \in \mathcal{I}$ (аксиома пополнения).

(I3) $|I| \leq k$ для всех $I \in \mathcal{I}$.

Число $r(M)$, равное общей мощности максимальных независимых множеств матроида, называется *рангом матроида* M

Далее определим матроид ранга, не превосходящего k, на языке исчисления предикатов первого порядка с равенством.

Матроид M *ранга, не превосходящего* $k \in \mathbb{N}$, — это алгебраическая система $M = \langle U, \Sigma_I \rangle$, где U — непустое множество, а сигнатура $\Sigma_I = \langle I_0, I_1, ..., I_k, = \rangle$ состоит из $k+1$ предикатов независимости, местность каждого из которых совпадает с его порядковым номером, и предиката равенства, причем предикаты независимости удовлетворяют условиям *неупорядоченности и неповторения элементов, наследственности* и *пополнения*:

1) $\forall x_1 \ ... \ \forall x_n \ [I_n(x_1, ..., x_n) \to \bigwedge\limits_{\pi} I_n(\pi(x_1), ..., \pi(x_n))]$, где π пробегает по всем перестановкам элементов $x_1, ..., x_n$, $n \in \{1, ..., k\}$;

2) $\forall x_1 \ ... \ \forall x_n \ [I_n(x_1, ..., x_n) \to \bigwedge\limits_{i \neq j} (x_i \neq x_j)]$, $n \in \{1, ..., k\}$;

3) $\forall x_1 \ ... \ \forall x_n \ [(I_n(x_1, ..., x_n) \to I_{n-1}(x_2, ..., x_n) \wedge \ ... \ \wedge I_{n-1}(x_1, ..., x_{n-1})) \ \wedge \ I_0]$, $n \in \{2, ..., k\}$;

4) $\forall x_1 \ ... \ \forall x_n \ \forall y_1 \ ... \ \forall y_{n+1} \ [I_n(x_1, ..., x_n) \ \wedge \ I_{n+1}(y_1, ..., y_{n+1}) \ \to \bigvee\limits_{i \in \{1, ..., n+1\}} I_{n+1}(x_1, ..., x_n, y_i)]$, $n \in \{1, ..., k-1\}$.

Таким образом, класс матроидов ранга, не превосходящего k, конечно универсально аксиоматизируем. Кроме того, для любого $k \in \mathbb{N}$ справедлива теорема.

Теорема. *Универсальная теория матроидов ранга, не превосходящего* $k \in \mathbb{N}$, *разрешима.*

Институт математики им. С.Л. Соболева СО РАН, Омск
E-mail: artyom_iljev@mail.ru

О принадлежности функций алгебры логики максимальным мультиклонам

А. С. Казимиров, В. И. Пантелеев

Пусть $|A|$ — мощность множества A, 2^A — множество всех подмножеств A и $E_2 = \{0, 1\}$. Определим следующие множества функций:

$$P_{2,n}^{*-} = \{f \mid f : E_2^n \to 2^{E_2}\}, P_2^{*-} = \bigcup_n P_{2,n}^{*-}.$$

Функции из P_2^{*-} называются мультифункциями. Очевидно, что множество функций алгебры логики вкладывается в множество P_2^{*-}. Суперпозиция

$$f(f_1(x_1, \dots, x_m), \dots, f_n(x_1, \dots, x_m))$$

мультифункций $f(x_1, ..., x_n)$, $f_1(x_1, ..., x_m)$, ..., $f_n(x_1, ..., x_m)$ определяет мультифункцию $g(x_1, ..., x_m)$ следующим образом:

$$g(\alpha_1, \dots, \alpha_m) = \bigcup_{\beta_i \in f_i(\alpha_1, \dots, \alpha_m)} f(\beta_1, \dots, \beta_n)$$

для любого набора $(\alpha_1, \dots, \alpha_m) \in E_2^m$.

Множества, содержащие все функции-проекции и замкнутые относительно суперпозиции, называются клонами. Клон называется максимальным, если единственным клоном, его содержащим и не совпадающим с ним, является клон всех мультифункций.

В [**1**] описаны все 15 максимальных клонов мультифункций.

Для каждой мультифункции однозначным образом определим вектор принадлежности максимальным клонам, в котором на i-й позиции $(i = 1, \dots, 15)$ стоит 0, если мультифункция принадлежит i-му максимальному клону, и 1 иначе.

На множестве всех мультифункций определим отношение эквивалентности следующим образом: эквивалентными будут мультифункции, у которых совпадают векторы принадлежности максимальным клонам мультифункций.

Теорема. *Множество функций алгебры логики порождает 18 классов эквивалентности.*

Известно, что относительно принадлежности максимальным клонам функций алгебры логики число аналогичных классов эквивалентности равно 15 [**2**].

Работа выполнена при поддержке РФФИ, проект №13-01-00621.

Список литературы

[1] *Пантелеев В. И.* Критерий полноты для недоопределенных частичных булевых функций // Вестник НГУ. Серия: Математика, механика, информатика. 2009. Т. 9, вып. 3. С. 95–114.

[2] *Яблонский С. В.* О суперпозициях функций алгебры логики // Мат. сб. 1952. Т. 30,№ 2 (72), С. 329–348.

Иркутский государственный университет, Иркутск
E-mail: a.kazimirov@gmail.com, vl.panteleyev@gmail.com

О чистых подполугруппах вполне простых полугрупп

О. В. Князев

В [**1**] определяется понятия чистоты для произвольных универсальных алгебр и ставится задача изучения чистых подалгебр. Мы решаем эту задачу в классе всех вполне простых полугрупп. Вполне простые полугруппы рассматриваются здесь как алгебры сигнатуры $< \cdot,^{-1} >$, где $^{-1}$ есть взятие обратного элемента к данному в максимальной подгруппе, содержащей данный элемент. В этой сигнатуре, как хорошо известно, класс всех вполне простых полугрупп является многообразием. Пусть $\mathbf{V}$ — многообразие всех вполне простых полугрупп, $L(\mathbf{V})$ — решетка подмногообразий многообразия $\mathbf{V}$, $\mathbf{X} \in L(\mathbf{V})$, $S \in \mathbf{V}$. Произвольное дизъюнктное семейство подполугрупп полугруппы S называют *россыпью* полугруппы S, а полугруппы, которые ее составляют, — *компонентами* россыпи. Через $K(S)$ обозначим полную решетку всех россыпей полугруппы S, а через $\wedge$ — операция пересечения в этой решетке. Пусть $\mathbf{X}(S)$ есть $\mathbf{X}$-вербал полугруппы S, т.е. россыпь, компоненты которой в точности все классы $\mathbf{X}$-вербальной конгруэнции полугруппы S, являющиеся подполугруппами полугруппы S. Подполугруппу S_1 полугруппы S называют *чистой* в S, если равенство $\mathbf{X}(S_1) = \mathbf{X}(S) \wedge S_1$ выполняется для любого атома $\mathbf{X}$ из решетки $L(\mathbf{V})$. Заметим, что одним из атомов решетки $L(\mathbf{V})$ будет многообразие $\mathbf{A}_p$ всех абелевых групп простой экспоненты p, а всякая вполне простая полугруппа S изоморфна некоторой регулярной рисовской полугруппе $M(A; I, \Lambda; P)$ матричного типа над группой A с сэндвич-матрицей $P = (p_{\lambda i})$.

Пусть $S = M(A; I, \Lambda; P)$, $S_1 = M(A_1; I_1, \Lambda_1; P_1) \leq S$, $N(P)$ — нормальная подгруппа группы A, порожденная элементами сэндвич-матрицы P, $N(P_1)$ — нормальная подгруппа группы A_1, порожденная элементами сэндвич-матрицы P_1.

Имеет место

ТЕОРЕМА. *Полугруппа S_1 является чистой подполугруппой полугруппы S тогда и только тогда, когда равенство $(N(P)\mathbf{A}_p(A)) \cap A_1 = N(P_1)\mathbf{A}_p(A_1)$ выполняется для любого простого p.*

Исследование выполнено при поддержке Министерства образования и науки Российской Федерации, задание №2014/336.

Список литературы

[1] *Мартынов Л. М.* О понятиях полноты, редуцированности, примарности и чистоты для произвольных алгебр // Универсальная алгебра и ее приложения. Труды междунар. семинара. Волгоград: Перемена 2000, 179 – 190.

Омский государственный педагогический университет, Омск
E-mail: knyazev50@rambler.ru

Алгебраический подход к получению условий устойчивости свойств динамических систем

Н. В. Нагул

В докладе освещается метод логико-алгебраических уравнений как один из методов, обеспечивающих редукцию (сведение) изучения одной динамической системы к изучению другой за счет сохранения свойств при переходе между системами. Еще в 1974 году для обеспечения алгоритмического формирования критериев сохранения свойств динамических систем на основе логических методов В. М. Матросов предложил *метод сравнения*, получивший в дальнейшем широкое развитие в его научной школе (Л. Ю. Анапольский, С. Н. Васильев, Р. И. Козлов и др.). Одним из основных применений критериев сохранения является сведение на их основе задачи изучения сложной модели к изучению более простой. Метод используется для установления наличия в динамической системе, описываемой, например, дифференциальными уравнениями, свойств устойчивости ее решений, диссипативности и т.д. при существовании этих свойств во вспомогательной системе.

Для получения критериев сохранения свойств динамических систем, состоящих из условий, имеющих смысл легко проверяемых условий типа сохранения операций или отношений, на стыке динамики систем, алгебры и логики был предложен метод логико-алгебраических уравнений (ЛАУ), который позволяет генерировать условия сохранения свойств многоосновной алгебраической системы (МАС) при отображениях ее базисных множеств в базисные множества однотипной ей системы. Именно к МАС приводит алгебраизация динамических систем (основными множествами в этом случае выступают пространство состояний, шкала времени и др.), причем их функции и отношения определены не просто на базисных множествах или их декартовых произведениях, а на произвольных ступенях в смысле Н. Бурбаки. Понятие ступени расширенно дополнительной операцией образования последовательностей, введение которой было мотивировано стремлением охватить вопрос сохранения свойств таких динамических систем, как дискретно-событийные системы (ДСС). На примере модели супервизорного (диспетчерского) управления ДСС показано применение метода ЛАУ для получения условий сохранения полезных свойств супервизора при его упрощении. Метод применим как для изучения свойств более сложных моделей супервизоров (с частично наблюдаемыми и форсируемыми событиями, распределенных и децентрализованных), так и для исследования других динамических систем.

Работа выполнена при частичной поддержке РФФИ (проекты 14-07-00740, 14-07-31192-мол-а).

Институт динамики систем и теории управления СО РАН, Иркутск
E-mail: sapling@icc.ru

Инверсные полугруппы линейных отношений

М. И. Наумик

Пусть V — векторное пространство над полем F. Напомним, что линейным отношением на V называется подпространство пространства $V \oplus V$. Множество всех линейных отношений на V с операцией умножения является полугруппой $LR(V)$. $LR'(V)$ — полугруппа всех полулинейных отношений пространства V.

Теорема. *Если пространство V конечномерно, то каждый элемент $a \in LR(V)$ содержится в некоторой инверсной подполугруппе $D \subset LR(V)$.*

Этот результат дает частичное решение аналогичной задачи, поставленной Б. М. Шайном [**1**]. Аналогичная теорема справедлива и для полугруппы $LR'(V)$.

Список литературы

[1] *Шайн Б. М.* Сильно регулярные кольца // I Всесоюзный симпозиум по теории колец и модулей. Резюме сообщений и докладов. Кишинев, 1969.

ВГУ имени П.М. Машерова, Витебск
E-mail: naumik@tut.by

Компаньоны

А. Т. Нуртазин

С помощью компаньон-классов можно напрямую ввести понятие просто экзистенциально замкнутой структуры. Для счётной предикатной сигнатуры Σ *классом Фрэсе* F мы также называем произвольный абстрактный обладающий свойством совместного вложения и замкнутый относительно взятия подструктур и обеднений класс конечных структур всевозможных конечных подсигнатур Σ. Таким является класс $F(M)$ обеднений на конечные подсигнатуры конечных структур, вложимых в структуру M. С помощью классов Фрэсе можно значительно упростить определение широко используемого в теории экзистенциально замкнутых моделей понятия *компаньона.*

Определение. *Структуры M и N чисто предикатной сигнатуры Σ назовём компаньонами друг друга, если совпадают их классы Фрэсе:*

$F(M) = F(N)$.

Для данной структуры M полной теории T совокупность всех её компаньонов мы обозначаем через $C(M)$, а элементарную теорию этого класса — через T^c.

Теорема 1. (1) *Компаньон-класс $C(M)$ данной $\Sigma-$структуры M аксиоматизируем и является классом всех моделей теории $T_\exists \cup T_\forall$.*

(2) *Данные структуры M и N чисто предикатной сигнатуры Σ являются компаньонами, если и только если каждая из них может быть изоморфно вложена в некоторое элементарное расширение другой.*

(3) *Модели полных теорий S и T являются компаньонами, если и только если совпадают классы их экзистенциально замкнутых моделей.*

Следующее утверждение отвечает на вопрос о возможном числе счётных неизоморфных компаньонов.

Теорема 2. *Данная компаньон-теория T^c может иметь либо одну, либо счётное число, либо континуум счётных моделей.*

Список литературы

[1] *Нуртазин А. Т.* Счётные экзистенциально замкнутые модели универсально аксиоматизируемых теорий, Математические труды, 2015, том 18, № 1, 1-50.

Институт информационных и вычислительных технологий, Алматы
E-mail: abyznurtazin@mail.ru

Экзистенциально замкнутые структуры и их теории

А. Т. Нуртазин

С помощью компаньон-классов можно напрямую ввести понятие просто экзистенциально замкнутой структуры.

Определение. *Данную $\Sigma-$структуру M называем экзистенциально замкнутой, если она экзистенциально замкнута в своём компаньон-классе $C(M)$.*

Как показывает следующая теорема, экзистенциальную замкнутость можно считать семантико-алгебраиеским аналогом счётной насыщенности. Естественно ожидать, что она может оказаться полезной при доказательстве экзистенциальной замкнутости именно конкретных $\Sigma-$структур.

Теорема. *Данная $\Sigma-$структура M экзистенциально замкнута, если и только если для любого её компаньон-расширения N, конечной подсигнатуры σ сигнатуры Σ и кортежей $\bar{a}$ из M и $\bar{b}$ из N в M найдётся кортеж $\bar{b}^0$ той же длины как и $\bar{b}$ и такой, что покоординатное соответствие из $\bar{a}\bar{b}$ на $\bar{a}\bar{b}^0$ является изоморфизмом структур $<\bar{a}\bar{b};\sigma>$ и $<\bar{a}\bar{b}^0;\sigma>$.*

Следующий локальный синтаксический критерий из [**1**] оказывается полезным для поиска условий, когда данная теория является теорией некоторого класса экзистенциально замкнутых структур.

Теорема. *Данная $\Sigma-$структура M экзистенциально замкнута, если и только если для любого её кортежа $\bar{a}$ и выполняющейся на нём универсальной формулы $\psi(\bar{b})$ найдётся также истинная на этом кортеже экзистенциальная формула $\varphi(\bar{x})$, для которой выполняется*

$$M \models \varphi(\bar{x}) \to \psi(\bar{b}).$$

Теорема. *Данная $\Sigma-$теория T является элементарной теорией некоторого класса экзистенциально замкнутых $\Sigma-$структур, если и только если для любых выполнимых в T $\varphi(\bar{x})$ универсальной $\psi(\bar{x})$ таких, что $T \vdash \varphi(\bar{x}) \to \psi(\bar{x})$ найдётся некоторая экзистенциальная формула $\theta(\bar{x})$ с условием, что в T непротиворечиво*

$$\exists\bar{x}[\varphi(\bar{x})\&\theta(\bar{x})]\&\forall\bar{x}[\theta(\bar{x}) \to \psi(\bar{x})].$$

Список литературы

[1] *Нуртазин А. Т.* Компаньоны, Этот сборник, 2015.

Институт информационных и вычислительных технологий, Алматы
E-mail: abyznurtazin@mail.ru

Конечно-аксиоматизируемые суператомные булевы алгебры с выделенной плотной подалгеброй конечной ширины

Д. Е. Пальчунов, А. В. Трофимов

Определение [**1**]. Подалгебра $\mathfrak{B}$ булевой алгебры $\mathfrak{A}$ называется *подалгеброй ширины* n, если под любым атомом подалгебры $\mathfrak{B}$ найдется не более n атомов алгебры $\mathfrak{A}$, и любой атом алгебры $\mathfrak{A}$ лежит под некоторым атомом подалгебры $\mathfrak{B}$. Подалгебра $\mathfrak{B}$ называется *плотной*, если $\mathfrak{A} = sub_{\mathfrak{A}}(\mathfrak{B}, F(\mathfrak{A}))$ - наименьшая подалгебра алгебры $\mathfrak{A}$, содержащая в себе подалгебру $\mathfrak{B}$ и идеал Фреше $F(\mathfrak{A})$.

Определение [**1**]. Обозначим $\mathfrak{A} \leq \mathfrak{B}$, если найдется $\mathfrak{C}$ такая, что $\mathfrak{B} \equiv \mathfrak{A} \times \mathfrak{C}$. Алгебраическая система $\mathfrak{A}$ называется *неисчезающей*, если из $\mathfrak{A} \equiv \mathfrak{M} \times \mathfrak{N}$ следует $\mathfrak{A} \equiv \mathfrak{M}$ или $\mathfrak{A} \equiv \mathfrak{N}$. Алгебраическая система $\mathfrak{A}$ называется *локальной*, если число попарно элементарно неэквивалентных неисчезающих алгебраических систем $\mathfrak{B} \leq \mathfrak{A}$ конечно, т.е. существуют $\mathfrak{B}_1, \ldots, \mathfrak{B}_n$ такие, что для произвольной неисчезающей $\mathfrak{C} \leq \mathfrak{A}$ выполнено $\mathfrak{C} \equiv \mathfrak{B}_i$ для некоторого $i \leq n$.

Определение. Алгебраическая система $\mathfrak{A}$ называется *идемпотентной*, если $\mathfrak{A} \equiv \mathfrak{A} \times \mathfrak{A}$, и *неидемпотентной*, если $\mathfrak{A} \not\equiv \mathfrak{A} \times \mathfrak{A}$.

Теорема. *Пусть* $\mathfrak{A}$ *— суператомная булева алгебра с выделенной плотной подалгеброй конечной ширины. Элементарная теория* $Th(\mathfrak{A})$ *конечно аксиоматизируема тогда и только тогда, когда* $\mathfrak{A} = \mathfrak{A}_1 \times \ldots \times \mathfrak{A}_n$ *для некоторых локальных неисчезающих неидемпотентных* $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$.

Список литературы

[1] *Пальчунов Д. Е., Трофимов А. В.* Локальные и неисчезающие суператомные булевы алгебры с выделенной плотной подалгеброй, Алгебра и логика, 50:6 (2011), 822–847.

ИМ СО РАН, НГУ, Новосибирск
E-mail: palch@math.nsc.ru, tr0f@mail.ru

Об обогащениях категоричных антиаддитивных хорновых теорий

Е. А. Палютин

В докладе даются необходимые и достаточные условия для того, чтобы категоричные антиаддитивные хорновы теории обогащались до аддитивных.

Категоричные хорновы теории делятся на 2 класса: антиаддитивные и аддитивные. Антиаддитивными называются теории, в которых нельзя примитивно проинтерпретировать бесконечную группу.

Пусть T — категоричная антиаддитивная хорнова теория. Группа G_T называется базисной группой теории T, если она изоморфна группе примитивно определимых подстановок некоторого сильно минимального примитивного множества в некоторой T-модели.

Предложение. *Для категоричной антиаддитивной хорновой теории T базисная группа G_T определена однозначно с точностью до изоморфизма.*

Группа G называется аффинной, если она является некоторой подгруппой группы подстановок некоторого векторного пространства V над телом K, вида $\alpha x + c$, где $\alpha \in K$, $c \in V$.

Теорема. *Для того, чтобы категоричная антиаддитивная хорнова теория T обогащалась до категоричной аддитивной хорновой теории, необходимо и достаточно, чтобы ее базисная группа G_T была аффинной.*

Заметим, что из описания категоричных квазимногообразий в [**3**] следует, что любая группа G является базисной для некоторого антиаддитивного квазимногообразия. Известно, что не каждая группа является аффинной, поэтому из предудущей теоремы вытекает, что существуют категоричные антиаддитивные хорновы теории, которые не обогащаются до категоричных аддитивной хорновых теорий.

Список литературы

[1] *Palyutin E. A.* Additive theories, in: Proceedings of Logic Colloquium'98 (Lectures Notes in Logic, v. 13), ASL, Massachusetts, 2000, p. 352-356.

[2] *Палютин Е. А.* Категоричные хорновы классы 1., Алгебра и логика, т.19, N 5(1980), с. 582-614.

[3] *Палютин Е. А.* Описание категоричных квазимногообразий, Алгебра и логика, 14, № 2 (1975), 145-185.

Институт математики им. С.Л.Соболева СО РАН
E-mail: palyutin@math.nsc.ru

Минимальные алгебры унарных мультиопераций

Н. А. Перязев

Пусть $B(A)$ — множеств всех подмножеств A. Отображение из A в $B(A)$ называется унарной мультиоперацией на A. Используем обозначение M^1_A.

Пусть $S \subseteq M^1_A$. Алгебра $\mathfrak{F} =< S; *, \cap, \mu, \varepsilon, \theta, \pi >$ с ниже определенными операциями подстановки $(f*g)$, пересечения $(f \cap g)$, обратимости (μf) и нульместными операциями ε, θ, π называется *алгеброй унарных мультиопераций* над A:

$(f * g)(a) = \{b \mid$ существует $c \in g(a)$ такой, что $b \in f(c)\}$;

$(f \cap g)(a) = f(a) \cap g(a)$; $(\mu f)(a) = \{b \mid a \in f(b)\}$;

$\varepsilon(a) = \{a\}$; $\theta(a) = \varnothing$; $\pi(a) = A$.

Мощность множества A называется рангом алгебры. В работе [**1**] рассматривались алгебры умо рангов 2 и 3. В частности доказано, что существует 19 алгебр унарных мультиопераций ранга 2 и 2079040 алгебр ранга 3. Среди их минимальными являются, соответственно, 4 и 18 алгебр. Ниже получено описание всех минимальных алгебр умо для произвольных конечных рангов.

Теорема. *Минимальными алгебрами умо $\langle f \rangle$ являют алгебры удовлетворяющие одному из следующих условий и только такие алгебры.*

1. $f \cap \varepsilon = \varepsilon, \mu f = f, f^2 = f$.
2. $f \cap \varepsilon = \varepsilon, \mu f = f, f^2 = \pi$.
3. $f \cap \varepsilon = \theta, \mu f = f, f^2 = \varepsilon$.
4. $f \cap \varepsilon = \theta, \mu f = f, f^2 = \pi$.
5. $f \cap \varepsilon = \varepsilon, \mu f \cap f = \varepsilon, f * \mu f = \mu f * f = \pi, f^2 = f$.
6. $f \cap \varepsilon = \varepsilon, \mu f \cap f = \varepsilon, f * \mu f = \mu f * f = \pi, f^2 = \pi$.
7. $f \cap \varepsilon = \theta, \mu f \cap f = \theta, f * \mu f = \mu f * f = \varepsilon, f^p = \varepsilon$, *где p простое число и* $p \geq 3$.
8. *Существует $b \in A$ такой, что $f(a) = \{b\}$ для всех $a \in A$ или $f(b) = \{b\}$ и $f(a) = \varnothing$ для всех $a \neq b$ или $f(b) = A$ и $f(a) = \varnothing$ для всех $a \neq b$.*
9. *Существует не одноэементное множество $B \subset A$ такое, что $f(a) = B$ для всех $a \in A$ или $f(b) = \{b\}$ для всех $b \in B$ и $f(a) = \varnothing$ для всех $a \in A \backslash B$ или $f(b) = A$ для всех $b \in B$ и $f(a) = \varnothing$ для всех $a \in A \backslash B$ или $f(b) = B$ для всех $b \in B$ и $f(a) = \varnothing$ для всех $a \in A \backslash B$.*

Отметим, что алгебры типа 1–4 состоят из четырех элементов, типа 5, 6 — из пяти, типа 8 — из шести, типа 9 — из семи и типа 7 — из $p + 2$ элементов.

Работа выполнена при поддержке ФЦП “Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014-2020 годы”, контракт № 14.579.21.0092.

Список литературы

[1] *Казимиров А. С., Перязев Н. А.* Алгебры унарных мультиопераций // Международная конференция “Мальцевские чтения”. Тезисы докл. — Новосибирск, 2013. — С. 156.

Санкт-Петербургский государственный электротехнический университет, Санкт-Петербург
E-mail: nikolai.baikal@gmail.com

О Ihm-дозволенных и Ihm-запрещенных квазипорядках

А. Г. Пинус

Понятие алгебраического множества для универсальной алгебры $\mathfrak{A} = < A; \sigma >$ связано (см. [**1**]) с некоторым отношением квазипорядка $\leqslant_{Ihm\mathfrak{A}}$ на множестве A определенным следующим образом: для $a, b \in A$ $a \leqslant_{Ihm\mathfrak{A}} b$ тогда и только тогда, когда существует гомоморфизм φ алгебры $< b >_{\mathfrak{A}}$ на алгебру $< a >_{\mathfrak{A}}$ такой, что $\varphi(b) = a$. Здесь $< c >_{\mathfrak{A}}$ - подалгебра алгебры $\mathfrak{A}$ порожденная элементом c из A.

Квазипорядок $\leqslant$ на множестве A называется *Ihm-дозволенным (Ihm-запрещенным)*, если существует универсальная алгебра $\mathfrak{A} = < A; \sigma >$ для которой $\leqslant_{Ihm\mathfrak{A}}$ совпадает с $\leqslant$ (если ни для какой $\mathfrak{A} = < A; \sigma >$ квазипорядок $\leqslant_{Ihm\mathfrak{A}}$ не совпадает с $\leqslant$).

Теорема 1. *Для любого кардинала $k \geqslant 4$ существует k-элементный Ihm-запрещенный квазипорядок. Все не более чем трехэлементные квазипорядки Ihm-дозволены.*

Теорема 2. а) *Любой линейный квазипорядок является Ihm-дозволенным.* б) *Любая нижняя полурешетка Ihm-дозволенна.*

Работа выполнена при финансовой поддержке Министерства образования и науки РФ по государственному заданию № 2014/138, проект 1052.

Список литературы

[1] *Пинус А. Г.* О квазипорядке индуцированном внутренними гомоморфизмами универсальных алгебр и об алгебраических множествах этих алгебр. — в печати.

Новосибирский государственный технический университет, Новосибирск
E-mail: a.g.pinus@gmail.com

О счетных моделях теорий абелевых групп с конечными инвариантами Шмелевой

Р. А. Попков

Напомним, что модель $\mathcal{M}$ теории T называется *простой моделью над множеством* A, если любая константно содержащая A модель $\mathcal{N}$ теории T содержит элементарную подмодель $\mathcal{M}'$, также константно содержащую A и изоморфную модели $\mathcal{M}$. Модель $\mathcal{M}$ теории T называется *предельной*, если она является объединением счетной элементарной цепи простых над конечными множествами моделей и не изоморфна никакой простой над конечным множеством модели [**1**].

Следующие числа для произвольных p и n (p – простое, n – натуральное) называются *инвариантами Шмелевой* абелевой группы A [**2**]:

$$\alpha_{p,n}(A) = \min\{\dim((p^n A)[p]/(p^{n+1}A)[p]), \omega\},$$

$$\beta_p(A) = \min\{\inf\{\dim((p^n A)[p] \mid n \in \omega\}, \omega\},$$

$$\gamma_p(A) = \min\{\inf\{\dim((A/A[p^n])/p(A/A[p^n])) \mid n \in \omega\}, \omega\},$$

$$\varepsilon(A) \in \{0,1\}\,\text{и}, \varepsilon(A) = 0 \Leftrightarrow (nA = \{0\}\,\text{для некоторого}\,n \in \omega, n \neq 0).$$

Верна следующая

Теорема. *Если счетная модель $\mathcal{M}$ теории бесконечной абелевой группы A с конечными инвариантами Шмелевой содержит элементарную подмодель $\mathcal{M}'$, которая является простой над некоторым конечным множеством, то $\mathcal{M}$ либо проста над некоторым конечным множеством, либо предельна.*

Список литературы

[1] *Судоплатов С. В.* Классификация счетных моделей полных теорий. Ч 2. Новосибирск: Изд-во НГТУ, 2014. – 448 с.

[2] *Ершов Ю. Л., Палютин Е. А.* Математическая логика : Учеб. пособие для вузов. М. : Физматлит, 2011. – 356 с.

Новосибирский государственный технический университет, Новосибирск
E-mail: r-popkov@yandex.ru

Полигоны с $(P,1)$-стабильной теорией

Д. О. Птахов

В данной работе рассматриваются полигоны с $(P,1)$-стабильной теорией. Понятие $(P,1)$-стабильной теории было введено в [**1**]. Это понятие является обобщением понятия стабильности теории. В [**2**] приводится характеризация $(P,1)$-стабильных теорий как класса теорий, определимо интерпретируемых в какой-либо теории языка, состоящего только из одноместных предикатов.

Под левым полигоном ${}_SA$ над моноидом S или просто полигоном понимается множество A, на котором определено действие элементов из S, причем единица действует на A тождественно. Пусть T – теория языка L, язык L_P получается из языка L добавлением одноместного предикатного символа P, Δ – некоторое множество предложений языка L_P. Теория T называется P_Δ-стабильной в мощности λ, если для любого множества X мощности $\leq \lambda$ в теории T множество

$$T_\Delta(X) = T(X) \cup \{P(a) \mid a \in X\} \cup \Delta$$

имеет не более λ пополнений в языке $(L(X))_P$, где $L(X)$ – язык, получаемый из языка L добавлением множества X в качестве множества новых констант. Теория T называется P_Δ-стабильной, если она является P_Δ-стабильной в некоторой бесконечной мощности λ. Теория T называется $(P,1)$-стабильной, если она P_Δ-стабильна для $\Delta = \varnothing$. Полигон ${}_SA$ называется P_Δ-стабильным, если теория $Th({}_SA)$ этого полигона P_Δ-стабильна.

Теорема. *Полигон ${}_SA$ является $(P,1)$-стабильным тогда и только тогда, когда для любого $t \in S$ множества $t\dot{A}\backslash\{a \in A \mid ta = a\}$ и $\{a \in A \mid ta = a \wedge \exists b(tb = a, b \neq a)\}$ конечны.*

Копроизведением двух полигонов ${}_SA_1$ и ${}_SA_2$ называется их дизъюнктное объединение и обозначается: ${}_SA_1 \sqcup {}_SA_2$. Через $S - Act$ обозначим класс всех полигонов над моноидом S. Класс полигонов назовем P_Δ-стабильным, если каждый полигон этого класса является P_Δ-стабильным.

Следствие 1. *Пусть ${}_SA = {}_SA_1 \sqcup {}_SA_2$. Тогда полигон ${}_SA$ является $(P,1)$-стабильным тогда и только тогда, когда полигоны ${}_SA_1$ и ${}_SA_2$ являются $(P,1)$-стабильными.*

Следствие 2. *Пусть S – группа. Полигон ${}_SS$ является $(P,1)$-стабильным тогда и только тогда, когда S — конечная группа.*

Следствие 3. *Класс $S - Act$ является $(P,1)$-стабильным тогда и только тогда, когда $|S| = 1$.*

Список литературы

[1] *Палютин Е. А.* E^*-стабильные теории, Алгебра и Логика, т. 42, N 2 (2003) с. 194-210.

[2] *Русалеев М. А.* Характеризация $(P,1)$-стабильных теорий, Алгебра и Логика, т. 46, N 2 (2007) с. 346-359.

Дальневосточный федеральный университет, Владивосток
E-mail: ptaxov@mail.ru

Дистрибутивные и стандартные элементы решетки многообразий эпигрупп

Д. В. Скоков

Эпигруппой называется полугруппа S, в которой некоторая степень каждого элемента лежит в некоторой подгруппе полугруппы S. На всякой эпигруппе можно некоторым естественным способом ввести унарную операцию, называемую *псевдообращением* (см., например, [**2**]). Это позволяет рассматривать многообразия эпигрупп как алгебр в сигнатуре, состоящей из умножения и псевдообращения.

Мы продолжаем начатое в [**4**] изучение специальных элементов в решетке многообразий эпигрупп. В [**4**] рассматриваются нейтральные, модулярные и верхнемодулярные элементы этой решетки (определения этих типов элементов см. в [**3**] или [**4**]). В данной работе изучаются ее дистрибутивные и стандартные элементы. Напомним, что элемент x решетки L называется *дистрибутивным* [*стандартным*], если $\forall\, y, z \in L: \quad x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ [соответственно $(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z)$.

В [**1**] полностью описаны дистрибутивные элементы решетки всех многообразий полугрупп. Описание стандартных элементов решетки всех многообразий полугрупп можно найти в работе [**5**]. В данной работе получены эпигрупповые аналоги этих результатов.

Через $\mathcal{T}$ и $\mathcal{SL}$ будем обозначать тривиальное многообразие и многообразие полурешеток. Положим $\mathcal{Q} = \mathrm{var}\,\{x^2y = xyx = yx^2 = 0\}$, $\mathcal{Q}_n = \mathrm{var}\,\{x^2y = xyx = yx^2 = x_1x_2\cdots x_n = 0\}$, $\mathcal{R} = \mathrm{var}\,\{x^2 = xyx = 0\}$ и $\mathcal{R}_n = \mathrm{var}\,\{x^2 = xyx = x_1x_2\cdots x_n = 0\}$.

Теорема 1. *Для многообразия эпигрупп $\mathcal{V}$ следующие условия эквивалентны:*

а) *$\mathcal{V}$ является дистрибутивным элементом решетки многообразий эпигрупп;*

б) *$\mathcal{V}$ является стандартным элементом решетки многообразий эпигрупп;*

в) *$\mathcal{V} = \mathcal{M} \vee \mathcal{N}$, где $\mathcal{M}$ — одно из многообразий $\mathcal{T}$ и $\mathcal{SL}$, а $\mathcal{N}$ — одно из многообразий $\mathcal{Q}$, $\mathcal{Q}_n$, $\mathcal{R}$ и $\mathcal{R}_n$ для некоторого натурального n.*

Список литературы

[1] *Верников Б. М., Шапрынский В. Ю.* Дистрибутивные элементы решётки многообразий полугрупп // Алгебра и логика, 2010, Т. 49, №3, С. 303–330.

[2] *Шеврин Л. Н.* К теории эпигрупп. I, II // Мат. сб. 1994. Т. 185, № 8. С. 129–160; № 9. С. 153–176.

[3] *Grätzer G.* Lattice Theory: Foundation, Birkhäuser, Springer Basel AG, 2011.

[4] *Shaprynskiĭ V. Yu., Skokov D. V., Vernikov B. M.* Special elements of the lattice of epigroup varieties // Algebra Universalis, submitted; available at http://arxiv.org/abs/1408.0356.

[5] *Vernikov B. M.* Special elements in lattices of semigroup varieties // available at http://arxiv.org/abs/1309.0228. [P. 1-28.]

Уральский федеральный университет, Екатеринбург
E-mail: dmitry.skokov@gmail.com

(P,s)- и (P,e)-стабильные полигоны

А. А. Степанова, Д. О. Птахов

Понятия $(P, s)-$ и $(P, e)-$стабильности полных теорий, являющиеся частными случаями $P_\Delta-$стабильности, введены в работе [**1**]. В работе [**2**] исследована взаимосвязь различных частных случаев $P_\Delta-$стабильности и их связь со стабильностью полных теорий. Абелевы группы с $(P, s)-$ и $(P, e)-$стабильными теориями изучены в [**3**], где дано описание $(P, s)-$стабильных абелевых групп и доказано, что любая абелева группа является $(P, e)-$стабильной.

Напомним некоторые определения. Теория называется $(P, s)-$стабильной, если она $P_\Delta-$стабильна для множества Δ, состоящего из предложений, выражающих замкнутость предиката P относительно функций, определимых функциональными символами. Теория называется $(P, e)-$стабильной, если она $P_\Delta-$стабильна для множества Δ, состоящего из предложений, выражающих тот факт, что предикат P является элементарной подсистемой. Структура $P_\Delta-$стабильна, если теория этой структуры $P_\Delta-$стабильна. Класс структур одного языка $P_\Delta-$стабилен, если каждая структура этого класса $P_\Delta-$стабильна.

Пусть S – моноид, e – единица моноида S. Структура $\langle A; L_S\rangle$ языка $L_S = \{s \in S\}$ называется левым S-полигоном, если

$$(st)a = s(t(a)), \quad e(a) = a$$

для всех $a \in A$, $s, t \in S$. Через $S - Act$ обозначим класс всех левых S-полигонов.

Теорема. *Следующие условия эквивалентны:*

1) *класс $S - Act$ является $(P, e)-$стабильным;*

2) *класс $S - Act$ является $(P, s)-$стабильным;*

3) *моноид S является группой.*

Список литературы

[1] *Палютин Е. А.* E^*-стабильные теории, Алгебра и логика, т. 42, N 2 (2003) с. 194-210.

[2] *Русалеев М. А.* Характеризация $(P, 1)-$стабильных теорий, Алгебра и логика, т. 46, N 2 (2007) с. 346-359.

[3] *Палютин Е. А.* P-стабильные абелевы группы, Алгебра и логика, т. 52, N 5 (2013) с. 606-631.

Дальневосточный федеральный университет, г. Владивосток
E-mail: stepltd@mail.ru, ptaxov@mail.ru

Обобщенные вербальные категории и аналитические функторы

С. Н. Тронин

Доклад посвящен обобщению результатов [**1**]. Вербальные категории были определены в [**2**], [**3**]. В данном докладе вводится обобщение вербальных категорий, использующее двойные категории. *Базовая вербальная категория* — это двойная категория, объекты которой — конечные слова в алфавите S, где S — некоторый класс. Горизонтальные стрелки — морфизмы категории P_S из [**3**, с.1185], вертикальные — морфизмы из моноидальной категории, обладающей рядом свойств. В частности, тензорное произведение объектов-слов является их произведением как элементов свободной полугруппы. Кроме того, должен существовать тождественный на объектах функтор в категорию $FSet_S$ [**3**, с.1185], который переводит квадраты двойной категории в многосортные аналоги коммутативных диаграмм вида (1) из [**3**, с.1186], и обладает некоторыми другими свойствами. Примеры таких категорий конструируются с использованием групп кос, лент, и некоторых других геометрических объектов. *Обобщенные вербальные категории* — это двойные подкатегории базовых вербальных категорий с тем же самым классом объектов, такие, что соответствующий класс вертикальных стрелок замкнут относительно тензорных произведений.

Далее, определяется аналог *species of structures*, где место категории биекций конечных множеств занимает обобщенная вербальная категория, а место категории всех множеств - моноидальная категория с необходимыми свойствами. Мы будем использовать для этого понятия имеющийся в русском переводе “Теории множеств” Бурбаки термин *род структуры*. По данному роду структуры F определяется аналог аналитического (или полиномиального) функтора $\widetilde{F}$. Основным результатом доклада является следующий аналог теоремы А.Жояля [**4**]:

Теорема. *Пусть дана обобщенная вербальная категория и два заданных на ней рода структуры F и G. Тогда существует определенный с точностью до естественного изоморфизма род структуры $F \circ G$ такой, что $\widetilde{F} \cdot \widetilde{G} \cong \widetilde{F \circ G}$.*

Список литературы

[1] *Tronin S. N.* Verbal categories and analytic functors // Материалы конференции “Алгебра и математическая логика: теория и приложения” (г. Казань, 2-6 июня 2014 г.) и сопутствующей молодежной летней школы “Вычислимость и вычислимые структуры”. - Казань: Изд-во Казан. ун-та, 2014. - С.145-146.

[2] *Тронин С. Н.* Абстрактные клоны и операды // Сиб. мат. журн. — 2002. — Т. 43. — № 4. — С. 924–936.

[3] *Тронин С. Н.* Мультикатегории и многообразия многосортных алгебр // Сиб. мат. журн. — 2008. — Т. 49. — № 5. — С. 1185–1202.

[4] *Joyal A.* Foncteurs analitiques et espaces de structures // Lecture Notes in Math. — 1986. — V. 1234. — P. 126–159.

Казанский федеральный университет, Казань
E-mail: stronin@kpfu.ru

О вербальности категории перетасовок

С. Н. Тронин, А. Р. Гайнуллина

В работе [**1**] было показано, как можно использовать коммутативные операды [**2**] в криптографии с открытым ключом. В связи с этим оказалось важным изучить свободные коммутативные операды и их линеаризации, являющиеся многомерными аналогами алгебр многочленов. Существенной частью теории свободных коммутативных операд должны стать аналоги базисов Грёбнера-Ширшова. Такие базисы построены для некоммутативных операд [**3**]. В этой работе используется понятие перетасовок (shuffle) и соответствующих операд (см. также [**4**]). Нами показано, что:

Теорема. *Категория перетасовок является вербальной категорией* (*в смысле* [**5**], [**6**]).

Это позволяет использовать для построения базисов Грёбнера-Ширшова в случае коммутативных операд и их линеаризаций общую теорию операд над вербальными категориями [**6**].

Список литературы

[1] *Тронин С. Н., Гайнуллина А. Р.* Некоторые применения теории операд в криптографии с открытым ключом // Материалы международн. конф. “Алгебра и математическая логика: теория и приложения” (Казань, 2-6 июня 2014 г.). — Казань: Издательство Казанского университета. — 2014. — С. 147-148.

[2] *Тронин С. Н.* Операды и многообразия алгебр, определяемые полилинейными тождествами // Сиб. мат. журн. — 2006. — Т. 47. № 3. — С. 670-694.

[3] *Dotsenko V., Khoroshkin A.* Gröbner bases for operads // Duke Math. J. — 2010. — V. 153. No 2. — P. 363-396.

[4] *Méndez M.* Set Operads in Combinatorics and Computer Science. — Heidelberg-New York-Dordrecht-London: Springer International Publishing, 2015. – xv+129 p.

[5] *Тронин С. Н.* Абстрактные клоны и операды // Сиб. мат. журн. — 2002. — Т. 43. № 4. — С. 924-936.

[6] *Тронин С. Н.* Вербальные категории и тождества универсальных алгебр // Ученые записки Казанского университета. Серия Физико-математические науки. — 2012. — Т. 154. Кн. 2. — С. 125-141.

Казанский федеральный университет, Казань
E-mail: Serge.Tronin@kpfu.ru, GaynullinaAlina@gmail.com

Теория коммутаторов для модулярных алгебраических систем

В. И. Урсу

Теория коммутаторов, наряду с описанием конгруэнции в терминах трансляций А.И. Мальцева [**1**], в значительной части основываясь на них, дала толчок развитию многообразия модулярных алгебр. Основы этой теории, обобщение теории коммутаторов нормальных подгрупп в теории групп, были заложены в начале 70-х годов в работе Смита [**2**] для многообразия Мальцева (конгруэнц-перестановочные многообразия). Позже в [**3**] была изложена теория коммутаторов Хагеманна и Нерманна для модулярных многообразиий. Подробное изложение с многими применениями теории коммутаторов представлено в книге Р. Фриза и Р. Маккензи [**4**].

В [**5**] В.А. Горбунов задал иное определение конгруэнции на алгебраической системе, которое определено раньше (см. [**6**]). При таком определении конгруэнция связана не только с основными операциями, но и с основными отношениями, которые позволяют в значительной степени перенести результаты и методы для универсальной алгебры в теорию алгебраических систем. Следуя Гумму [**7**], в этой работе удалось описать теорию коммутаторов на языке конгруэнции алгебраической системы. Это позволило ввести понятия абелевых, нильпотентных и разрешимых алгебраических систем, которые являются обобщением понятий в универсальных алгебрах.

Список литературы

[1] *Мальцев А. И.* К общий теории алгебраических систем, Мат. сборник, 1954, 35, № 1, 3-20.

[2] *Smith J. D. H.* Mal'cev varieties, LNM 554, Berlin-Heidelberg-New York, 1976.

[3] *Hagemann J., Herrmann C.* A concrete ideal multiplication for algebraic systems and its relation to congruence distributivity, Arch. Math., 1979, 32, 234-245.

[4] *Freese R., McKenzie R.* Commutator theory for congruence modular varieties, London Mathematical Society Lecture Note Series 125, Cambridge University Press, Cambridge, 1987.

[5] *Горбунов В. А.* Алгебраическая теория квазимногообразии, Сибирская школа Алгебры и Логики, Новосибирск "Научная книга", 1999.

[6] *Горбунов В. А., Туманов В. И.* О строении решеток квазимногообразий, Доклады АН СССР, 1980, 254, № 2, 272-275.

[7] *Gumm H. P.* An easy way to the commutator in modular varieties, Arch. Math., 1980, 34, 220-228.

Институт математики "Симион Стойлов" Академии Румыни,
Технический Университет Молдовы
E-mail: Vasile.Ursu@imar.ro, vasileursumd@yahoo.com

Об экзистенциально замкнутых компаньонах кольца целых чисел

З. Г. Хисамиев

В работе изучаются экзистенционально замкнутые кольца в классе колец $\mathcal{C}(\mathbb{Z})$, являющихся модельными компаньонами кольца целых чисел $\mathbb{Z} = \langle Z;\ +,\ *\rangle$. Класс $\mathcal{C}(\mathbb{Z})$ состоит из всех колец, которые имеют, с точностью до изоморфизма, конечные подструктуры такие же как и $\mathbb{Z}$. Кольцо $\mathbb{R} \in \mathcal{C}(\mathbb{Z})$ называется экзистенционально замкнутым в классе $\mathcal{C}(\mathbb{Z})$, если любое его расширение $\mathbb{R}_1$ в классе $\mathcal{C}(\mathbb{Z})$, является его экзистенциональным расширением. Такой подход изучения классов структур и соответствующая проблематика были сформулированы в работах [**1**] и [**2**] и на семинарах по теории моделей в г.Алматы.

Предложение. 1. *Кольцо $\mathbb{Z}$ является экзистенционально замкнутым кольцом в классе $\mathcal{C}(\mathbb{Z})$.* 2. *Простое трансцендентное расширение $\mathbb{Z}[x]$ кольцо $\mathbb{Z}$ принадлежит классу $\mathcal{C}(\mathbb{Z})$, но не экзистенционально замкнуто в нем*

Теорема. *Пусть $f(\beta, x)$ – неприводимый многочлен над кольцом $\mathbb{Z}[\beta]$. Фактор кольцо $\mathbb{Z}[\beta]/f$ является модельным компаньоном кольца $\mathbb{Z}$, тогда и только тогда, когда число решений уравнения $f(\beta, x) = 0$, в целых числах бесконечно.*

Теорема. *Существует, по крайней мере, счетное число счетных, неизоморфных, экзистенционально замкнутых колец в классе $\mathcal{C}(\mathbb{Z})$.*

Список литературы

[1] *Нуртазин А. Т.* Компаньоны, Этот сборник, 2015.

[2] *Нуртазин А. Т.* Экзистенциально замкнутые структуры и их теории, Этот сборник, 2015.

Казахский национальный университет им.аль-Фараби, Алматы
E-mail: KhisamievZ@mail.ru

On Jónsson's problem for algebras of relations with domino operaions

D. A. Bredikhin

For any set Ω of operations on binary relations, denote by $R\{\Omega\}$ the class of all algebras isomorphic to ones whose elements are binary relations and whose operations are members of Ω. Let $Var\{\Omega\}$ $(Q\{\Omega\})$ be the variety (quasi-variety) generated by the class $R\{\Omega\}$. In the paper [**1**], B. Jónsson considered the class of algebras of relations with the operations of relation product $\circ$, relation inverse, and the intersection. He has shown that this class is a quasi-variety and raised the problem of whether it is a variety. Negative solution of this problem is obtained in [**2**]. Note that for Tarski's algebras of relations this problem has a positive solution. We will consider this problem for relation algebras with operations of relation product $\circ$ and unary domino operations [**3, 4**] that are defined as follows: for any binary relation $\rho \subseteq X \times X$,

$\nabla_1(\rho) = \{(u,v) : (\exists w)(w,u) \in \rho\}$ and $\nabla_2(\rho) = \{(u,v) : (\exists w)(v,w) \in \rho\}$.

The finity bases of identities for the varieties $Var\{\circ, \nabla_1\}$ and $Var\{\circ, \nabla_2\}$ are found in [**5**].

Theorem. *The classes $R\{\circ, \nabla_1\}$ and $R\{\circ, \nabla_2\}$ form a quasi-variety. The quasi-varieties $Q\{\circ, \nabla_1\}$ and $Q\{\circ, \nabla_2\}$ do not form a variety, i.e., $R\{\circ, \nabla_1\} = Q\{\circ, \nabla_1\} \neq Var\{\circ, \nabla_1\}$ and $R\{\circ, \nabla_2\} = Q\{\circ, \nabla_2\} \neq Var\{\circ, \nabla_2\}$.*

References

[1] *Jónsson B.* Represantation of modula lattices and of relation algebras. Trans. Amer. Math. Soc. 92, 449–464 (1959).

[2] *Andreka H., Bredikhin D. A.* The equational theory of union-free algebras of relations. Alg. Univers. 33, 516–532 (1994).

[3] *Kuhn S.* The domino relations: flattening a two-dimensional logic. Journal of Philosophical Logic. 2, 173–195 (1989).

[4] *Venema Y.* Many-dimensional modal logic. Universiteit van Amsterdam, Amsterdam, 1989.

[5] *Bredikhin D. A.* On identities of relation algebras wih domino operations. Russian Mathematics. 59, No 2, 435–436 (2015).

Saratov (Russia)
E-mail: bredikhin@mail.ru

Questions on indiscernibility of a set in weakly circularly minimal structures

B. Sh. Kulpeshov

Here we continue studying the notion of *weak circular minimality* originally introduced in [**1**]. A *circular* order relation is described by a ternary relation K satisfying the following conditions:

(co1) $\forall x \forall y \forall z (K(x,y,z) \to K(y,z,x))$;

(co2) $\forall x \forall y \forall z (K(x,y,z) \land K(y,x,z) \Leftrightarrow x=y \lor y=z \lor z=x)$;

(co3) $\forall x \forall y \forall z (K(x,y,z) \to \forall t [K(x,y,t) \lor K(t,y,z)])$;

(co4) $\forall x \forall y \forall z (K(x,y,z) \lor K(y,x,z))$.

A circularly ordered structure $M = \langle M, K, \ldots \rangle$ is *weakly circularly minimal* if any definable (with parameters) subset of M is a finite union of convex sets.

Let M be weakly circularly minimal and $p \in S_1(\emptyset)$ be non-algebraic. We consider the case when $p(M)$ is non-convex. Then obviously there exists $m > 1$ such that $p(M)$ is partitioned into m convex components, i.e. $p(M) = \cup_{i=1}^{m} U_i$, where each U_i is convex. In this case M is *m-convex*. Suppose that $K(U_1, \ldots, U_m)$.

We say that $p(M)$ is *2-indiscernible over $\emptyset$* if for all $\langle a_1, a_2 \rangle, \langle a_1', a_2' \rangle \in [p(M)]^2$ with $a_1 \neq a_2$, $a_1' \neq a_2'$ and either for some i $K(a_1, M, a_2) \subseteq U_i$ and $K(a_1', M, a_2') \subseteq U_i$ or $\langle a_1, a_2 \rangle, \langle a_1' a_2' \rangle \in U_i \times U_j$ where $i \neq j$ we have that $tp(\langle a_1, a_2 \rangle / \emptyset) = tp(\langle a_1', a_2' \rangle / \emptyset)$. We say that $p(M)$ is *n-indiscernible over $\emptyset$* $(n \geq 3)$ if for all n, k, $n_1, \ldots, n_k$ ш $i_1, \ldots, i_k$ such that $k \leq m$, $n_1 + \ldots + n_k = n$ and $1 \leq i_1 < i_2 < \ldots < i_k \leq m$, and all n-tuples $\bar{a} = \langle a_1^{i_1}, \ldots, a_{n_1}^{i_1}; \ldots; a_1^{i_k}, \ldots, a_{n_k}^{i_k} \rangle$, $\bar{b} = \langle b_1^{i_1}, \ldots, b_{n_1}^{i_1}; \ldots; b_1^{i_k}, \ldots, b_{n_k}^{i_k} \rangle \in [p(M)]^n$ with $a_j^{i_s}, b_j^{i_s} \in U_{i_s}$ for all $j \in \{1, \ldots, n_s\}$, $s \in \{1, \ldots, k\}$, $K(a_1^{i_1}, \ldots, a_{n_k}^{i_k})$ and $K(b_1^{i_1}, \ldots, b_{n_k}^{i_k})$, we have that $tp(\bar{a}/\emptyset) = tp(\bar{b}/\emptyset)$. We also say that $p(M)$ is *indiscernible over $\emptyset$* if for every $n \in \omega$ $p(M)$ is n-indiscernible over $\emptyset$.

We say that a family of convex components $\{U_1, \ldots, U_s\}$ of p is *weakly orthogonal over $\emptyset$* if every s-tuple $\langle a_1, \ldots, a_s \rangle \in U_1 \times \ldots \times U_s$ satisfies the same type over $\emptyset$. We say that p has *convexity rank 1* $(RC(p) = 1)$ if there is no parametrically definable equivalence relation with infinitely many infinite convex classes in $p(M)$.

We prove the following theorem that is a criterion for indiscernibility of the set of realizations of a non-algebraic 1-type with convexity rank 1.

Theorem. *Let M be an $\aleph_0$-categorical m-convex weakly circularly minimal structure, $m > 1$, $p \in S_1(\emptyset)$ — non-algebraic, $RC(p) = 1$. Then $p(M)$ is indiscernible over $\emptyset$ iff the family of all convex components of p is pairwise weakly orthogonal over $\emptyset$.*

References

[1] *Kulpeshov B. Sh., Macpherson H. D.* Minimality conditions on circularly ordered structures, Mathematical Logic Quarterly, 51 (2005), pp. 377–399.

International Information Technologies University, Almaty (Kazakhstan)
E-mail: b.kulpeshov@iitu.kz

Finitely generated free algebras with hyperidentities of lattice varieties

Yu. M. Movsisyan

It is commonly known that the free Boolean algebra on n free generators is isomorphic to the Boolean algebra of Boolean functions of n variables. The free distributive lattice on n free generators is isomorphic to the lattice of monotone Boolean functions of n variables. A problem posed by B.I. Plotkin in 1970s has required finding the varieties of algebras with analogous functional representations of free finitely generated algebras. In this talk we present the varieties of algebras with similar functional representations of free finitely generated algebras.

References

[1] *Movsisyan Yu. M.* Hyperidentities in algebras and varieties // Uspekhi Matematicheskikh Nauk, 53 (1998), pp. 61–114. English translation in Russian Mathematical Surveys 53(1998), pp. 57–108.

Yerevan State University, Yerevan (Armenia)
E-mail: yurimovsisyan@yahoo.com

Representations of regular rings and complemented involutive lattices

M. V. Schwidefsky and C. Herrmann

An involutive lattice [an algebra with involution, or a $*$-algebra] S is representable, if there is a pre-hermitean space V_F such that A embeds into the subspace lattice [into the endomorphism algebra] of V_F, where involution is defined via orthogonality. Several results on representable structures are presented. Among those are:

— The class of representable complemented modular involutive lattices [of representable modular orholattices, $*$-Λ-algebras, respectively] is closed under homomorphic images;

— $\exists$-[semi]-varieties of representable structures are generated by subspace lattices [endomorphism algebras, respectively] of finite-dimensional spaces;

— There is a one-to-one correspondence between certain *exists*-semivarieties of Arguesian complemented involutive lattices [of regular $*$-Λ-algebras, respectively] and semivarieties of pre-hermitean spaces.

— For a semivariety of pre-hermitean spaces, the class of representable structures forms an $\exists$-variety.

IM SB RAS, Novosibirsk (Russia)
E-mail: udav17@gmail.com

On e-spectra of theories of E-combinations and P-combinations

S. V. Sudoplatov

Let E be an equivalence relation, $(\mathcal{A}_i)_{i\in I}$ be a family of relational structures such that each E-class is a universe of $\mathcal{A}_i$, $i \in I$, E-classes are disjoint for distinct $\mathcal{A}_i$, and the symbol E is disjoint with languages for the structures $\mathcal{A}_j$, $j \in I$. The structure $\mathcal{A}_E \rightleftharpoons \bigcup\limits_{i\in I} \mathcal{A}_i$ expanded by the predicate E is the E-*union* of the structures $\mathcal{A}_i$, and the operator mapping $(\mathcal{A}_i)_{i\in I}$ to $\mathcal{A}_E$ is the E-*operator*. The structure $\mathcal{A}_E$ is also called the E-*combination* of the structures $\mathcal{A}_i$ and denoted by $\mathrm{Comb}_E(\mathcal{A}_i)_{i\in I}$; here $\mathcal{A}_i = (\mathcal{A}_E \upharpoonright A_i) \upharpoonright \Sigma(\mathcal{A}_i)$, $i \in I$. Structures $\mathcal{A}'$, which are elementary equivalent to $\mathcal{A}_E$, are also considered as E-combinations.

For a structure $\mathcal{A}_E$ the number of *new* structures with respect to the structures $\mathcal{A}_i$, i. e., of the structures $\mathcal{B}$ which are structures of E-classes in $\mathcal{A}' \equiv \mathcal{A}_E$, pairwise elementary non-equivalent and elementary non-equivalent to the structures $\mathcal{A}_i$, is called the e-*spectrum* of $\mathcal{A}_E$ and denoted by e-$\mathrm{Sp}(\mathcal{A}_E)$. The value $\sup\{e\text{-}\mathrm{Sp}(\mathcal{A}')) \mid \mathcal{A}' \equiv \mathcal{A}_E\}$ is called the e-*spectrum* of the theory $T = \mathrm{Th}(\mathcal{A}_E)$ and denoted by e-$\mathrm{Sp}(T)$.

Clearly, for a given language Σ, $0 \leq e\text{-}\mathrm{Sp}(\mathrm{Th}(\mathcal{A}_E)) \leq 2^{\max\{|\Sigma|,\omega\}}$.

Theorem 1. *For any cardinality λ there is a theory $T = \mathrm{Th}(\mathcal{A}_E)$ of a language Σ such that $|\Sigma| = |\lambda + 1|$ and e-$\mathrm{Sp}(T) = \lambda$.*

Theorem 2. *For any infinite cardinality λ there is a theory $T = \mathrm{Th}(\mathcal{A}_E)$ of a language Σ such that $|\Sigma| = \lambda$ and e-$\mathrm{Sp}(T) = 2^\lambda$.*

Replacing E-classes by unary predicates P_i (not necessary disjoint) being universes for structures $\mathcal{A}_i$, we get the notions of P-*combination* $\mathcal{A}_P$, the P-*operator*, and the e-spectrum e-$\mathrm{Sp}(\mathrm{Th}(\mathcal{A}_P))$. We have $e\text{-}\mathrm{Sp}(\mathrm{Th}(\mathcal{A}_P)) \neq 1$ for any countable theory $\mathrm{Th}(\mathcal{A}_P)$ with the complete type $p_\infty(x) = \{\neg P_i(x) \mid i \in I\}$ having non-symmetric or definable semi-isolation. Applying constructions in [**1**], the results for E-combinations are modified for P-combinations:

Theorem 3. *For any cardinality λ there is a theory $T = \mathrm{Th}(\mathcal{A}_P)$ of a language Σ such that $|\Sigma| = \max\{\lambda, \omega\}$ and e-$\mathrm{Sp}(T) = \lambda$.*

Theorem 4. *For any infinite cardinality λ there is a theory $T = \mathrm{Th}(\mathcal{A}_P)$ of a language Σ such that $|\Sigma| = \lambda$ and e-$\mathrm{Sp}(T) = 2^\lambda$.*

The research is partially supported by Committee of Science in Education and Science Ministry of the Republic of Kazakhstan, Grant No. 0830/GF4.

References

[1] *Sudoplatov S. V.* Classification of Countable Models of Complete Theories. — Novosibirsk : NSTU, 2014.

Sobolev Institute of Mathematics, Novosibirsk State Technical University, Novosibirsk State University, Novosibirsk (Russia)
E-mail: sudoplat@math.nsc.ru

On categorical properties of Jonsson sets

A. R. Yeshkeyev

Let L is a countable language of first order. Let T - perfect Jonsson theory complete for existential sentences in the language L and its semantic model is a C.

Definition 1. We say that a set X - Σ-definable if it is definable by some existential formula. The set X is called *Jonsson in theory* T, if it satisfies the following properties: 1) X is Σ-definable subset of C; 2) $Dcl(X)$ is the support of some existentially closed submodel of C.

The set X is called *algebraically Jonsson in theory* T, if it satisfies the following properties: 1) X is Σ-definable subset of C; 2) $Acl(X)$ is the support of some existentially closed submodel of C.

Definition 2. An existentially closed model M is said to be *minimal* if any Σ-definable subset of M using parameters is either finite or a complement of a finite one.

Definition 3. An algebraically Jonsson set A is said to be *independent* if $\mathrm{acl}(A) \neq \mathrm{acl}(A')$ for any proper subset $A' \subset A$.

A maximal independent subset of a algebraically Jonsson set A is said to be a *basis* of A.

Lemma. Any two bases B and C of a algebraically Jonsson set A are of the same cardinality

Definition 4. Let M be an existentially closed minimal model of theory T and let $D \subseteq M^n$ be an infinite algebraically Jonsson set in theory T. We say that D is *minimal* in M if for any definable $Y \subseteq D$ either Y is finite or $D \setminus Y$ is finite. If $\phi(\bar{v}, \bar{a})$ is the formula that defines D, then we also say that $\phi(\bar{v}, \bar{a})$ is minimal.

We say that D and ϕ are *strongly minimal* if ϕ is minimal in any existentially closed extension N of M. We say that a Jonsson theory T is strongly minimal if for any $M \in E_T$ every Σ-definable subset of M is either finite or cofinite.

Definition 5. Let $A, B \in E_T$ and $A \subset B$. Then B called *algebraically prime model extension* A in E_T if for any model $C \in E_T$ such that A is isomorphically embedded in C then B isomorphically embedded in the C.

Let X is algebraically Jonsson set, $\mathrm{acl}(X)$=M, formula which define the set X is existential strongly minimal formula. Let us consider $Th_{\forall\exists}(M) = T_M$.

Theorem 1. *The following conditions are equivalent:*

1) T^*_M is ω_1-categorical; 2) any countable model of E_{T_M} has a prime algebraic extension in E_{T_M}.

Let X Jonsson set and M is existentially closed model where $\mathrm{dcl}(X)$=M.

Theorem 2. *Let T_M be as above. Then the following conditions are equivalent:*

1) T_M is complete; 2) T_M is model complete.

Karaganda State University, Karaganda (Kazakhstan)
E-mail: modth1705@mail.ru

Similarity of Jonsson sets

A. R. Yeshkeyev, O. I. Ulbrikht, M. T. Kasymetova

Let T be an arbitrary Jonsson theory, then $E(T) = \bigcup\limits_{n<\omega} E_n(T)$, where $E_n(T)$ is the lattice of existential formulas with exactly n free variables.

Let T_1 and T_2 be Jonsson theories.

We shall say that T_1 and T_2 are *J-syntactically similar* if and only if there exists a bijection $f : E(T_1) \to E(T_2)$ such that:

1) the restriction of f up $E_n(T_1)$ is isomorphism of the $E_n(T_1)$ and $E_n(T_2)$, $n < \omega$;

2) $f(\exists v_{n+1}\varphi) = \exists v_{n+1} f(\varphi)$, $\varphi \in E_n(T)$, $n < \omega$,

3) $f(v_1 = v_2) = (v_1 = v_2)$.

Let us recall the definition of a polygon.

Definition 1. By a polygon over a monoid S we mean a structure with only unary functions $\langle A; f_{\alpha:\alpha\in S}\rangle$ such that

(i) $f_e(a) = a, \forall a \in A$, where e is the unit of S;

(ii)$f_{\alpha\beta}(a) = f_\alpha(f_\beta(a)), \forall \alpha, \beta \in S, \forall a \in A$.

Definition 2. We say that a set X is Σ-definable if it is definable by some existential formula.

The set X is called *algebraically Jonsson in theory* T, if it satisfies the following properties: 1) X is Σ-definable subset of C; 2) $Acl(X)$ is the support of some existentially closed submodel of C.

Let us consider $Th_{\forall\exists}(M) = T_M$.

Definition 3. Algebraically Jonsson sets X and Y are *syntactically similar* between each other if syntactically similar correspondingly its T_{M_1} and T_{M_2}, where acl(X)=M_1, acl(Y)=M_2.

If X and Y are syntactically similar between each other, then we have the following result:

Theorem. *Let T_{M_1} and T_{M_2} be $\exists$-complete perfect Jonsson theories. Then the following conditions equivalent:*

1) $T^*_{M_1}$ and $T^*_{M_2}$ are syntactically similar as complete theories as in [**1**]*;*

2) T_{M_1} and T_{M_2} are J-syntactical similar.

Corollary. *For each algebraically Jonsson set there exist J-syntactically similar a some Σ-complete perfect Jonsson theory of polygons, such that its center is model complete.*

References

[1] *Mustafin T. G.* On similarities of complete theories // Lecture Notes in Logic. 1993. V. 2. P. 259-265.

Karaganda State University, Karaganda (Kazakhstan)
E-mail: modth1705@mail.ru, ulbrikht@mail.ru, mairushaasd@mail.ru

On free left n-dinilpotent dimonoids

A. V. Zhuchok, Yuliia V. Zhuchok

As usual, $\mathbb{N}$ denotes the set of all positive integers. Let $(D, \dashv, \vdash)$ be a dimonoid [1] and $x_1, \ldots, x_n \in D$. By $T(x_1, \ldots, x_n)$ we denote the set of all expressions of the form $x_1 \circ_1 \ldots \circ_{n-1} x_n$ with parenthesizing, giving rise to elements in D; here $\circ_1, \ldots, \circ_{n-1} \in \{\dashv, \vdash\}$. A dimonoid $(D, \dashv, \vdash)$ will be called left dinilpotent, if for some $n \in \mathbb{N}$, any $x \in D$ and any $t(x_1, \ldots, x_n) \in T(x_1, \ldots, x_n)$ the following identities hold:

$$t(x_1, \ldots, x_n) \dashv x = t(x_1, \ldots, x_n), \quad t(x_1, \ldots, x_n) \vdash x = x_1 \vdash \ldots \vdash x_n.$$

The least such n we shall call the left dinilpotency index of $(D, \dashv, \vdash)$. For $k \in \mathbb{N}$ a left dinilpotent dimonoid of left dinilpotency index $\leq k$ is said to be left k-dinilpotent. The notion of a left dinilpotent dimonoid is an analog of the notion of a left nilpotent semigroup [2]. It is clear that operations of any left 1-dinilpotent dimonoid coincide and it is a left zero semigroup. The class of all left n-dinilpotent dimonoids forms a subvariety of the variety of all dimonoids. A dimonoid which is free in the variety of left n-dinilpotent dimonoids will be called a free left n-dinilpotent dimonoid.

Let X be an arbitrary nonempty set, $F[X]$ be the free semigroup on X and $w \in F[X]$. The length of w will be denoted by l_w. Fix $n \in \mathbb{N}$. If $l_w \geq n$, by $\overset{n}{\overrightarrow{w}}$ denote the initial subword with the length n of w. Define operations $\dashv$ and $\vdash$ on $F_n = \{(w, m) \in F[X] \times \mathbb{N} \mid m \leq l_w \leq n\}$ by

$$(w_1, m_1) \dashv (w_2, m_2) = \begin{cases} (w_1 w_2, m_1), & l_{w_1} + l_{w_2} \leq n, \\ (\overset{n}{\overrightarrow{w_1 w_2}}, m_1), & l_{w_1} + l_{w_2} > n, \end{cases}$$

$$(w_1, m_1) \vdash (w_2, m_2) = \begin{cases} (\overset{n}{\overrightarrow{w_1 w_2}}, n), & n < l_{w_1} + m_2, \\ (\overset{n}{\overrightarrow{w_1 w_2}}, l_{w_1} + m_2), & l_{w_1} + m_2 \leq n < l_{w_1} + l_{w_2}, \\ (w_1 w_2, l_{w_1} + m_2), & l_{w_1} + l_{w_2} \leq n \end{cases}$$

for all $(w_1, m_1), (w_2, m_2) \in F_n$. The algebra $(F_n, \dashv, \vdash)$ will be denoted by $FD_n^l(X)$.

Theorem. *$FD_n^l(X)$ is the free left n-dinilpotent dimonoid.*

We also consider separately free left n-dinilpotent dimonoids of rank 1 and characterize the least left n-dinilpotent congruence on a free dimonoid. In order to construct free right n-dinilpotent dimonoids and characterize the least right n-dinilpotent congruence on a free dimonoid we use the duality principle.

References

[1] *Zhuchok A. V.* Dimonoids, Algebra and Logic, 50 (2011), no. 4, 323–340.

[2] *Schein B. M.* One-sided nilpotent semigroups, Uspekhi Mat. Nauk, 19:1 (115) (1964), 187–189 (in Russian).

Luhansk Taras Shevchenko National University, Starobilsk (Ukraine)
E-mail: zhuchok_a@mail.ru, yulia.mih@mail.ru

On free abelian digroups

Yuriĭ V. Zhuchok

The notion of a digroup first appeared in Loday's work [**1**] and it is based on the notion of a dimonoid. An algebra $(D, \dashv, \vdash)$ with two binary associative operations $\dashv$ and $\vdash$ is called a *dimonoid* if for all $x, y, z \in D$ the following conditions hold:

$$(x \dashv y) \dashv z = x \dashv (y \vdash z),$$
$$(x \vdash y) \dashv z = x \vdash (y \dashv z),$$
$$(x \dashv y) \vdash z = x \vdash (y \vdash z).$$

A dimonoid $(D, \dashv, \vdash)$ is called a *digroup* if there exists $e \in D$ such that for all $g \in D$,

$$e \vdash g = g = g \dashv e,$$

and for every $g \in D$ there exists a unique element $g^{-1} \in D$ such that

$$g \vdash g^{-1} = e = g^{-1} \dashv g.$$

A digroup $(D, \dashv, \vdash)$ is called *abelian* [**2**] if for all $x, y \in D$,

$$x \dashv y = y \vdash x.$$

It is clear that the notion of a digroup generalizes the notion of a group. Digroups and related systems have been studied by many authors (see, e.g., [**2**]–[**4**]).

Let X be an arbitrary nonempty set, $X^{-1} = \{x^{-1} \mid x \in X\}$ and $X' = X \cup X^{-1}$. Denote by $FAg(X)$ the free abelian group on X and put

$$FAd(X) = X' \times FAg(X).$$

Define binary operations $\dashv$ and $\vdash$ on $FAd(X)$ as follows:

$$(x; u) \dashv (y; v) = (x; uyv), \ \ (x; u) \vdash (y; v) = (y; xuv).$$

Theorem. *The algebra* $(FAd(X), \dashv, \vdash)$ *is a free abelian digroup.*

If ρ is a congruence on a dimonoid $(D, \dashv, \vdash)$ such that $(D, \dashv, \vdash)/\rho$ is an abelian digroup, we say that ρ is an abelian digroup congruence.

In addition, we construct a digroup which is isomorphic to the free abelian digroup of rank 1 and describe the least abelian digroup congruence on a free dimonoid.

References

[1] *Loday J.-L.* Dialgebras, in: Dialgebras and related operads, Lect. Notes Math., 1763, Springer-Verlag, Berlin, 2001, 7–66.

[2] *Felipe R.* Generalized Loday algebras and digroups, Comunicaciones del CIMAT, no. I-04-01/21-01-2004.

[3] *Phillips J. D.* A short basis for the variety of digroups, Semigroup Forum, 70 (2005), 466–470.

[4] *Zhuchok A. V.* Dimonoids, Algebra and Logic, 50 (2011), no. 4, 323–340.

Taras Shevchenko National University of Kyiv, Kyiv (Ukraine)
E-mail: zhuchok_y@mail.ru

VII. Секция «Неклассические логики»

Фрагмент исчисления Ламбека с итерацией

С. Л. Кузнецов, Н. С. Рыжкова

Определим исчисление Ламбека без умножения $L(\backslash, /)$ [**1**]. Его типы (формулы) строятся из примитивных типов $p_1, p_2, \ldots$ с помощью связок $\backslash$ (левое деление) и $/$ (правое деление). Секвенции $L(\backslash, /)$ имеют вид $\Gamma \to A$, где Γ — последовательность типов, A — тип. Аксиомы имеют вид $A \to A$. Правила вывода таковы:

$$\frac{A\,\Pi \to B}{\Pi \to A\backslash B}, \text{ где } \Pi \text{ непуста;} \qquad \frac{\Pi \to A \quad \Gamma\, B\, \Delta \to C}{\Gamma\, \Pi\, (A\backslash B)\, \Delta \to C}$$

Правила для другого деления ($/$) симметричны.

Каждый тип A интерпретируется формальным языком $w(A) \subseteq \Sigma^+$ (Σ — алфавит): $w(p_i)$ произвольны, $w(A\backslash B) = w(A)\backslash w(B) = \{u \in \Sigma^+ \mid (\forall v \in w(A))\ vu \in w(B)\}$, $w(B/A) = w(B)/w(A) = \{u \in \Sigma^+ \mid (\forall v \in w(A))\ uv \in w(B)\}$.

Имеет место **теорема о полноте** [**2**]: $L(\backslash, /) \vdash A_1 \ldots A_n \to B$ *тогда и только тогда, когда* $w(A_1) \cdot \ldots \cdot w(A_n) \subseteq w(B)$ *для всех* w.

Интерес представляет расширение исчисления Ламбека новой одноместной связкой $(\cdot)^+$ *(итерация)*, так что $w(A^+) = \{u_1 \ldots u_n \mid n \geqslant 1, u_i \in w(A)\}$. Мы рассматриваем ограниченное расширение, где A^+ может появляться лишь в знаменателях. Можно считать, что мы добавляем две составные связки: ${}^+\backslash$ и $/^+$.

Исчисление $L(\backslash, /, {}^+\backslash, /^+)_\omega$ получается добавлением к $L(\backslash, /)$ правил

$$\frac{A^n\Pi \to B \text{ для всех } n \geqslant 1}{\Pi \to A^+\backslash B} \qquad \frac{\Gamma\, B\, \Delta \to C \quad \Pi_i \to A\ (i = 1, \ldots, n)}{\Gamma\, \Pi_1 \ldots \Pi_n\, (A^+\backslash B)\, \Delta \to C}$$

(и аналогичных для другого деления). Первое из этих правил имеет бесконечно много посылок, таким образом, вывод будет деревом с бесконечным ветвлением.

Исчисление $L(\backslash, /, {}^+\backslash, /^+)_\infty$ получается добавлением правил

$$\frac{A\,\Pi \to B \quad A\,\Pi \to A^+\backslash B}{\Pi \to A^+\backslash B} \qquad \frac{\Pi \to A \quad \Gamma\, B\, \Delta \to C}{\Gamma\, \Pi\, (A^+\backslash B)\, \Delta \to C} \qquad \frac{\Pi \to A \quad \Gamma\, (A^+\backslash B)\, \Delta \to C}{\Gamma\, \Pi\, (A^+\backslash B)\, \Delta \to C}$$

(и аналогичных для другого деления). При этом в выводах допускаются бесконечные ветви (они могут появляться за счёт применения первого из правил).

Теорема. *Исчисления* $L(\backslash, /, {}^+\backslash, /^+)_\infty$ *и* $L(\backslash, /, {}^+\backslash, /^+)_\omega$ *эквивалентны между собой и полны относительно интерпретации типов формальными языками.*

Список литературы

[1] *Ламбек И.* Математическое исследование структуры предложений. Математическая лингвистика: сборник переводов. М.: Мир, 1964. С. 47–68.

[2] *Buszkowski W.* Compatibility of a categorial grammar with an associated category system // Zeitschrift für mathematische Logik und Grundlagen der Mathematik. 1982. Vol. 28. P. 539–548.

Математический институт им. В. А. Стеклова РАН, Москва
Московский государственный университет им. М. В. Ломоносова, Москва
E-mail: sk@mi.ras.ru

Допустимые правила вывода линейной логики Знания и Времени LTK_r с интранзитивным отношением времени. Гипотеза о конечной аксиоматизируемости LTK_r.

А. Н. Лукьянчук

Зафиксируем язык $\mathcal{L}^{LTK}$, состоящий из счетного множества пропозициональных переменных, стандартных булевых операций $\{\wedge, \vee, \to, \neg\}$, множества одноместных модальных операторов $\{\Box_T, \Box_\sim, \Box_i (1 \leq i \leq k)\}$ и вспомогательных символов (скобок).

В [**1**] семантически определена логика Знания и Времени LTK_r с интранзитивным и рефлексивным отношением времени, как множество формул языка $\mathcal{L}^{LTK}$, истинных на LTK_r-фреймах специального вида. Была доказана

Теорема 1 *Логика LTK_r разрешима относительно допустимости правил вывода.*

Рассотрим следующую аксиоматическую систему AS_{LTK_r}:
Аксиомы **CPC** (классического пропозиционального исчисления);
$L_{\Box_T}$: $\Box_T(\Box_T A \to B) \vee \Box_T(\Box_T B \to A)$;
$K_{\Box_\xi}$: $\Box_\xi(A \to B) \to (\Box_\xi A \to \Box_\xi B)$, $\xi \in \{T, \sim, 1, \dots, k\}$;
$T_{\Box_\xi}$: $\Box_\xi A \to A$, $\xi \in \{T, \sim, 1, \dots, k\}$;
$4_{\Box_\xi}$: $\Box_\xi A \to \Box_\xi \Box_\xi A$, $\xi \in \{\sim, 1, \dots, k\}$;
$5_{\Box_\xi}$: $\neg\Box_\xi A \to \Box_\xi \neg\Box_\xi A$, $\xi \in \{\sim, 1, \dots, k\}$;
$Tr.C.1$: $\Diamond_T \Diamond_\sim A \to \Diamond_T A$;
$Tr.C.2$: $\Diamond_\sim \Diamond_T A \to \Diamond_T A$.
AL: $\Box_\sim A \wedge \Box_\sim B \wedge \Diamond_T(\neg A \wedge \Box_\sim B) \to \Box_T B$.
$M.1$: $\Box_T A \to \Box_\sim A$;
$M.2$: $\Box_\sim A \to \Box_i A$, $1 \leq i \leq k$;

Правила вывода AS_{LTK_r}:

$$MP : \frac{A, A \to B}{B} \quad Nec : \frac{A}{\Box_\xi A}$$

Определим $LTK_{r_{ax}} := \{A \in Fma(\mathcal{L}^{LTK}) | \vdash_{AS_{LTK_r}} A\}$.

Доказано:
Теорема 2. $\forall A \in Fma(\mathcal{L}^{LTK})$ $(A \in LTK_{r_{ax}} \Longrightarrow A \in LTK_r)$.

В данный момент исследуется вопрос конечной аксиоматизируемости логики LTK_r, в том числе рассматривается следующая гипотеза:

Гипотеза 1. *Система AS_{LTK_r} образует полную систему аксиом логики LTK_r.*

Список литературы

[1] *Lukyanchuk A.* Decidability of multi-modal logic LTK of linear time and knowledge // Journal of Siberian Federal University. 2013. Vol. 6, № 2. P. 220–226.

Сибирский Федеральный Университет, Красноярск
E-mail: a.lukyanchuk@inbox.ru

Интервалы Одинцова и интерполяция над минимальной логикой

Л. Л. Максимова, В. Ф. Юн

Статья посвящена проблеме интерполяции в расширениях минимальной логики J Йохансона [**1**].

С. П. Одинцов [**2**] предложил классификацию J-логик в соответствии с их интуиционистскими и негативными напарниками, при этом все логики разбиваются на интервалы. Более точно, для любой L определяются ее интуиционистский и негативный напарники [**2**]: $L_{int} = L + (\bot \to p)$, $L_{neg} = L + \bot$.

Пусть L_1 – с.и.л., L_2 – негативная логика.

$$[L_1; L_2] = \{L|\ L_{int} = L_1,\ L_{neg} = L_2\}.$$

$$L_1 * L_2 = \mathrm{J} + \{I(A)|\ A \in L_1\} + \{\bot \to B|\ B \in L_2\},$$

где $I(A)$ есть результат подстановки в A формулы $p_k \vee \bot$ вместо каждой переменной p_k.

Теорема. [**2**] *Для любых с.и.л. L_1 и негативной L_2 множество $[L_1; L_2]$ образует интервал с нижним концом $L_1 * L_2$ и верхним концом $L_1 \cap L_2$.*

В [**3**] доказано, что верхний конец интервала имеет интерполяционное свойство Крейга CIP тогда и только тогда, когда оба его напарника имеют CIP.

Доказано, что такой же результат верен для нижних концов интервалов:

Теорема 1. *Логика $L_1 * L_2$ имеет CIP тогда и только тогда, когда L_1 и L_2 имеют CIP.*

Также показана узнаваемость всех концов, которые имеют CIP, и найдена их семантическая характеризация.

Теорема 2. *Если L_1 и L_2 имеют CIP, то $L_1 * L_2$ и $L_1 \cap L_2$ узнаваемы над J.*

Список литературы

[1] *Johansson I.* Der Minimalkalkül, ein reduzierter intuitionistischer Formalismus // Compositio Mathematica. 1937. Vol. 4. P. 119–136.

[2] *Odintsov S.* Logic of classic refutability and class of extensions of minimal logic // Logic and Logical Philosophy. 2001. Vol. 9. P. 91–107.

[3] *Максимова Л. Л.* Неявная определимость в расширениях минимальной логики // Логические исследования. 2001. Т. 8 (2001). С. 72–81.

Институт математики им. С. Л. Соболева, Новосибирск
E-mail: lmaksi@math.nsc.ru, veta_v@mail.ru

Теорема о характеризации для квадрата симметричной логики

И. И. Осипов

Классический результат Ван Бентема [**1**] позволяет описать в терминах бисимуляций множество всех первопорядковых формул, эквивалентных в классе всех моделей стандартным переводам модальных формул. Этот результат распространяется на класс всех конечных моделей (теорема Ван Бентема-Розена [**1**]), но его нельзя обобщить, например, на случай конечных транзитивных моделей [**3**].

В бимодальном случае оказывается возможным обобщить теорему Ван Бентема на классы конечных моделей на шкалах логики K × K и логики KB × KB.

Определение. *Произведением шкал* $F_1 = (W_1, R_1)$ *и* $F_2 = (W_2, R_2)$ *называется шкала с двумя отношениями* $F_1 \times F_2 = (W_1 \times W_2, R_h, R_v)$, *где* $(u, v)R_h(u', v') \Leftrightarrow uR_1u'$ *и* $v = v'$, $(u, v)R_v(u', v') \Leftrightarrow u = u'$ *и* vR_2v'.

Определение. $L \times L = Log\{F_1 \times F_2 \mid F_1, F_2$ *– шкалы* $L\}$.

Как можно заметить, не все шкалы логики K × K являются произведениями шкал. Множество всех ее шкал составляют шкалы с двумя коммутирующими отношениями, обладающие свойством Черча-Россера [**2**]. Множество шкал логики KB × KB составляют шкалы с двумя симметричными коммутирующими отношениями.

Определение. *Бисимуляцией между моделями*

$$M = (W, R_1, R_2, \vec{P}) \quad \text{и} \quad M' = (W', R_1', R_2', \vec{P}')$$

называется непустое отношение $E \subset W \times W'$ *такое, что для любых* $w, v \in W$, $w', u' \in W'$ *если* $(w, w') \in E$, *то:*
1) $\forall i(P_i(w) = P_i'(w'))$,
2) $wR_1v \Rightarrow \exists v'(w'R_1'v' \wedge vEv')$, $wR_2v \Rightarrow \exists v'(w'R_2'v' \wedge vEv')$
3) $w'R_1u' \Rightarrow \exists u(wR_1u \wedge uEu')$, $w'R_2u' \Rightarrow \exists u(wR_2u \wedge uEu')$.

Теорема. *1) Пусть* C *– класс конечных моделей на шкалах логики* KB × KB, $\phi(x)$ *– формула первого порядка от одной переменной в сигнатуре с двумя отношениями и семейством одноместных предикатов. Тогда* $\phi(x)$ *эквивалентна в классе* C *стандартному переводу бимодальной формулы тогда и только тогда, когда* $\phi(x)$ *сохраняется при бисимуляциях в классе* C.

2) Аналогичное утверждение верно, если в качестве C *взять класс конечных моделей на шкалах логики* K × K.

Список литературы

[1] *Goranko V., Otto M.* Model Theory of Modal Logics. In: Handbook of Modal Logic. Elsevier, 2006. P. 255–325.

[2] *Gabbay D., Shehtman V.* Products of Modal Logics, part 1 // Logic Journal of the IGPL. 1998. Vol. 6. P. 73–146.

[3] *Dawar A., Otto M.* Modal Characterisation Theorems over Special Classes of Frames // Annals of Pure and Applied Logic. 2009. Vol. 161. P. 1–42.

Институт проблем передачи информации РАН, Москва
E-mail: osipovilia@gmail.com

Некоторые свойства безранговых кванторов

Х. М. Рухая, Л. М. Тибуа, Г. О. Чанкветадзе

Работа является продолжением работы [1]. В нём определены [2] безранговые кванторы существования и всеобщности и сформулированы некоторые их свойства [3,4].

$$\exists^{n+1} x A_1 \ldots A_n A — (\tau_x \wedge^{n+1} A_1 \ldots A_n A/x) \wedge^{n+1} A_1 \ldots A_n A$$

Читается: "существует такой x свойств$A_1, \ldots, A_n$, который имеет свойство A, $n = 0, 1, \ldots$.

$$\forall^{n+1} x A_1 \ldots A_n A — \neg \exists^{n+1} x A_1 \ldots A_n \neg A$$

Читается: каждый x свойств $A_1, \ldots, A_n$ имеет свойство A,$n = 0, 1, \ldots$.
Заметим, что если с вышеопределенных операторов убрать верхние индексы, то получим безранговые кванторы.

(1) $\forall x A_1 \ldots A_n A \to (T/x)[[\wedge A_1 \ldots A_n] \to A]$
(2) $\neg \forall x A_1 \ldots A_n A \leftrightarrow \exists x A_1 \ldots A_n \neg A$
(3) $\forall x A_1 \ldots A_n \neg A \leftrightarrow \neg \exists x A_1 \ldots A_n A$
(4) $\forall x A_1 \ldots A_n [A \wedge B] \leftrightarrow [\forall x A_1 \ldots A_n A \wedge \forall x A_1 \ldots A_n B]$
(5) $\exists x A_1 \ldots A_n [A \vee B] \leftrightarrow [\exists x A_1 \ldots A_n A \vee \exists x A_1 \ldots A_n B]$
(6) $\forall x A_1 \ldots A_n A \leftrightarrow \forall x [[A_1 \ldots A_n] \to A]$
(7) $\exists x A_1 \ldots A_n A \leftrightarrow \exists x [[A_1 \wedge \ldots \wedge A_n] \wedge A]$
Если символ x не имеет свободное вхождение в A, то
(8) $\forall x A_1 \ldots A_n [A \vee B] \leftrightarrow [A \vee \forall x A_1 \ldots A_n B]$
(9) $\forall x A_1 \ldots A_n [A \wedge B] \leftrightarrow [A \wedge \forall x A_1 \ldots A_n B]$

Если $\forall x [A \leftrightarrow B]$, тогда

(10) $\forall x A_1 \ldots A_n A \leftrightarrow \forall x A_1 \ldots A_n B$
(11) $\exists x A_1 \ldots A_n A \leftrightarrow \exists x A_1 \ldots A_n B$

Список литературы

[1] *Рухая Х. М., Тибуа Л. М., Чанкветадзе Г. О., Миканадзе Г. М.* Безранговая формальная математическая теория // Международная конференция Мальцевские чтения 2012, тезисы докладов. 2012. С. 32.
[2] *Пхакадзе Ш. С.* Некоторые вопросы теории обозначений. Тбилиси: Изд. ТГУ, 1977. С. 195.
[3] *Бурбаки Н.* Теория множеств. М.: Наука, 1965. С. 3–13.
[4] *Rukhaia Kh. M., Tibua L. M.* One Method of constructing a formal system // Applied Mathematics, Informatics and Mechanics. 2006. Vol. 11, № 2. P. 3–15.

Институт прикладной математики им. И. Векуа, Тбилиси (Грузия),
Сухумский государственный университет, Тбилиси (Грузия)
E-mail: khimuri.rukhaia@gmail.com

Логика Даммета, иррефлексивная модальность и полнота по П. С. Новикову

А. Д. Яшин

Пусть Int — интуиционистская пропозициональная логика. *Логика Даммета* (*логика цепей*) определяется как $LC := Int + (A \to B) \vee (B \to A)$. Известно, что LC характеризуется классом конечных цепей

$$\mathbf{C} := \{C_n \mid C_n\text{— } n\text{–элементная цепь}, n \in \omega\}.$$

К пропозициональному языку добавляется одноместная связка $\varphi(\cdot)$, класс формул соответственно расширяется. Формулы без φ называются *чистыми.* В каждой конечной цепи связку φ интерпретируем как *иррефлексивную модальность*

$$x \Vdash \varphi(A) :\Leftrightarrow \forall y > x : y \Vdash A.$$

Множество $\mathcal{LC}$ формул расширенного языка, общезначимых в классе $\mathbf{C}$, является φ-логикой в смысле П.С.Новикова над LC, т.е. включает в себя LC и содержит аксиому замены для φ: $(A \leftrightarrow B) \to (\varphi(A) \leftrightarrow \varphi(B))$. Более того, $\mathcal{LC}$ является консервативным расширением LC, т.е. для любой чистой формулы A из $A \in \mathcal{LC}$ следует $A \in LC$. (Первоначальные формулировки подхода П.С. Новикова даны в [**1, 2**].)

В работе [**3**] построено счётное семейство φ-логик $\mathcal{L}_k$, каждая из которых определяет новую неконстантную связку в LC. Все они попарно несовместимы над LC, т.е. φ-логика $\mathcal{L}_k + \mathcal{L}_m$ неконсервативна над LC при $k \neq m$.

Теорема 1. *$\mathcal{LC}$ определяет новую неконстантную логическую связку (по П.С. Новикову) φ в логике Даммета LC. При этом $\mathcal{LC}$ несовместима с каждой из $\mathcal{L}_k$.*

В соответствии с проблемой П.С.Новикова интерес представляют максимальные консервативные ($\equiv$ *полные по П.С. Новикову*) расширения, определяющие новую неконстантную связку в LC.

Теорема 2. *$\mathcal{LC}$ является примером полного по П.С. Новикову расширения логики Даммета с новой неконстантной связкой.*

Список литературы

[1] *Сметанич Я. С.* О полноте исчисления высказываний с дополнительной операцией от одной переменной // Труды Московского математического общества. 1960. Т. 9. С. 357–371.

[2] *Сметанич Я. С.* Об исчислениях высказываний с дополнительной операцией // Доклады АН СССР. 1961. Т. 139, № 2. С. 309–312.

[3] *Яшин А. Д.* Иррефлесивная модальность как новая логическая связка в логике Даммета // Сибирский математический журнал. 2014. Т. 55, № 1. С. 228–234.

Московский городской психолого–педагогический университет, Москва
E-mail: yashin.alexandr@ya.ru

On proof search for prenex sentences of infinite-valued first-order Lukasiewicz logic

A. S. Gerasimov

Infinite-valued first-order Łukasiewicz logic Ł∀ is one of the most important fuzzy logics that formalize approximate reasoning [**2**]. Aiming at an efficient proof search system for Ł∀, in [**3**] we introduce the metavariable proof system $\mathrm{T_m}$Ł∀ together with its ground version TŁ∀. These proof systems are more suitable for automatic proof search than the hypersequent calculus GŁ∀ [**1**] and any Ł∀-sentence provable in GŁ∀ is provable in TŁ∀ and $\mathrm{T_m}$Ł∀. However developing algorithms that search for proofs (or check provability) of Ł∀-sentences in TŁ∀ (or other calculi) is an open problem, which we address in this work constraining ourselves to prenex Ł∀-sentences.

Let $\mathrm{G^1}$Ł∀ be the hypersequent reformulation of the tableau-like system TŁ∀, so each rule of $\mathrm{G^1}$Ł∀ is cumulative (i. e., each premise of a rule application contains principal sequent from the conclusion). By $\mathrm{G^2}$Ł∀ denote the hypersequent calculus that is formulated just as $\mathrm{G^1}$Ł∀, but only universal-type quantifier rules are cumulative.

Theorem 1. *For any prenex sentence A, $\vdash_{\mathrm{G^1Ł\forall}} A$ iff $\vdash_{\mathrm{G^2Ł\forall}} A$.*

Then we investigate permutability of some adjacent applications of $\mathrm{G^2}$Ł∀-rules.

Theorem 2. *If a prenex sentence is $\mathrm{G^2}$Ł∀-provable, then there exists a $\mathrm{G^2}$Ł∀-proof of the sentence such that all applications of the propositional rules are above all applications of the quantifier rules.*

Theorem 3. *Suppose $\exists\bar{x}A(\bar{x})$ is a sentence, where $A(\bar{x})$ is quantifier-free; then $\vdash_{\mathrm{G^2Ł\forall}} \exists\bar{x}A(\bar{x})$ iff the hypersequent $\big(\Rightarrow A(\bar{t}_1)|\ldots|\Rightarrow A(\bar{t}_n)\big)$ is $\mathrm{G^2}$Ł∀-provable for some lists $\bar{t}_1,\ldots,\bar{t}_n$ of terms from the Herbrand universe of $A(\bar{x})$. A prenex sentence and its Skolem form are equally provable or unprovable in $\mathrm{G^2}$Ł∀.*

Theorem 4. *The problem of checking $\mathrm{G^2}$Ł∀-provability for prenex existential sentences is undecidable.*

Thus we have an algorithm (based on theorem 3) such that for any prenex sentence it returns "provable" iff the sentence is $\mathrm{G^2}$Ł∀-provable. Furthermore, we work out (using permutability of $\mathrm{G^2}$Ł∀-rules applications) a scheme of algorithms such that for any prenex sentence provable in $\mathrm{G^2}$Ł∀ any algorithm complying to the scheme produces some proof of the sentence.

References

[1] *Baaz M., Metcalfe G.* Herbrand's theorem, skolemization and proof systems for first-order Łukasiewicz logic // Journal of Logic and Computation. 2010. Vol. 20, No. 1. P. 35–54.

[2] *Cintula P., Hájek P., Noguera C., eds.* Handbook of mathematical fuzzy logic. London: College Publications, 2011.

[3] *Gerasimov A. S.* A proof system with metavariables for infinite-valued first-order Lukasiewicz logic // International Conference "Mal'tsev Meeting 2014": Collection of Abstracts, Novosibirsk. 2014. P. 156.

Saint Petersburg (Russia)
E-mail: alexander.s.gerasimov@ya.ru

On the Complexity of Semantic Combinations of Logical Theories

Y. Kazakov, D. Ponomaryov

We consider a novel way of combining logical theories, which generalizes the union operation over axiom sets and allows to specify the signature in which the theories can "interact". To define a combination, one needs to specify a network over a given family of theories which induces agreements between their models. We say that structures $\mathcal{I}$ and $\mathcal{J}$ *agree* on a signature Σ, written $\mathcal{I} =_\Sigma \mathcal{J}$, if the domains of $\mathcal{I}$ and $\mathcal{J}$ coincide and the interpretation of Σ-symbols in $\mathcal{I}$ is the same as in $\mathcal{J}$.

Definition. *A theory network is a finite set $\mathcal{N}$ of tuples $\langle \mathcal{T}_1, \Sigma, \mathcal{T}_2 \rangle$, where $\mathcal{T}_1$ and $\mathcal{T}_2$ are theories and Σ a signature. We say that $\mathcal{T}_1$ imports Σ from $\mathcal{T}_2$.*

A model agreement for $\mathcal{N}$ is a mapping ν that assigns to every theory $\mathcal{T}$ occurring in $\mathcal{N}$ a class $\nu(\mathcal{T})$ of models of $\mathcal{T}$ such that for every $\langle \mathcal{T}_1, \Sigma, \mathcal{T}_2 \rangle \in \mathcal{N}$ and every $\mathcal{I}_1 \in \nu(\mathcal{T}_1)$, there exists $\mathcal{I}_2 \in \nu(\mathcal{T}_2)$, with $\mathcal{I}_1 =_\Sigma \mathcal{I}_2$.

We say that interpretation $\mathcal{I}$ is a model of $\mathcal{T}$ in the network $\mathcal{N}$ (notation $\mathcal{I} \models_\mathcal{N} \mathcal{T}$) if there exists a model agreement ν for $\mathcal{N}$ such that $\mathcal{I} \in \nu(\mathcal{T})$. A theory $\mathcal{T}$ entails a formula φ in the network $\mathcal{N}$ (notation $\mathcal{T} \models_\mathcal{N} \varphi$) if $\mathcal{I} \models \varphi$ whenever $\mathcal{I} \models_\mathcal{N} \mathcal{T}$.

Note that if $\mathcal{N} = \{\langle \mathcal{T}_1, \Sigma, \mathcal{T}_2 \rangle\}$ is a theory network, where Σ contains *all* symbols of $\mathcal{T}_2$, then for any model $\mathcal{I}$, it holds $\mathcal{I} \models_\mathcal{N} \mathcal{T}_1$ iff $\mathcal{I} \models \mathcal{T}_1 \cup \mathcal{T}_2$. A theory network can be seen as a labeled directed multigraph in which nodes are labeled by theories and edges are labeled by signatures. Each edge in this graph, thus, represents an import relation between two theories. Note that the definition also allows for *cyclic theory networks* if this graph is cyclic. That is, a theory may import itself through a chain of import relations.

For a range of Description Logics we consider the complexity of entailment in theory networks, i.e. the problem to decide for a network $\mathcal{N}$, a theory $\mathcal{T}$ occurring in $\mathcal{N}$, and a formula φ, whether $\mathcal{T} \models_\mathcal{N} \varphi$. The obtained results are summarized in the table below, where the notation (a) means that the result holds for acyclic theory networks, and the absence of (a) means that the result holds for arbitrary (i.e. possibly cyclic) networks.

Interval of Logics	Complexity of Entailment
Horn propositional – full propositional	ExpTime-complete/PSpace-complete (a)
logics containing $\mathcal{EL}$	Σ^0_1-complete
$\mathcal{EL}$–$\mathcal{EL}^{++}$	ExpTime-complete (a)
$\mathcal{ALC}$–$\mathcal{SHIQ}$	2ExpTime-complete (a)
$\mathcal{ALCIOF}$–$\mathcal{SHOIQ}$	N2ExpTime-complete (a)
$\mathcal{SR}$–$\mathcal{SRIQ}$	3ExpTime-complete (a)
$\mathcal{SROIF}$–$\mathcal{SROIQ}$	N3ExpTime-complete (a)

University of Ulm, Ulm (Germany)
Institute of Informatics Systems, Novosibirsk (Russia)
E-mail: yevgeny.kazakov@uni-ulm.de, ponom@iis.nsk.su

Fuzzy approach in insurance and finance sector

S. Kumar, A. Gupta

The preventive avoidance of cancelation is a key problem facing insurance companies. A conversation with the client held prior to the latter's decision to cancel a contract increases the likelihood of contract continuity. So companies are in need of reliable expert system that can help them to evaluate the risk of cancelation of the policies in future. With the help of fuzzy system it is possible to identify clients who may potentially cancel and take timely measures to safeguard the portfolio. Here a model is presented, which is designed by using fuzzy mathematics and expert system to provide indicative results on the risk of cancelation of the policies in future.

Dr. B. R. Ambedkar University, Agra (India)
E-mail: sanjeevibs@yahoo.co.in

VIII. Авторский указатель